Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский институт информатики и автоматизации
Российской академии наук (СПИИРАН)

На правах рукописи

Лившиц Илья Иосифович

Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени доктора технических наук

Научный консультант
доктор технических наук, профессор
Молдовян Александр Андреевич

Санкт-Петербург – 2018

СОДЕРЖАНИЕ

Введение

Актуальность темы исследования. В настоящее время увеличивается количество атак злоумышленников, направленных не столько на данные, сколько на компоненты систем управления и технологические процессы различных критичных объектов. Соответственно, значительно увеличилась актуальность общей проблемы создания интегрированных систем менеджмента (ИСМ) для обеспечения безопасности объектов, именуемых сложными промышленными объектами (СлПО). Фокус интересов данных работ обращен к решению актуальных проблем информационной безопасности (ИБ), т.к. современный уровень информационных технологий (ИТ) практически обеспечил глубокое погружение в автоматизацию производственных процессов, поддержку принятия управленческих решений для высшего менеджмента (лиц, принимающих решения – ЛПР), реализацию автоматических (автоматизированных) процедур защиты и аудита состояний технических систем и промышленной автоматики. Применение ИТ призвано снизить сложность управления производственных процессов в режиме, близком к режиму реального времени (РРВ), но, вместе с тем, привнесло характерные риски в обеспечение безопасности СлПО. Известные подходы управления ИБ, основанные на риск-ориентированных стандартах, позволяют предложить набор систем менеджмента (СМ), базирующихся на «классическом» цикле PDCA и имеющих успешные практические отраслевые реализации. В целях оптимизации затрат и повышения уровня качества управления в последнее время для многих крупных СлПО реализуются проекты ИСМ. Проведенный анализ выполненных проектов создания ИСМ (как в Российской Федерации, так и в мире) с целью обеспечения ИБ для СлПО, а также конкретных систем менеджмента информационной безопасности (СМИБ) – как отдельно, так и в составе ИСМ, оценка их результативности за длительные периоды наблюдений, позволил установить **ряд объективных противоречий** между требованиями практики и существующими положениями теории обеспечения ИБ на современном этапе.

Первое противоречие связано с тем фактом, что значительное количество разработанных стандартов (международных, государственных, отраслевых) обуславливает широчайшую вариативность комбинаций их применения для целей обеспечения ИБ в ИСМ для СлПО. В частности, национальные стандарты ГОСТ Р не успевают обновляться синхронно с пересмотром международных стандартов ISO (например, ISO/IEC 27001:2013 и ГОСТ Р ИСО/МЭК 27001-2006). Более серьезное отставание демонстрируют ведомственные (отраслевые) системы стандартизации, где запаздывание идет уже на 2 и более поколения (например, стандарт СТО Газпром 4.2-3-003-2009 СОИБ «Анализ и оценка рисков»[1] содержит ссылку на отмененный британский стандарт BS серии 7799:3 выпуска 2006 г., а «Положение по аттестации объектов информатизации по требованиям безопасности информации» утверждено еще председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.).

Второе противоречие определяется тем фактом, что выбор наилучшего множества применимых стандартов для формирования ИСМ по критерию наилучшего достижения поставленной цели – обеспечение заданного уровня ИБ в ИСМ для СлПО, затруднен отсутствием механизма единственного гарантированного «разумного подхода» ЛПР (в терминах Парето). В частности, ряд публикаций существенно ограничивают (или даже исключают) роль ЛПР в формировании «разумного подхода» к выбору и ограничению критериев. Соответственно, возникает риск неверного определения целей создания ИСМ как единой системы управления (СУ) для СлПО и функциональной неполноты при формировании области распространения ИСМ (*scope*), в частности, на процессы ИБ. На практике наблюдаются ситуации, при которых *scope* всех СМ в составе ИСМ необоснованно стремятся сделать равным, при этом не принимается во внимание, что технические решения (в частности, СМИБ) не в полной мере могут гарантировать требуемый уровень обеспечения ИБ для полного перечня бизнес-процессов СлПО. Кроме того, от ЛПР ожидают

[1] http://vniigaz.gazprom.ru/activities/other/standardization-and-certification/zakaz-dokumentov-sistemy-stand/

фиксированного перечня множества применяемых критериев и ограничения их размерности, при которых задача выбора парето-оптимального множества решений имеет перспективы результативного применения в приемлемое время (РРВ). Для целей обеспечения заданного уровня ИБ необходимо решать несколько противоречивых задач, в частности – перечень и размерность критериев доступных к внедрению СМ, ограниченность бюджета, временных ресурсов и доступность квалифицированного персонала на определенный временной интервал.

Третье противоречие вызвано стремлением ЛПР к снижению издержек в процессах жизненного цикла (ЖЦ) ИСМ, что не всегда согласуется с требованиями формирования внутреннего и внешнего контекста (*context*, с учетом требований Annex SL 2012 г.), применения риск-ориентированного подхода и минимизации потерь при возникновении факторов и проявлений рисков в СлПО. Данное противоречие обусловлено также высокой динамикой изменений, присущих всем СлПО, тем более, функционирующих круглосуточно, например, объектам топливно-энергетического комплекса (ТЭК) и аэропортовых комплексов (АК). Попытки ЛПР по снижению издержек на ИСМ хорошо согласуются с общими принципами бизнеса, но в тоже время не в полной мере обеспечивают принцип «процессного подхода», предложенного Э.Демингом. Более того, на практике наблюдаются попытки ЛПР по блокированию «вторжения» моделей и решений ИБ в существующие исторически механизмы управления, необоснованной минимизации количества применяемых технических средств (мер) обеспечения ИБ (*controls*), что явно негативно влияет на полноту оценки и привносит новые риски в проекты ИСМ в СлПО. Соответственно, проект ИСМ, реализованный не в полной мере, не будет способен обеспечивать ЛПР оперативной, достоверной и необходимой информацией для принятия эффективных управленческих решений в части обеспечения ИБ для СлПО. В частности, произошедшие инциденты на объектах ТЭК (Япония, Украина, Германия, США, Китай, Саудовская Аравия) и АК

(Польша, Великобритания, Бельгия) объективно подтверждают важность данного противоречия.

Четвертое противоречие связано с проблемой соответствия законодательным требованиям (*compliance*) и обеспечения повышения стоимости СлПО как совокупности ценных активов благодаря низкой аварийности, высокой устойчивости (*sustainability*), лучшей отраслевой репутации, управляемости, экономической эффективности ИСМ. Это противоречие на практике демонстрируется разноплановыми и несогласованными требованиями различных регуляторов, частыми изменениями существующей нормативной и законодательной базы (например, постоянные изменения 152-ФЗ «О персональных данных»), а также негативными последствиями социальных и политических конфликтов. Обратим внимание, что по данным экспертов RSA в течение года может быть внесено свыше 8000 изменений только финансового (банковского) законодательства. На практике отмечено, что организации, внедрившие ИСМ, легче парируют дестабилизирующие воздействия в силу единого системного подхода к менеджменту рисков. Однако в практике аудита наблюдается, что ЛПР уделяют вопросам соответствия законодательным требованиям ровно такое минимальное внимание, которое позволяет принятая бизнес-практика. В частности, указанная проблема наиболее явно проявилась при внезапном прекращении сервиса со стороны международных платежных систем Visa и MasterCard в отношении ряда банков в 2014 г. Этот пример также показал, что современное банковское сообщество на существующей ступени развития ИТ оказалось не готово к реализации известных угроз, даже при наличии у профильного регулятора – ЦБ РФ собственной отраслевой системы стандартизации в области ИБ – СТО БР ИББС.

Преодоление указанных противоречий между текущим состоянием теории и требованиями практики обеспечения ИБ для СлПО требует решения ряда задач научного характера, направленных на развитие теории ИБ как системы взаимосвязанных идей, основанных на классических трудах в области

кибернетики, системного анализа и обеспечения безопасности, учитывающих также перспективные подходы стандартизации и применения современных риск-ориентированных стандартов, которые дают целостное представление о закономерностях, принципах, тенденциях и условиях обеспечения ИБ для СлПО. В представленной диссертационной работе изложены научно обоснованные методические подходы и технические решения, применение которых вносит вклад в повышение уровня ИБ для СлПО нашей страны.

Степень разработанности проблемы. Научные разработки автора, представленные в настоящем исследовании, сформировались прежде всего на базе научных работ В.И. Воробьева, И.А. Зикратова, И.В. Котенко, В.М. Крикуна, В.Н. Кустова, В.А. Липатникова, П.А. Лонциха, А. А. Молдовяна, В.Д. Ногина, И.Б. Саенко, Б.В. Соколова, Р.М. Юсупова и др., а также зарубежных ученых Э. Деминга, Н. Винера, Р. Кини, С. Кобле, Д. Мако, М. Месаровича, И. Пригожина, Х. Райфа, И. Такахара, Д. Чаума, Б. Шнайера, и др.

Анализ современных работ свидетельствует, что наряду с имеющимися существенными достижениями в области обеспечения ИБ – как в соответствии с требованиями международных стандартов (ISO, IEC, IATA), государственных стандартов (ГОСТ Р) и отраслевых требований (СТО БР ИББС, СТО Газпром СОИБ), в настоящее время недостаточно разработаны методологические подходы к обеспечению ИБ для СлПО.

Известны научно-методические подходы ФСТЭК и ФСБ к построению моделей угроз и защиты государственных информационных ресурсов, а также ключевых систем информационной инфраструктуры (КСИИ), которые широко применяются в РФ. Основной акцент этих методических документов сделан на формировании статической модели нарушителя, фиксированного перечня деструктивных действий (ДД), угроз безопасности информации (УБИ), экспертной оценки вероятности реализации и уровня значимости угроз для объектов защиты (ОЗ), прежде всего – информационных систем обработки персональных данных (ИСПДн). За исключением отдельных нормативных актов (в частности, Приказы ФСТЭК № 31 от 14.03.2014) практически не применяется

подход менеджмента рисков, основанный на современных риск-ориентированных стандартах, более того, практически не встречаются процедуры учета остаточных рисков, особенно для СлПО.

В работах Р.М. Юсупова, Б.В. Соколова и ряда других авторов широко освещается новая расширенная концепция ИБ, под которой, в отличие от «стандартной базы» ISO, понимается следующая триада: защита информации, защита от информации и добывание информации о намерениях и возможностях противоборствующей стороны в информационной сфере. Данная триада, к сожалению, не рассматривается подробно в нормативных документах ФСБ, ФСТЭК, соответственно, не предложены решения для обеспечения полного цикла ИБ для ИСМ в СлПО.

В современных автоматизированных системах управления (АСУ) СлПО (например, Siemens, Yokogawa, Hirschmann) представляется и, соответственно, обрабатывается только информация о состояниях отдельных компонентов, иногда – о статусах компонентов, но не всего ОЗ в целом. Создание АСУ применительно к процессам обеспечения ИБ является до сих пор сложной задачей, решение которой также затрудняется невысокой «информационной культурой» менеджеров и даже ряда специалистов. В частности, по данным РТ за 2017 г. количество подключенных к сети интернет критических систем возросло в 1,5 раза. Решения класса GRC («Governance, Risk management and Compliance»), предложенные известными разработчиками (например, SAP, Oracle, RVision), пока не находят широкого применения в силу высокой сложности внедрения, фрагментарного охвата функций безопасности, обязательным участием многочисленного и дорогостоящего персонала для ручной настройки и высокой стоимостью.

В работах Ю.А. Арбузова, В.Г. Лим, В.Н. Химич рассмотрены вопросы обеспечения ИБ в АСУ предприятий ТЭК. Предложена методология построения модели угроз и приведена схема алгоритма формирования модели угроз ИБ в АСУ для объектов ТЭК. В работах М.В. Кремкова и А.В. Корнеева систематизированы наиболее характерные внутренние производственные,

технические и финансово обусловленные риски, имеющие место в работе предприятий ТЭК и даны рекомендации по своевременному учёту и управлению рисками при отражении кибернетического нападения, в том числе – опыт по защите энергетической инфраструктуры от дистанционного кибертерроризма. Отметим, что термин «*кибербезопасность*» был определен в Рекомендации МСЭ-Т X.120 (утвержденной в 2010 г.), при этом отмечались такие общие задачи как обеспечение доступности, целостности (которая может включать аутентичность и неотказуемость) и конфиденциальности.

В то же время, как показывает общий анализ печатных работ и выступлений на научно-практических конференциях, существенную проблему представляет методический и последующий технологический разрыв между средствами обеспечениям ИБ (*controls*), функционирующими в масштабе времени, близком к РРВ, с одной стороны, и базовыми возможностями СУ по комплексной оценке уровня ИБ, конкретно – наиболее «медленной» ее составляющей (в частности, процессы аудита) – с другой стороны.

Следует заметить, что эту проблему поднимали Н.Винер и И.Пригожин в своих работах по теории кибернетики, но актуальность решения данной проблемы объективно сохраняется до сих пор. Например, в годовом отчете Cisco по ИБ за 2016 г. отмечается, что с мая 2015 г. компания Cisco сократила среднее время до обнаружения известных УБИ до 17 часов (то есть меньше одних суток)[2]. При этом отмечается, что достигнутый показатель намного превосходит текущие средние оценочные показатели в отрасли, которые составляют от 100 до 200 дней. В ряде зарубежных стандартов и методик (ISO, IEC, NIST, ISAGO, IEEE, ITIL, COBIT, TOGAF и пр.) проблеме обеспечения ИБ для СлПО также уделяется пристальное внимание, однако, даже несмотря на более частое применение риск-ориентированных стандартов, общей универсальной концепции, увязанной с фазами жизненного цикла (ЖЦ) и «сквозного» управления рисками, с общими принципами реализации механизмов ИБ в ИСМ (в цикле PDCA) к настоящему времени не представлено.

---

[2] blogs.cisco.com/security/talos/locky-returns-necurs

В работах Б.Г. Юдина, Р.М. Юсупова, Б.В. Соколова отражены новые подходы к созданию защищенных ИС, которые предоставляют практические реализации новых направлений в науке, в частности – «технонауки» (*technoscience*). Показано, что новые признаки «технонауки» – это существенно более глубокая интеграция результатов научного познания в процесс создания (применения) новых технологий, неуклонное приближение науки и соответствующих технологий к человеку. Новое направление «технонауки» хорошо увязывается с общими принципами классической кибернетики – более активное применение контуров обратной связи для усиления полезных воздействий контуров отрицательной обратной связи для ослабления нежелательных входных воздействий, внутренних возмущений и ускорения стабилизации защищаемого объекта (СлПО) в заданных пределах.

В то же время на практике не представлены ИСМ, которые, применительно к СлПО, обеспечивают требуемый доказательный уровень обеспечения ИБ. До сих пор основной метод противодействия злоумышленным действиям заключался в «привязке» фиксированного перечня УБИ и, соответственно, рекомендации выбора фиксированного перечня мер защиты, но не «настройки» процессов ИСМ (например, управления инцидентами, управления непрерывностью функционирования, управления аудитом). Такой подход наблюдается для АСУ (АСУ ТП), для которых практически реализуют только базовый уровень обеспечения ИБ. В работах зарубежных ученых Д. Кэннона, С. Кобле, Л. Дерека, Л. Гордона, Г. Хинсона и др. отражены современные проблемы идентификации, управления стоимостью, формирования и применения метрик ИБ, в том числе для СлПО.

Существенным недостатком современных подходов к созданию, внедрению, документированию и сопровождению ИСМ является практическое отсутствие достоверного методического аппарата для получения численных оценок уровня ИБ, в том числе алгоритмов доказательного формирования оптимального перечня метрик ИБ, контроля адекватности процесса оценивания и финального этапа – получения достоверных оценок уровня ИБ в СлПО для

ЛПР в режиме, близком к РРВ. В частности, не представлена оценка результативности СУ, которую в ряде работ предлагается формировать через суперкритерии (например, Р. Кини, Х. Райфа, И. Пригожин, Ф. Перегудов и др.), что не позволяет использовать надежный математический аппарат для ИСМ в СлПО. Отчасти, положения теории Парето для доминирующих множеств позволяют формировать вектора принятия решения для дискретного числа альтернатив и применять эффективно для выбора оптимального для принятия решения ЛПР множества. Но в то же время необходимо отметить, что до настоящего времени не предложено метода оценки компонент векторов возможных решений при условии значительного различия их значимости (ценности) и возможных замещений – применительно к задачам обеспечения ИБ для СлПО. Наилучшей иллюстрацией данного факта является многолетняя «эффективная» работа вируса Stuxnet, в создании которого обоснованно подозреваются специальные службы ряда государств. Приблизительные задержки в развитии ядерной программы Ирана без какого-либо силового вмешательства или военной операции составили 4 года, а в результате управляемого увеличения резонанса частот были разрушены 1888 центрифуг для обогащения урана из более 5 тыс. имеющихся[3].

Практически не представлены работы (за исключением исследований А.Н. Ефимова и Г. Хинсона), позволяющие предложить гибкий и простой математический аппарат для формирования наиболее оптимального множества метрик ИБ, адаптивных к динамически изменяемым требованиям в ИСМ, в частности – изменениям внешнего и/или внутреннего контекста. Очевидно, что введение в существующий к настоящему времени математический аппарат функций риск-менеджмента, «привязки» к фазам ЖЦ (для каждого уникального СлПО) и введения соответствующих контуров обратной связи (соответствующих циклу PDCA) позволило бы значительно поднять скорость принятия эффективного управленческого решения ЛПР. Представляется перспективным реализовать совместно функции риск-менеджмента, гибкой

[3] http://www.iiss.org/en/persons/mark-s-fitzpatrick

обратной связи, «замыкания» цикла PDCA, простого и эффективного математического аппарата в модели «мгновенных аудитов» ИБ. В развитии этого метода оптимизации служит обоснование способности противостоять современным атакам, в том числе целевым (таргетированным) атакам ATP (*advanced persistent threats*).

Обратим внимание на обзор[4], в котором эксперты в области ИБ в 2016 г. формируют основные угрозы современной цифровой экономике:

1. По данным Генпрокуратуры РФ, количество киберпреступлений выросло в 4 раза (до 44 тыс.) по причине резкого роста числа мошенничеств (с 2,2 тыс. до 13,4 тыс.) и краж (2,3 тыс. до 8,5 тыс.), совершенных с помощью Интернета. При этом в 5,5 раза (с 995 до 5,5 тыс.) увеличилось количество фактов хищений, удалений и блокировки компьютерной информации.
2. По усредненным оценкам экспертов, экономический ущерб от кибератак достиг 203,3 млрд. руб. (0,25% ВВП России), из которых 79,8 млрд. составили затраты на устранение последствий атак. При этом с кибератаками столкнулись 92% из 600 респондентов.

В том же обзоре высказываются опасения, что деятельность созданных 15 лет назад спецподразделений МВД России не всегда соответствует масштабу и скорости распространения киберугроз. Отметим обзор НКЦКИ, согласно которому в 2017 г. количество инцидентов, в расследовании которых принимал участие НКЦКИ, по сравнению с 2016 г. увеличилось в 5 раз. В абсолютных значениях, в 2017 г. ФСБ приняло участие в расследовании порядка 200 инцидентов, а также закрыло более 3 тыс. вредоносных ресурсов[5].

Выступление Президента РФ В.В. Путина на пленарном заседании Петербургского международного экономического форума (ПМЭФ-2017) являлось важнейшим в современной истории РФ импульсом к обеспечению цифрового суверенитета. По стенографическому отчету от 2 июня 2017 года о пленарном заседании ПМЭФ-2017 выделим важнейшие тезисы, цитата[6]:

---

4 http://www.ng.ru/ideas/2016-12-23/5_6893_kiber.html
5 https://www.securitylab.ru/blog/personal/plutsik/343983.php?R=1
6 http://kremlin.ru/events/president/news/54667

1. *«Необходимо сформировать принципиально новую, гибкую нормативную базу для внедрения цифровых технологий во все сферы жизни. При этом все решения должны приниматься с учётом обеспечения информационной безопасности государства, бизнеса и граждан»;*
2. *«Будем создавать опорную инфраструктуру цифровой экономики, в том числе безопасные линии связи и центры обработки данных. Кстати, обращаю внимание, это должна быть инфраструктура, основанная на самых передовых технологиях и разработках»;*
3. *«И в авиации, и в других сферах, которые являются критически важными для развития России, нам нужны именно свои разработки и компетенции. Надо их восстанавливать или создавать заново. Это передовые производственные технологии и материалы, энергетика и системы накопления энергии, транспорт и управление логистикой, системы информационной безопасности…».*

Следует отметить, что по данному вопросу опубликовано достаточное количество материалов и эта тематика заслуженно занимает повестку дня самых представительных конференций по тематике обеспечения ИБ. Прошедший в Санкт-Петербурге ПМЭФ-2017 снова поднял данную проблему, на этот раз – на уровень Президента РФ. Этот факт свидетельствует о том, что, несмотря на определенное движение и наличие в РФ ряда профильных организаций, до решения поставленной проблемы еще далеко.

На Международном конгрессе по кибербезопасности, прошедшем в Москве 5–6 июля 2018 г. Президент РФ Путин В.В. отметил: «*Особого внимания, конечно, требует сегодня безопасность глобального информационного пространства. Мы видим, что количество угроз и рисков здесь только растёт. Так, по данным Всемирного экономического форума, в 2017 году потери только от кибератак в мире составили порядка триллиона долларов США, и, по мнению экспертов, если не предпринимать эффективных, результативных мер ущерб будет ещё больше. Как и другие страны, Россия также сталкивается с подобными вызовами. К примеру, в первом квартале этого года по сравнению с*

аналогичным периодом прошлого года число кибератак на российские ресурсы увеличилось на треть»[7].

Кроме того, были даны четкие направления обеспечения в области оценки (аудита): «*В-третьих, будем стремиться, чтобы действующие в России программное обеспечение и инфраструктура связи основывались на отечественных технологиях и решениях, которые прошли соответствующую проверку и сертификацию – конечно, не в ущерб конкуренции: само собой разумеется, речь идёт о конкурентоспособных продуктах, соответствующих самым высоким запросам потребителей*».

И особо была подчеркнута роль международных стандартов, необходимых для обеспечения ИБ на необходимом уровне: «*При этом особенно важно выработать единые правила игры, общие для всех международные стандарты, которые бы максимально учитывали права и интересы всех государств, были бы универсальными, приемлемыми для всех*».

Также необходимо принять во внимание то обстоятельство, что, по мнению экспертов РАЭК, законы принимаются без учета мнения «технарей», тех, кто создает цифровую действительность[8]. В частности, отмечается, цитата: «*Государства и компании игнорируют стандарты, в том числе стандарты безопасности, которые кропотливо разрабатывало сообщество… Часто действия государства увеличивают угрозы для критической инфраструктуры цифрового мира — например, попытаться «запретить VPN», потребовать хранить все данные пользователей или передавать ключи шифрования на самом деле приводят к снижению безопасности*».

Более того, по мнению эксперта в области ИБ И. Пискунова, с ГосСОПКА «*отнюдь не все так гладко по причине целого ряда технических проблем. Речь идет об отсутствии собственного программного обеспечения многих классов, как общесистемного (операционных систем, систем управления базами данных), так и прикладного (например, для моделирования месторождений); об*

---

7 http://kremlin.ru/events/president/news/57957

8 http://spb.rbcplus.ru/news/595ad6d37a8aa91a5880836a

отсутствии собственной элементной базы и отечественного телекоммуникационного оборудования на всей территории страны»[9].

Опубликованные работы зарубежных ученых и специалистов в области ИБ свидетельствуют о достаточном внимании к методам и практикам только отдельных, фрагментарных процессов в широком перечне требований ИСМ, например: управления идентификацией (работы С. Кобле, М. Хансена, Д. Чаума), управления безопасностью ПДн (работы А. Аквисти), управления чрезвычайными ситуациями (работы С. Дое), применения метрик ИБ (К.Бротби и Г. Хинсона). В то же время, факты свидетельствует о том, что эффективные исследования по множеству указанных выше направлений, тем не менее, не позволяют предложить целостный подход для комплексного противодействия современным угрозам ИБ для СлПО. В этой связи, крайне актуальным представляется постулат Н. Винера о методе управления с помощью информирующей обратной связи и предложенный подход к локализации ошибок обратным процессом, с условием, что бы проверка шла с такой же скоростью, что и само вычисление. Эти положения нашли свое применение в принципах аудита ИБ, основанных на цикле PDCA (цикле Деминга-Шухарта) и положительно зарекомендовавших на практике, в том числе – при реализации ИСМ (например – «КАМАЗ-Дизель», «Дальневосточное морское пароходство», «Транснефть», «Газпромнефть – ОНПЗ», «Газпром трансгаз» и пр.).

В опубликованных работах также не рассматриваются процессы проектирования ИСМ (как СУ в составе СлПО) с позиции обеспечения экономического баланса между стоимостью защищаемых активов в составе СлПО с уровнем обеспечения ИБ, заданным ЛПР, с одной стороны, и стоимостью комплекса технических средств (мер) ИБ, внедренных в строгом соответствии с функцией экономической эффективности ИСМ в СлПО, с другой стороны. В простейших рассмотренных случаях демонстрируется только фиксированный набор средств (мер) ИБ, рекомендованный ФСТЭК (Приказы №№ 31, 235, 239) и/или ФСБ (Приказ №796) и внедренных для типовых решений

---

9 http://www.ng.ru/ideas/2016-12-23/5_6893_kiber.html

– объектов ТЭК, Удостоверяющих Центров (УЦ), ИСПДн (152-ФЗ) и иных объектов информатизации – для целей аттестации. В зарубежной практике широко применяются «Общие критерии» (ISO/IEC 15408), а также новые модифицированные варианты, в частности, cPP (*common process performance*), призванные упростить и значительно ускорить процедуры формальной оценки информационных систем (ИС) и отдельных устройств.

Обобщая вышеизложенное, **научная проблема** представленной диссертационной работы формулируется как проблема разрешения противоречий между состоянием теории обеспечения ИБ и современными требованиями практики по обеспечению ИБ в ИСМ для СлПО.

Для решения данной проблемы потребуется пересмотр существующих статичных моделей УБИ и ДД, дополнительная и всеобъемлющая интеграция риск-менеджмента, учет требований, предъявляемых к планированию, выполнению и совершенствованию системы аудита ИБ в СлПО, принятие решения ЛПР при фиксированном множестве альтернатив, создание новых подходов к реализации аудита ИБ в СлПО, базирующихся на применении:

- моделей (***M = { M | f (a′, r′, k′, t′, g′) }),*** свойства которых ***(a′, r′, k′, t′, g′)*** функционально зависят ***f (a′, r′, k′, t′, g′)*** от свойств: ***A*** (требований к аудиту ИБ), ***R*** (собственных свойств ТС), ***K*** (мер и средств обеспечения ИБ), ***T*** (совокупности требований в аспекте ИБ для СлПО) и ***G*** (совокупности ДД и выявленных рисков);
- методов (***m***), обеспечивающих идентификацию, оценку и анализ объективных свидетельств (***C***) аудита ИБ при формировании эффективных решений ЛПР (***N***) с помощью оператора (***O***) в соответствии с установленными требованиями.

Математическая запись научной проблемы может быть представлена как:

Найти ***M: (A → A′, R → R′, K → K′, T → T′, G → G′),*** для

$\forall a' (a' \in A),\ \forall r' (r' \in R), \forall k' (k' \in K),\ \forall t' (t' \in T),\ \forall g' (g' \in G),$ такие что:

$\exists\ (N = N' \{M, a, a', r, r', k, k', t, t', g, g', \Delta N\}),$ при $\| N - N' \| \rightarrow \Delta \mathbf{N_{min}}$

$$m: C \xrightarrow{0} N$$

Актуальность и степень разработанности темы определяют **цель диссертационного исследования**: снижение длительности и стоимости аудита ИБ за счет использования новых моделей и методов аудита ИСМ, реализующих оперативное формирование количественной оценки уровня обеспечения ИБ в ИСМ для СлПО, выбор и применение наилучшего множества средств (мер) обеспечения ИБ для обработки выявленных рисков.

Достижение поставленной цели потребовало решения следующих **задач** для обеспечения требуемого уровня ИБ в СлПО:

1. Исследование системных требований, предъявляемых к процессам обеспечения ИБ в СлПО и выявление закономерностей между системными изменениями требований регуляторов, стандартов (международных, национальных, отраслевых) и объективными потребностями создания ИСМ для различных отраслей промышленности;
2. Исследование системных требований, предъявляемых при создании современных ИСМ, предназначеннх для защиты ценных активов и риск-ориентированного подхода при обеспечении ИБ для СлПО, а также формирование оптимального перечня критериев для оценки результативности ИСМ;
3. Исследование, анализ и создание иерархической структуры показателей (метрик) ИБ в процессах обеспечения ИБ, предназначенных для формирования требований к ИСМ для СлПО;
4. Разработка и обоснование методов обеспечения ИБ в составе ИСМ, с учетом минимизации издержек по защите перечня активов и, в частности, увеличения стоимости нематериальных активов (*goodwill*) СлПО;
5. Исследование практической применимости предложенных методов обеспечения ИБ в составе ИСМ для СлПО для различных отраслей.

Объект исследования: Интегрированные системы менеджмента (в аспекте информационной безопасности) для сложных промышленных объектов

Предмет исследования: Методы анализа, оценки и оптимизации процессов обеспечения ИБ для сложных промышленных объектов на основе современных риск-ориентированных международных стандартов.

Методы исследования. В качестве основных методов исследования использованы методы системного анализа, методы декомпозиции и агрегирования, теории автоматизированного управления, теории вероятностей, теории многокритериального выбора при фиксированном наборе альтернатив.

Цель исследования достигается решением научной проблемы исследования существующих подходов при разработке, внедрении и внешней независимой оценке (аудите) ИСМ и разработкой новых методов для обеспечения ИБ в СлПО.

Теоретической базой исследования являются работы Р.М. Юсупова, А.А. Молдовяна, И.Б. Саенко, И.В. Котенко, А.С. Маркова в области ИБ, обеспечения комплексной безопасности и теории управления. Развитие существующих подходов в области ИБ основано на предложенном ранее автором методе оценки (аудите) СМИБ на основе модифицированного метода анализа иерархий (МАИ), дополненном совокупностью необходимых моделей и методов. Дальнейшее развитие этого подхода применительно к поставленной научной проблеме состоит в расширении на основе базовой модели аудита ИСМ, специальным блоком оптимизации – для целей получения оценки уровня обеспечения ИБ СлПО в режиме, близком к РРВ. С учетом указанных выше особенностей проведения аудита ИБ в ИСМ для СлПО, центральное внимание должно быть уделено блоку оптимизации в предложенной модели, точнее формированию перечня оптимальных критериев для нахождения множества парето-оптимальных решений. Блок оптимизации учитывает («на входе») степень результативности бизнес-процессов СлПО (в том числе – оценки уровня обеспечения ИБ) и отрабатывает необходимые изменения в модели ИСМ («на выходе»), т.е. позволяет вносить управляющие воздействия в цикле PDCA по каналам обратной связи со скоростью, близкой к РРВ. Поставленная задача решается через формирование численной оценки результативности (оценки по

численным метрикам ИБ) как для отдельной СМИБ (частный случай), так и для ИСМ (общий случай).

Научные положения, выносимые на защиту. Решение задач диссертационного исследования позволило разработать и обосновать ряд научных положений, которые выносятся на защиту.

Первое научное положение – обобщенная модель ИСМ для обеспечения безопасности ИСМ, базовая модель аудита ИСМ и система численных показателей (метрик) ИБ для выполнения аудита ИСМ. Раскрыта специфика процесса планирования, выполнения и анализа результатов аудита ИБ в ИСМ, заключающаяся в широком применении системы численных показателей (метрик) ИБ для оценки результативности ИСМ согласно применимым требованиям. Предложенные новые модели: обобщенная модель ИСМ для обеспечения безопасности ИСМ и базовая модель аудита ИСМ совместно с новой системой численных показателей (метрик) ИБ дополняют существующие традиционные методы выполнения аудита и позволяют применять численные оценки показателей (метрик) ИБ как оценки результативности ИСМ в статическом и динамическом (прогнозном) вариантах в режиме, близком к РРВ.

Второе научное положение – метод проведения аудита ИСМ для СлПО. На основе выявления наиболее значимых потребностей ЛПР, предложен новый метод проведения «мгновенных аудитов» ИБ в ИСМ для СлПО. Новый метод, в отличие от известных методов аудита, позволяет учесть расширенный перечень критериев аудита (например, требований регуляторов и/или отраслевой специфики) и отличается применением численных показателей (метрик) ИБ с учетом специфики обеспечения безопасности различных видов СлПО. Предложенный метод реализует новый принцип управления аудитом ИБ по частоте и предоставляет ЛПР оценку роста уровня обеспечения ИБ в СлПО как показатель результативности (*effectiveness*) СМИБ (ИСМ) и соответствия применимым требованиям.

Третье научное положение – метод исследования динамики сертификации по международным стандартам ISO для СлПО. Предложен новый метод

исследования показателей динамики сертификации, основанный на публичных статистических данных ISO, устанавливающий оценку влияния «лидеров» разного ранга и учитывающий приоритеты отраслей в соответствии с международными кодами экономической деятельности ЕАС. Новый метод позволяет оценить «входные» динамические изменения потребностей бизнеса, выраженные в изменении предпочтений ЛПР по составу внедряемых СМ, прошедших внешний (независимый) аудит в составе ИСМ и формировать прогнозные оценки.

Четвертое научное положение – метод многошаговой оптимизации процесса аудита ИБ в ИСМ для СлПО, который, в отличие от известных стандартов ISO, обеспечивает координацию, распределение ресурсов и оперативное информирование ЛПР по оценке результативности аудита ИСМ. Предложенный метод обеспечивает научно обоснованное и целенаправленное функционирование СМИБ как самостоятельной СМ или в составе ИСМ, и отличается от существующих методов циклической непрерывной оценкой ИБ на основе оптимальной системы численных показателей (метрик) ИБ.

Научная новизна представленной диссертационной работы состоит в следующем. Впервые в целостном функциональном представлении сформулирован научно-методический аппарат для обеспечения аудита ИБ для СлПО, основанный на современном комплексном риск-ориентированном подходе, специальных моделях и методах выполнения аудита ИБ в СМИБ как самостоятельной СМ или в составе ИСМ. Результатом исследования нескольких смежных научных областей (теории управления, теории множеств и теории принятия решений), явилось развитие понятийного аппарата теории обеспечения ИБ для СлПО, а также разработка новых связанных моделей и методов аудита ИБ, позволяющих формировать оптимальный перечень метрик ИБ и выполнять количественную оценку уровня обеспечения ИБ. Новизна комплекса моделей и методов заключается в формировании функционально завершенной структуры для выполнения аудита ИБ в ИСМ.

Новизна первого научного положения заключается в том, что впервые предложены обобщенная модель ИСМ для обеспечения безопасности ИСМ и базовая модель аудита ИСМ, которые, в отличие от известных моделей, содержат все базовые сущности для выполнения аудита и совместно с новой системой численных показателей (метрик) ИБ для выполнения аудита ИБ позволяют генерировать численные оценки уровня обеспечения ИБ. Новая модель аудита ИСМ предполагает использование единого множества метрик, но на разных интерфейсах (для внутреннего и для внешних потребителей). Также введено воздействие на объект оценки (ОО), которое реализуется через подсистему анализа со стороны ЛПР. Дополнительно проведена структуризация предмета исследования и выполнено дальнейшее развитие иерархической системы показателей (метрик) ИБ, позволяющей, в отличие от применяющейся формальной аттестации или ежегодного фиксированного аудита, формировать и учитывать при принятии решения ЛПР метрики (оценки ИБ) в режиме, близком к РРВ.

Новизна второго научного положения заключается в том, что впервые для планирования и оценки (аудита) ИСМ для СлПО предложен метод «мгновенных аудитов», учитывающий адекватность выполнения применимых требований ИБ «не вообще», а в той мере, которая достаточна для достижения в срок поставленной цели аудита. Известно, что процесс аудита предполагает получение объективных оценок на основании свидетельств аудита, которые могут быть проверены независимыми экспертами. Новый метод с учетом управления «частотностью аудита», объективно, позволяет более оперативно контролировать динамику оценки уровня обеспечения ИБ («динамической перестройки» критериев аудита). Важным преимуществом нового метода является акцентирование именно на получении численных оценок, а не простого «соответствия» или «несоответствия». Предложенный метод позволяет дополнительно исправлять ошибки, присущие сложному процессу аудита, методом локализации обратным процессом, как показано в известной классической работе Н. Винера.

Новизна третьего научного положения заключается в том, что в отличие от публикующихся периодических обзоров (содержащих общую статистику), предложен новый метод исследования динамики сертификации по международным стандартам ISO. Представленный метод содержит математический аппарат, позволяющий оценивать зависимости степени развития разных организаций (например, по кодам отраслей EAC) от динамики сертификации ISO. Реализован корреляционный анализ для оценки динамики рассмотренных зависимостей, так как не все отрасли подтверждают равные тенденции (динамику сертификации). Дополнительно определяется коэффициент зависимости (корреляции) относительных величин – для определенных отраслей, ранжированных по новой введенной метрике «***лидер***». В частности, впервые оценки СМИБ, представленные в публичных статистических данных ISO в соответствии с представленным методом, позволяют проследить взаимосвязь с общим «успехом» по конкретной отрасли для «лидеров» разных рангов. Представленный метод универсален, реализует обобщенный подход к оценке и определяет «лидеров» вне каких-либо ограничений – по кодам EAC.

Новизна четвертого научного положения заключается в том, что в отличие от известных процессов выполнения аудита ИСМ для СлПО, предлагается новое решение задачи многошаговой оптимизации процесса обеспечения ИБ на всем интервале ЖЦ СлПО. Представленный новый метод оптимизации предусматривает проведение мониторинга результативности аудита в режиме, близком к РРВ, и оперативного информирования ЛПР в части обеспечения ИБ, в случае выявления такой необходимости, а не только фиксированные ежегодные встречи в рамках выполнения анализа СМИБ (ИСМ). Использование нового метода позволяет оптимизировать ресурсы для выполнения аудита (оценок) уровня обеспечения ИБ по этапам ЖЦ СлПО с учетом происходящих изменений. В частности, учитываются изменения перечня применяемых (рекомендованных) СрЗИ, предпочтения ЛПР, появления новых

УБИ в отношении защищаемых активов СлПО, а также новые законодательные и/или отраслевые нормативные требования.

Теоретическая значимость диссертационного исследования состоит в обосновании возможности применения новых методов обеспечения ИБ на основании независимой оценки (аудита) ИБ в СлПО, созданных в соответствии с требованиями современных риск-ориентированных стандартов; определении новых критериев выбора множества требований, оптимальных для конкретного СлПО; определении новых условий формирования оптимального множества критериев оценки (метрик) ИБ и развитии научного аппарата независимой оценки (аудита) СМИБ как отдельно, так и в составе ИСМ для СлПО.

Теоретическое значение имеют следующие научные результаты.

Первое научное положение позволяет расширить границы применимости теории обеспечения ИБ для СлПО, отличительными свойствами которой являются:

1. Непредсказуемость последующих состояний и наличие иерархической структуры, усложняющей создание точных адекватных универсальных моделей;
2. Постоянное изменение требований: юридических, технологических, регуляционных и пр., приводящих к появлению возмущений в существующих каналах управления;
3. Крайне малое время реакции на возмущения, требующее создания новых моделей, позволяющих ЛПР принимать «разумные решения» в режиме, близком к РРВ.

Второе научное положение позволяет реализовать в методе «мгновенных аудитов» ИСМ для СлПО важные методические аспекты:

1. Раздельные интерфейсы для внешних и внутренних заинтересованных сторон (*stakeholders*), реализующие предоставление информации с заданной частотностью;

2. Включение контуров гибкой ОС по всем типам аудита позволяет повысить уровень обеспечения ИБ и оперативно агрегировать всю необходимую информацию для ЛПР;
3. Вовлечение в принятие «разумных решений» ЛПР, которое может являться и коллегиальным органом управления, в том числе, с участием внешних заинтересованных сторон.

Третье научное положение позволяет обеспечить в методе исследования динамики сертификации по стандартам ISO необходимую информацию для поддержки принятия «разумных решений» ЛПР при обеспечении безопасности СлПО благодаря:

1. Формированию на основании публичной достоверной статистики ISO оценок приемлемости выбора: по составу СМ, по необходимости внешней оценки (аудита) для функции обеспечения стабильного роста, безопасности и устойчивости бизнес-процессов, защиты ценных активов (в том числе, нематериальных, *goodwill*);
2. Определению коэффициентов зависимости (корреляции) для отраслей «лидеров» по рангам, рассчитываемых для произвольного количества отраслей промышленности.

Четвертое научное положение включает систему методов многошаговой оптимизации аудита ИБ (как в составе СМИБ, так и для ИСМ) и позволяет реализовать гибкий подход к выполнению аудита ИБ в зависимости от фазы ЖЦ для СлПО.

Выдвинутые теоретические положения подтверждены практикой в процессе выполнения диссертационного исследования и открывают новые перспективы для работ в области управления ИБ, в частности, аудита ИБ.

Практическая ценность полученных результатов состоит в улучшении методов оценки (аудита) ИБ для СлПО, основанных на применении оптимального множества риск-ориентированных стандартов в составе ИСМ, что обеспечивает эффективное противодействие ДД злоумышленников, достижение требуемого уровня ИБ, минимизацию потерь при возникновении ситуаций риска

ИБ, присущих СлПО, а также повышение степени соответствия законодательным требованиям (*compliance*). Представленные методы и модели аудита ИБ для СлПО реализованы как функционально завершенный элемент в системе мероприятий комплекса обеспечения ИБ. Результаты диссертационного исследования получили **практическую реализацию** в следующих предметных областях:

1. **Информационные технологии**. В компании ИТСК (РФ) реализован комплекс новых методов аудита ИБ с учетом иерархической системы критериев модели СМИБ (ИСМ).
2. **Воздушный транспорт**. В международных аэропортах Алматы и Астаны (Республика Казахстан) реализован комплекс новых моделей и методов аудита ИБ в составе ИСМ в соответствии с требованиями международных стандартов ISO и дополнительных отраслевых требований IATA (ISAGO).
3. **Системная интеграция**. В группе компаний «Газинформсервис» (РФ) реализован комплекс новых моделей и методов аудита ИБ при создании ИСМ, в том числе, для группы компаний «Газпром нефть».
4. **Образование.** В международной компании AQS (Азербайджан) реализованы новые принципы обучения аудиторов (ведущих аудиторов) ИБ, основанные на разработанных методах проведения аудита ИБ, в том числе, с учетом требований международных стандартов ISO.
5. **Банковское дело**. В Акционерном коммерческом банке «Рускобанк» (РФ) реализован комплекс новых методов проведения аудита ИБ, в том числе, с учетом требований ISO и СТО БР ИББС.
6. **Управление коммунальными объектами критической инфраструктуры.** В ГУП «Водоканал Санкт-Петербурга» (РФ) реализован комплекс новых методов проведения аудита ИБ для СМИБ в составе ИСМ с учетом требований, предъявляемых к СлПО.

Достоверность и обоснованность полученных результатов подтверждается:

- широким обсуждением на всероссийских и международных научных и научно-практических конференциях;
- доказанным положительным эффектом от ряда внедрений результатов представленного диссертационного исследования;
- сопоставление результатов с известными аналогичными исследованиями за длительный период (Reuters, Deloitte, Ernst&Young, McKinsey, PwC);
- сопоставление с публичными данными национальных («Эшелон», Центральный банк РФ, ФСТЭК России, Positive Technology) и международных аналитических обзоров сертификации (ISO);
- корректностью применения апробированного в научной практике исследовательского и аналитического аппарата;
- строгостью математических соотношений, использованных для моделей и методов оценки (аудита) ИБ;
- результатами независимых оценок (аудита) ИСМ в рассматриваемых предметных областях («Русский Регистр», TUV, Lloyd, BSI, DNV);
- публикацией результатов диссертационного исследования в рецензируемых научных изданиях, в т.ч. в **38** изданиях, включенных в список ВАК Российской Федерации и в **15** изданиях, индексируемых Scopus и/или Web of Science.

Основное содержание диссертационной работы и сопутствующие результаты выполненных исследований опубликованы в печати. Научные результаты получены лично автором и непосредственно связаны с его научно-практической деятельностью, в том числе, при выполнении им проектов в области ИБ на территории РФ и стран СНГ.

Апробация и реализация результатов диссертации проводилась в виде докладов на конференциях: на научно-технической конференции «Техногенная энергобезопасность и энергоресурсосбережение», Московский институт энергобезопасности и энергосбережения (2018 г., Москва), на V Международной научно-практической конференции «Управление информационной безопасностью в современном обществе» (2017 г., Москва, ВШЭ), на

конференции «Перспективные направления информационной безопасности» (2017 г., Самара), на международных конференциях «Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь» (DCCN 2015 – 2017, ИПУ РАН, Москва); на международной конференции «Finnish-Russian University Cooperation in Telecommunications» (FRUCT-20), на Научно-техническом совете по инновациям в машиностроительном комплексе Самарской области при Министерстве промышленности и технологий Самарской области (2016 г., Самара), на конференции «БИТ-Поволжье 2016» (2016 г., Самара), на Международной конференции «Менеджмент качества, транспортная и информационная безопасность, информационные технологии» (IT&MQ&IS, 2015 – 2017 гг.), на конференции «Информационная безопасность АСУ ТП КВО» (2016 – 2018 гг., Москва), на Международной научно-практической конференции «Теоретические и прикладные аспекты информационной безопасности» (2016 г., Минск), на Международной научно-практической конференции «Архитектура финансов: антикризисные стратегии в условиях глобальных перемен» (2015 и 2016 гг., Санкт-Петербург), на ежегодной Белорусско-российской научно-технической конференции «Технические средства защиты информации» (2014-2018 гг., Минск); на 13-й международной научной школе «Моделирование и анализ безопасности и риска в сложных системах» (МАБР – 2015, Санкт-Петербург); на Международной конференции «International Conference on Information Security and Protection of Information Technology» (ISPIT 2015, Санкт-Петербург); на III-й Международной научно-практической конференции «Информационная безопасность в свете Стратегии «Казахстан – 2050» (2015 г., Астана); на ежегодных международных научно-практических конференциях «Монолит-Серт» (2010 – 2018 гг.); на международных научно-практических конференциях «Банки. Процессы. Стандарты. Качество» (2010 – 2016 гг., Уфа); на международных конференциях «Информационная безопасность регионов России» (ИБРР 2015 – 2017 гг., Санкт-Петербург); на международных научно-практических конференциях Союзного Государства «Комплексная защита информации» (2011 – 2018 гг.); на

межбанковской конференции «Информационная безопасность банков» (2010, 2011 гг., Магнитогорск); на международной научно-практической конференции «ITSM Forum», (2012 г., Москва); на международной научно-практической конференции «Многогранность оценки бизнеса: проблемы и перспективы в условиях формирования наукоемкой экономики», Казахский Экономический университет им. Т. Рыскулова (2014-2015 гг., Алматы); на конференции «Информационные технологии в управлении» (ИТУ-2014, Санкт-Петербург); на Международной конференции IQNet (2009 г., Санкт-Петербург).

Результаты диссертации реализованы при выполнении ряда крупных проектов, в том числе комплексных аудитов ИСМ на предприятиях нефтегазового и газотранспортного комплекса (РФ, Казахстан), авиационного комплекса и комплекса управления воздушным движением (Казахстан), ИТ (РФ, Казахстан), образовательных учреждений (РФ, Белоруссия, Азербайджан), в кредитных организациях банковской системы (РФ) и пр.

Публикации. Основные результаты диссертационного исследования, впервые содержащие защищаемые научные положения, нашли отражения в **38** статьях, опубликованных в научных журналах и изданиях, рекомендованных ВАК Министерства образования и науки РФ, в **15** изданиях, индексируемых Scopus и/или Web of Science, в **2** рецензируемых учебных пособиях, а также в **12** публикациях в иных рецензируемых научных специализированных изданиях.

Личный вклад автора в основных публикациях с соавторами кратко характеризуется следующим образом: в [338] – [341] представлен гибкий подход к учету рисков ИБ и выполнению аудита ИБ; в [342] – [345] представлен гибкий подход к выполнению аудита ИБ в ИСМ; в [346] предложена концепция «мгновенных аудитов» ИБ; в [89], [98], [347] – [349] предложены метрики ИБ для выполнения аудита в СМИБ (ИСМ); в [82], [83], [118] представлены подходы к выбору активов СлПО и оценке безопасности ИТ; в [85], [86] и [101] – [103] представлена оценка доступности компонентов ТС при выполнении аудита СМИБ (ИСМ); в [97], [107], [108] представлен метод исследования динамики сертификации по международным стандартам ISO; в [115] и [117] представлены

модели аудита ИБ, а также рассмотрены модели для определения результативности как для СМИБ, так и для ИМС.

Структура и объем диссертации. Диссертационная работа включает: введение, **6** глав, заключение, перечень сокращений, перечень терминов и определений, список литературы и приложения. Объем диссертации: **407** страниц, из них список литературы на **29** страницах, **88** рисунков и **70** таблиц.

1 Глава. Обоснование и развитие теоретических и методологических аспектов выполнения аудита информационной безопасности

1.1 Постановка научно-технической проблемы для сложных объектов

В современном высокотехнологичном обществе практически невозможно представить неуправляемые или частично управляемые объекты. В качестве одного из способов управления предлагается применять механизм аудита, который хорошо зарекомендовал себя многолетней практикой применения стандартов ISO ([317], [311], [321], [323], [315]) и отраслевой сертификации (например, ISAGO [325], [326], [327]). Кроме того, уместно отметить, что по данным экспертов на территории РФ размещены свыше 4500 потенциально опасных объектов, для которых вопросы эффективного управления весьма критичны [252].

В специальной литературе отмечены несколько видов аудита, выполняемых для целей обеспечения контроля, измерения рисков и установления степени допустимых рисков. В частности, можно привести два «классических» подхода – основанных на идее оценки «*социального риска*» Фармера (предложенной в 1967 г.) по управлению F/N кривыми (соотношение числа пораженных при каждом сценарии от каждого источника опасности, больше определенного N и частоты событий F) и систем «*общего риска*», представленного в стандартах ISO. В РФ принцип «*социального риска*» реализован в «Методических указаниях по проведению анализа риска опасных производственных объектов»[10], а системы «*общего риска*» реализованы практически в современных риск-ориентированных стандартах ([33], [319]). Рассмотрим примеры управления «социальным риском» (см. рисунок 1.1). Как показано в работах И.Б. Шубинского и А.М. Замышляева (АО «НИИАС») по управлению рисками на железнодорожном транспорте, удобно на практике применять термин «*допустимый уровень риска*», который трактуется в соответствии с принципом ALARP как уровень риска, для которого затраты на его достижение являются экономически эффективными (см. рисунок 1.2).

---

10 http://docs.cntd.ru/document/1200012878

$$R = f(p, C) \quad R = \sum_{i=1}^{n} R_i \quad R = p * C$$

$$Если \quad C = (1 - гибель(смерть), 0 - жизнь), \; то \quad R = p$$

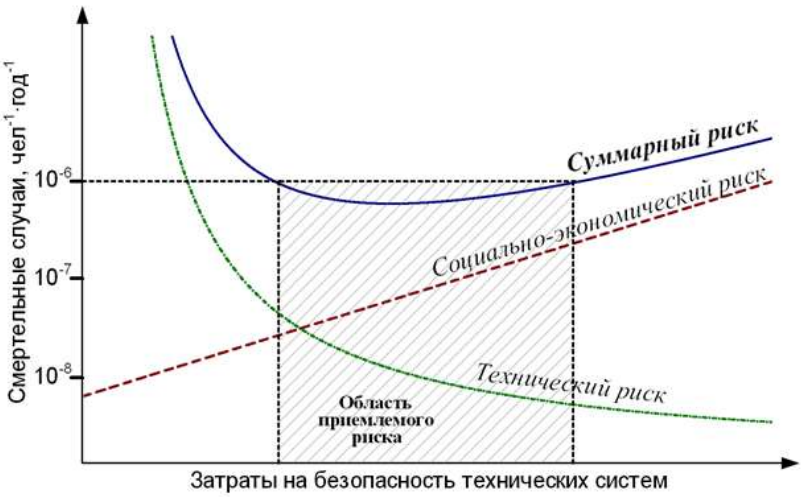


Рисунок 1.1 – Пример управления «социальным риском»

Применительно к кривым F/N Фармера управление риском по принципу ALARP сводится к построению и анализу области ALARP (см. рисунок 1.3).

Рисунок 1.2 – Пример управления риском по принципу ALARP

Отметим также иной подход к обеспечению безопасности при эксплуатации технических систем, который базируется на концепции ALAPA («*As Low As Practicable Achievable*»), т.е. «настолько низко, насколько это практически достижимо». Подразумевается, что должно быть гарантировано внедрение всех мер защиты, которые практически осуществимы.

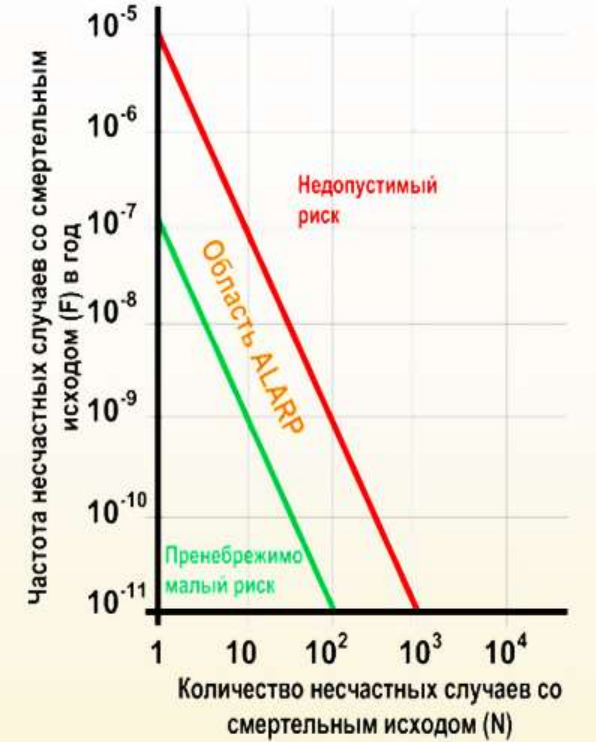


Рисунок 1.3 – Пример управления риском ALARP для кривых F/N Фармера

В определенной степени этот подход увязан с методическими документами ФСТЭК России (например, приказ № 31) [167] и КСИИ ([142] – [145]). Очевидно, что обеспечить гарантированную безаварийную работу сложных производственных объектов и достаточно дорого, и, как показывает отечественная и мировая практика, в настоящее время не представляется в полной мере возможным.

Оценка рисков (по любой приведенной методике) должна позволять формировать адекватную (насколько это возможно) оценку по каждому анализируемому объекту для представления ЛПР. В частности, можно воспользоваться методом, предложенным проф. М. А. Шахраманьяном [252] и определять риск как интеграл удаленности человека от объекта и вероятности поражения человека, например:

$$R = \int_{L=0}^{L=\infty} P(L) \int_{\sigma=0}^{\sigma=2\pi} r\,(\sigma, L) P\,(\sigma)\, d\sigma\, dL \qquad (1.1)$$

где:

r (σ, L) – расстояние от объекта до точки в полярных координатах (σ, L),

P (σ, L) – вероятность поражения человека в точке с координатами (σ, L),

где P (σ, L) определяется как:

$$P(\sigma, L) = \alpha(\sigma)\,\beta(L, \sigma)$$

где:

α (σ) – *вероятность направления ветра в момент аварии*

β (L, σ) – *вероятность поражения в направлении* σ *на удалении L*

Вполне возможно на базе формулы (1.1) предложить формулу оценки рисков, которая будет учитывать совокупность факторов (не только «*социальный риск*»), например – стоимость поврежденных (уничтоженных) активов организации или третьих лиц, если в результате аварии была затронута прилегающая территория. Такой подход может быть применен на базе современных стандартов ([311], [315], [317], [321], [323]). Таким образом, при формировании проблемы обоснования целесообразности аудита сложных объектов возможно принять во внимание собственные функциональные свойства объектов. Например, кривые отказов, которые могут быть описаны вероятностными характеристиками. На рисунке 1.4 а) показан пример реализации функции износа **φ(u),** на рисунке 1.4 б) показан пример плотности распределения сроков службы **F(t)** (с предположением нормального закона распределения вероятности отказов в конце ЖЦ объекта), на рисунке 1.4 в) показан пример вероятности безотказной работы **P(t)** (с предположением роста вероятности отказов в конце ЖЦ объекта).

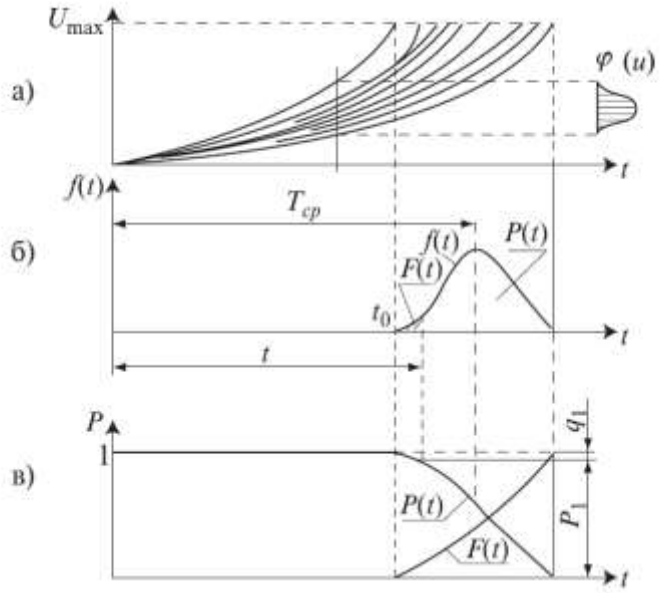


Рисунок 1.4 – Примеры определения вероятности отказов объектов

1.2 Аспекты проведения аудита для оценки влияния человека

В последнее время все более актуальной является проблема оценки влияния человека или более точно – оценка «надежности» человека в цепи управления безопасностью сложных объектов. В ряде источников приводятся цифры, характеризующие негативное влияние ошибок человека на сложные объекты. В частности, указано, что примерно 20–30 % отказов косвенно связаны с ошибками человека, а 10–15 % всех отказов непосредственно связаны с ошибками человека. По мнению академика В. А. Легасова, свыше 60 % аварий происходит из-за ошибок персонала «рисковых» объектов [4].

Отмечается, что при аварии на АЭС «Три-Майл-Айленд» (США, 1979 г.) существенную роль в аварии сыграл импульсный предохранительный клапан (ИПК) на линии от конденсатора давления (КД), который не закрылся после срабатывания. Похожая ситуация сложилась 11.05.1984 на Калининской АЭС, которая, к счастью, не привела к аварии. Возврат на место ИПК КД происходит далеко не всегда, наблюдались сбои и на других АЭС уже после аварии на «Три-Майл-Айленд» [4]. Однако, это не привело к исправлению положения, или, как говорят аудиторы, не привело к выявлению корневой причины (*root*) системного несоответствия и принятия корректирующих мер.

1.3 Фундаментальные правовые основы обеспечения безопасности сложных объектов

1.3.1 Конституция РФ

Нормой ч. 4 ст. 15 Конституции РФ установлено, что общепризнанные принципы и нормы международного права, а также международные договоры РФ являются составной частью ее правовой системы. В том случае, если международным договором России установлены иные правила, чем предусмотренные законом РФ, то применяются правила международного договора. Соответственно, можно констатировать приоритетность норм международного права[11]. Эта норма позволяет обеспечивать распространение международных нормативных документов в области обеспечения ИБ (в том

[11] http://www.constrf.ru/

числе – выполнения аудита, оценки и обработки рисков, реализации мер и средств обеспечения ИБ и пр.) в соответствии с требованиями гармонизированных стандартов в РФ. Однако, как показано в статье «Стандарт в роли правового памятника» (Журнал «Стандарты качество»[12], 2018 г.), существует значимая проблема гармонизации стандартов в мире. В частности, по данным проф. В.Белобрагина, уровень гармонизации национальных стандартов в США с международными составляет не более 25%.

1.3.2 Стратегия национальной безопасности РФ

Указ Президента РФ от 31.12.2015 № 683 ввел в действие новую Стратегию национальной безопасности РФ (далее – Стратегия[13]). Обратим внимание, что в Стратегии в п. 6 введено понятие «национальная безопасность», в дефиницию которого включена ИБ. Далее в разделе «Государственная и общественная безопасность» многократно подчеркивается важнейшая задача учета УБИ в части нарушения устойчивости функционирования объектов критической информационной инфраструктуры (КИИ) РФ (п.п. 43, 47 и 49). Отмечается и необходимость совершенствования системы мониторинга и прогнозирования чрезвычайных ситуаций (ЧС) и ликвидации последствий ЧС на потенциально опасных объектах.

В разделе «Экономический рост» отмечается одно из главных направлений – повышение уровня безопасности и обеспечение стабильного функционирования на объектах ТЭК. В разделе «Наука, технологии и образование» отмечаются факторы, негативно влияющие на национальную безопасность, в том числе – в сфере ИТ, и зависимость от поставок иностранных программных и аппаратных компонентов.

Тем не менее, в тексте Стратегии не отражены практически требования к аудитам ИБ – как к инструментам оценки ИБ. В частности, не в полной мере сформированы предпосылки для формирования программ аудита, оценки систем управления (СУ), подготовки предложений для постоянного улучшения и пр.

---

12 http://www.ria-stk.ru/stq/adetail.php?ID=166489

13 http://www.pravo.gov.ru

Следует отметить, что в тексте Стратегии даны точные и полные формулировки для выполнения оценки уровня безопасности (см. п. 62), управления рисками ЧС (см. п.п. 49 и 53). Дополнительно отметим, что в современном обществе недостаточно развита культура риск-менеджмента. В частности, по практике выполненных проектов ([91], [93]) возможно сделать выводы о следующих недостатках современных риск-менеджеров:

1. Недостаточная скорость каналов передачи информации в части ИБ.
2. Фрагментарное представление о рисках в крупных компаниях.
3. Нежелание и страх показать (расследовать) ошибки свои и команды.

1.3.3 Доктрина информационной безопасности РФ

Новая Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации В.В. Путиным 05.12.2016 г., № 646) отражает все современные вызовы, в том числе – в появлении новых рисков ИБ. Новая редакция Доктрины[14] включает несколько разделов. Первый раздел «Общие положения» описывает уровень стратегического планирования, дается ссылка на Стратегию национальной безопасности РФ (см. выше). Наибольшее внимание заслуживает тезис о необходимости организации международного сотрудничества РФ с другими государствами и международными институтами в области обеспечения ИБ. Кроме того, вводится дефиниция «*информационная инфраструктура РФ*», которая не включает, к сожалению, в явном виде КИИ в РФ. Но и в данной редакции это положение существенно развивает нормативную базу ФСТЭК КСИИ ([143] – [145]), сложившуюся еще в 2007 г. Необходимо принять во внимание, что на конференции ФСТЭК «Актуальные вопросы защиты информации» в 2018 г. комплект документов ФСТЭК КСИИ признан устаревшим. На вопрос «*Какова юридическая судьба документов по КСИИ?*» представитель ФСТЭК Д.Шевцов сообщил: «*Забудьте про них. Меняйте КСИИ на КИИ*»[15]. Также определенные изменения ожидаются в порядке аттестации

---

14 https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

15 http://lukatsky.blogspot.ru/2018/02/blog-post_9.html

АСУТП по требованиям безопасности, сертификация не предусмотрена. Отметим, что существует более 30 вариантов термина «аттестация» в российских нормативных документах[16].

Во втором разделе «Национальные интересы в информационной сфере» описывается возрастающая роль информационной сферы и особенно – обеспечение устойчивого развития и бесперебойного функционирования, прежде всего, критической информационной инфраструктуры РФ. Это положение существенно развивает сложившееся положение с гармонизацией риск-ориентированных стандартов (в частности, ISO серии 27001 [315]).

В третьем разделе «Основные информационные угрозы и состояние ИБ РФ» представлены новые вызовы и угрозы национальной безопасности. В том числе, отмечается наращивание возможностей зарубежных стран по использованию информационно-технических воздействий, в том числе – воздействие на КИИ РФ. Далее в этом разделе Доктрины отмечается недостаточный уровень защищенности ИС, что подтверждается негативными примерами возрастания противоправной деятельности, в т.ч. увеличения инцидентов ИБ, преступлений в кредитно-финансовой сфере, а также слабой корреляцией внедрения современных отечественных ИТ-технологий с задачами обеспечения ИБ. Отметим, что в Доктрине приводятся объективные причины сложившейся ситуации, в частности – отсутствие международной системы ИБ, отсутствие института международного права по регулированию кризисных ситуаций (применительно к обеспечению ИБ). Это положение позволяет более активно применять современные стандарты ISO, принятые в РФ в качестве национальных ГОСТ Р (например: [30] – [33]).

В четвертом разделе «Стратегические цели и основные направления обеспечения ИБ РФ» приведены несколько направлений обеспечения ИБ РФ:

— в области национальной обороны;

— в области государственной и общественной безопасности;

— в области защиты информации в организациях.

---

16 «Стандарты и качество», 2018 г., вып. 3 (969) стр. 20

В пятом разделе «Организационные основы обеспечения ИБ РФ» перечислены важные задачи, решение которых позволит повысить уровень обеспечения ИБ, в том числе: организацию прикладных научных исследований в области обеспечения ИБ в РФ. Кроме того, указан состав участников системы ИБ в РФ и отмечается, что это собственники объектов КИИ. Со времени принятия новой Доктрины произошли события, например, выступление Президента РФ Путина В.В. на ПМЭФ-2017[17], в котором были озвучены требования к обеспечению ИБ в РФ как стратегически важные направления.

Следующим примером является уже реальная потребность обеспечения развития ИБ именно как отрасли. В публикации «Независимого военного обозрения»[18] приведен точный пример анализа поставки газотурбинных агрегатов для кораблей проектов 1164 и 22350. Президент РФ Путин В.В. сказал, цитата: «*Выяснилось, что это не только какое-то особое производство, это особая отрасль науки, знаний и производства. В России этого не было».* Отмечается, что РФ чуть не потеряла к 2000 г. важнейшие технологии и производства в области авиа-, ракето- и судостроения, при этом для разработки турбины SGT5-8000H «Сименс» потратил 10 лет.

Аналогичные требования должны предъявляться и для обеспечения национального «цифрового суверенитета» в области ИБ[19]. Это положение также было отдельно подчеркнуто в Послании Президента РФ Путина В.В. в 2018 г., цитата «*Россия должна стать не только ключевым логистическим, транспортным узлом планеты, но и, подчеркну, одним из мировых центров хранения, обработки, передачи и надёжной защиты информационных массивов, так называемых больших данных. Технологическое отставание, зависимость означают снижение безопасности и экономических возможностей страны, а в результате – потерю суверенитета*»[20].

---

17 http://kremlin.ru/events/president/news/54667
18 http://nvo.ng.ru/polemic/2017-07-21/2_957_red.html
19 http://www.ng.ru/economics/2018-02-06/1_7166_import.html
20 http://www.kremlin.ru/events/president/news/56957

1.3.4 Федеральный закон РФ № 187-ФЗ

В РФ 26 июля 2017 г. утвержден 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который направлен на создание государственной системы обнаружения, предупреждения и ликвидации последствий атак на информационные ресурсы страны. В 187-ФЗ (ст. 5) определено, что понимается под информационными ресурсами РФ. В 187-ФЗ (ст. 12) определено, что оценка безопасности КИИ осуществляется федеральным органом исполнительной власти. На SOC-Форуме 2017 представитель 8 Центра ФСБ России И. Качалин выразил надежду, что «*законы, которые будут приняты в ближайшее время, поспособствуют тому, что безопасность станет более динамичным процессом*»[21]. В частности, необходимо выполнить основные требования регулятора (ФСБ):

- Обеспечение подключения к ГосСОПКЕ и установка соответствующих технических решений (решение «Яхонт-374-Голос» от «Норси-Транс»[22]).
- Уведомление об инцидентах на объектах КИИ (решения класса Security-GRC или процедурами по ISO 27035 или ГОСТ Р ИСО 18044).
- Выполнение требований по реагированию на инциденты и атаки.

Отметим, что Указом Президента РФ от 02.03.2018 № 98 внесены соответствующие изменения в перечень сведений, отнесенных к гостайне[23]. Теперь к ней относятся и «*сведения, раскрывающие меры по обеспечению безопасности критической информационной инфраструктуры РФ*» и «*сведения, раскрывающие состояние защищенности критической информационной инфраструктуры РФ от компьютерных атак*»[24].

В практике уже известны проекты защиты СлПО (АСУТП) в соответствии и 187-ФЗ, Приказом ФСТЭК России № 31 и требованиям международного стандарта IEC 62443 (ГОСТ Р МЭК 62443). Например, проект «ДиалогНаука» по созданию СОИБ «Объединенная энергетическая компания»[25].

---

21 https://www.securitylab.ru/news/489846.php
22 http://www.securitylab.ru/news/489073.php?R=1
23 https://www.securitylab.ru/blog/personal/Business_without_danger/343472.php
24 http://publication.pravo.gov.ru/Document/View/0001201803020009
25 http://www.cnews.ru/news/line/2017-12-04_dialognauka_vnedrila_sistemu_ib_v_astu_obedinennoj

1.4 Разработка общей модели объекта

1.4.1 Постановка задачи

В справочнике по эффективности технических систем (ТС) отмечается, что выделение некоторой сущности – «*системы, предназначенной для решения проблемы*», обладающей новыми свойствами (интегративными или эмерджентными) позволяет устранить противоречия [138]. Кроме того, показано, что ТС со слабо предсказуемым поведением относят к сложным, и именно данный тип ТС обладает важным признаком – способностью принимать решения, что особо актуально для области ИТ ([138], стр. 10). Также отмечается, что для достижения поставленной цели следует применять классическое значение операции, точнее, вовлечение средств (систем), непосредственно взаимодействующих с «*активными средствами*». К таким «*активным средствам*» операции относят как ТС, так и ресурсы, в том числе и информационные. Эти средства могут объединяться в системы, образуя новые управляющие контуры обратной связи, в частности – аудит ИБ ([32]). В эту гипотезу хорошо укладывается и предложение включать в состав таких управляющих систем «*распорядительные центры*» (в нотации [138], стр. 12), в частности, персонал, принимающий решения в процессе аудита ТС.

Постановку задачи для выбора ЛПР предпочтений можно сформировать (в нотации ([138]) по-новому, с учетом формальных контрольных процедур, базирующихся на измерениях. Обозначим (в нотации [138]):

- U – множество стратегий ЛПР;
- A – множество значений определенных и неопределенных факторов;
- G – множество исходов операции;
- Y – вектор характеристик исхода $g \in G$ (числовое выражение результата операции);
- H – модель соответствия множеств: $H: U \times A \rightarrow Y (G)$
- W – показатель эффективности;
- Ψ – оператор соответствия «результат – показатель»;
- K – критерий эффективности;

- **Ω** – модель предпочтений ЛПР на элементах множества: D = {U, A, G, Y, W, K},
- **θ'** – общая информация о проблемной ситуации.

Тогда модель проблемной ситуации описывается в нотации [138] как:

$$\langle \mathbf{U, A, H, G, Y, \Psi, W, K, \Omega, \theta'} \rangle \qquad (1.2)$$

Для решения проблемы принятия решения ЛПР требуется определить состав общей информации о проблемной ситуации **(θ'),** как важнейший элемент формирования оперативных и эффективных управленческих решений, основанных на объективных достоверных данных. В качестве ограничений рассматриваются сроки ожидания ЛПР, допустимые затраты, принципиальная возможность реализации всей системы сбора информации о проблемной ситуации и сложности практической реализации ряда компонентов, которые далее будут рассмотрены подробнее.

1.4.2 Оценка общей информации о проблемной ситуации

Современный этап развития теории управления включает в себя не только моделирование физических аспектов функционирования систем обеспечения ИБ (насколько это необходимо для создания адекватной модели), но и учет экономических факторов. Вторая (экономическая) часть необходима для учета внешних аспектов любой системы (*issues* в терминах стандартов [31], [32]) и разнородной структуры требований. Влияние указанных аспектов позволяет осуществить учет разнородной структуры требований безопасности [32], на базе которых формируется новая информация о проблемной ситуации $\boldsymbol{\theta_N}$. Обладая актуальной $\boldsymbol{\theta_N}$, ЛПР последовательно формирует компоненты (1.2), в частности: подмножества $\mathbf{U_N}$ $\mathbf{(U_N \in U)}$ и $\mathbf{A_N}$ $\mathbf{(A_N \in A).}$ Аналогично выбираются характеристики $\mathbf{Y_N}$ для исходов G_N и устанавливается H_N как $\mathbf{H_N : U_N \times A_N \rightarrow Y_N (G_N).}$ Далее с учетом $\mathbf{Y_N}$ формируется $\mathbf{\Psi_N}$ как $\mathbf{\Psi_N: \{ U_N \times A_N \rightarrow Y_N (G_N) \} \rightarrow W_N}$. Заметим, что аналогичный подход с 2012 г. изложен во всех риск-ориентированных стандартах (в частности [31], [32]), в которых в явном виде требуется определить «контекст» (*context*). На основании

этого базового требования представляется возможным формировать достоверную и объективную информацию о проблемной ситуации **(θ').**

1.4.3 Формирование общей модели объекта

Построение обобщенной модели начинается с построения модели объекта управления (в данном конкретном случае объектом управления является СлПО) и затем – формирования начальных условий, которые определяют состояния объекта управления в дискретные моменты времени **(t_1, …, t_k).** Для СМИБ важно, чтобы выбор шага (дискретности) моментов времени был четко увязан с известными ограничениями, связанными с особенностями функционирования СлПО. В работе [138] показано, что модель должна адекватно отображать исследуемые операции с т.з. информационных связей, и рекомендуется рассматривать модель как «кибернетическую систему» (КС). Для данного конкретного применения важно, что КС допускает формальное описание, в рамках которого каждый элемент может менять свое состояние.

В смысле моделирования КС для целей обеспечения ИБ принципиально важно учесть, что в данном конкретном случае рассматриваются именно «*поведенчески неоднозначные системы*» («*нерефлексные*» в нотации [138]). Данное отношение определяется фактом, что КС включает несколько субъектов с несовпадающими интересами и изменения проблемной ситуации могут быть весьма неравномерными. В современной нотации (ISO 27001, в частности), это означает, что ИСМ в общем или СМИБ в частности включает ряд заинтересованных сторон (*stakeholders*), чьи интересы, действительно, резко отличаются [362].

1.4.4 Замысел при формировании модели объекта

Для создания новых моделей ИСМ для обеспечения безопасности объекта и формализации роли аудитов ИБ в процессе поддержания заданных режимов работы и штатного функционирования технических систем, предполагается реализовать следующий замысел. Текущее положение «как есть» управления техническими системами, с учетом ожидания ЛПР достижения требуемых результатов, анализа проблем (причин проблем) представлено на рисунке 1.5.

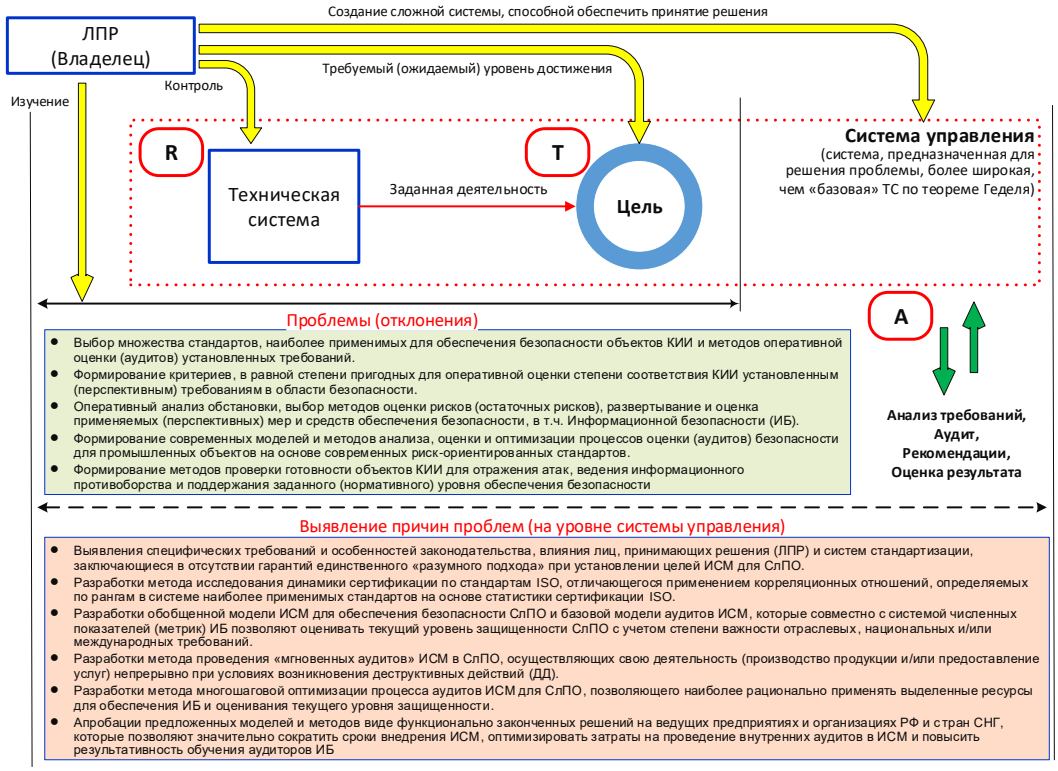


Рисунок 1.5 – Замысел создания новых моделей ИСМ для обеспечения безопасности объекта («как есть»)

Перспективное положение «как нужно» учитывает новые требования к созданию интегрированной системы управления, в том числе, применение механизмов аудита для оценки степени соответствия требованиям применимых стандартов, представлено на рисунке 1.6.

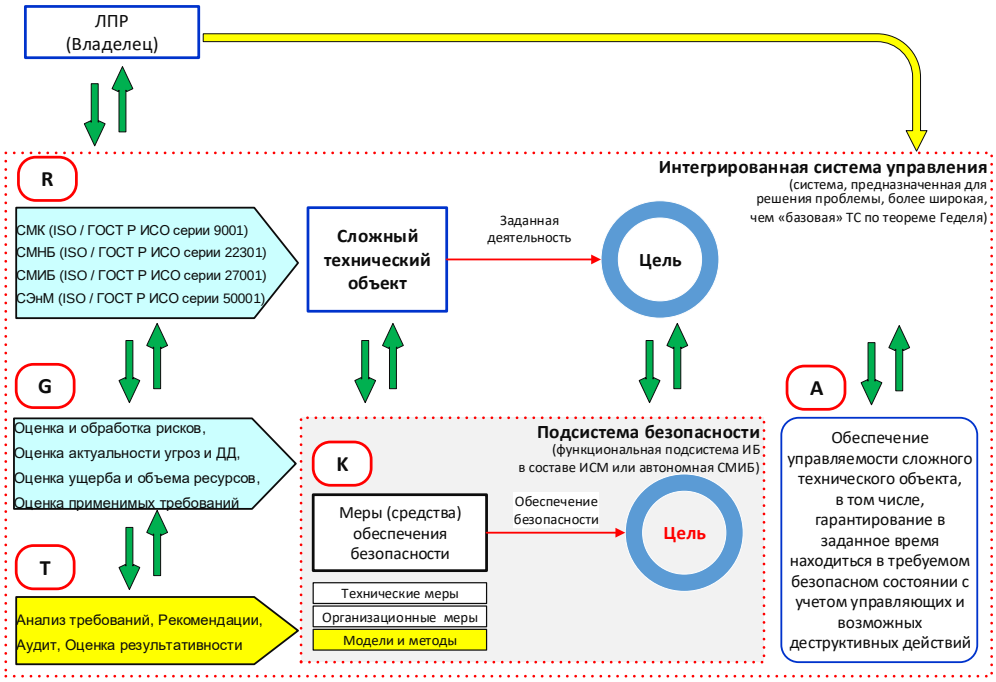


Рисунок 1.6 – Замысел создания новых моделей ИСМ для обеспечения безопасности объекта («как нужно»)

1.4.5 Обобщенная модель объекта

С учетом замысла, рассмотрим обобщенную модель сложной системы, которая включает СлПО (как объект управления) и СУ, реализованную на базе ИСМ для СлПО в терминах [96] (см. рисунок 1.7). Для обеспечения ИБ СУ СлПО (в расширенном толковании термина «ИБ») важно определить размерность пространства состояний модели ИСМ для обеспечения безопасности СлПО (в том числе – внешней среды) для корректного описания аспектов моделирования СлПО и выбора нужной степени детализации модели.

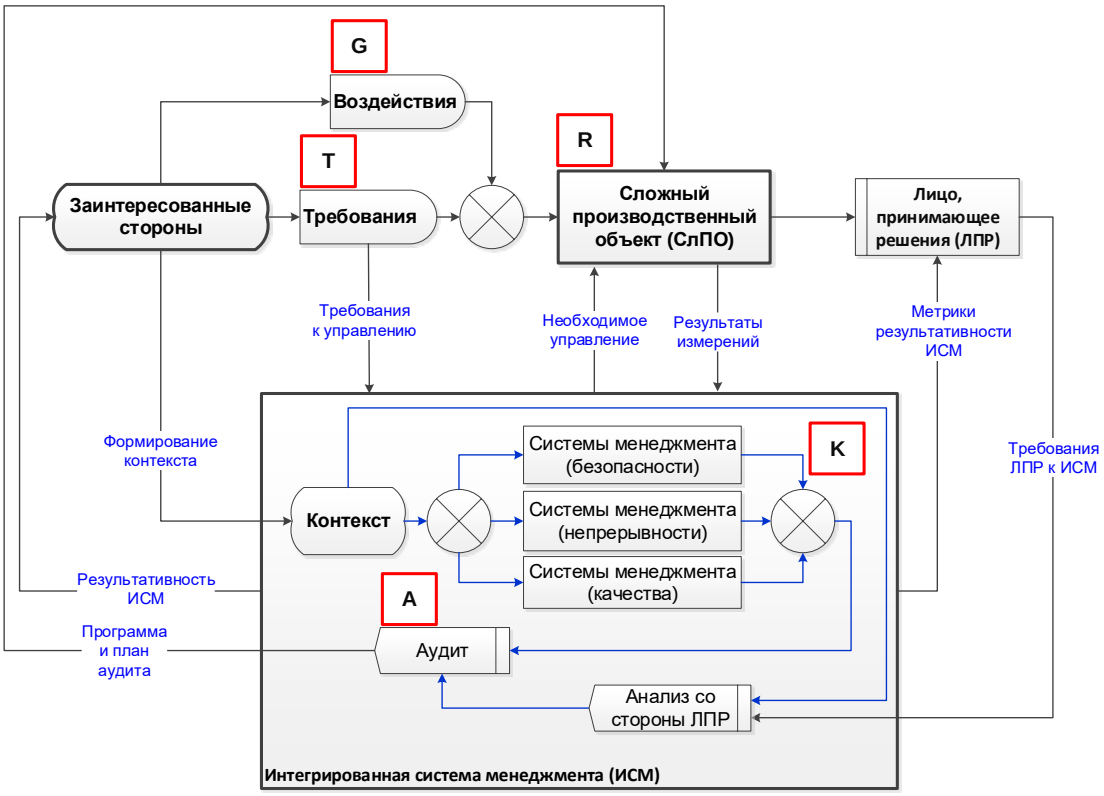


Рисунок 1.7 – Обобщенная модель ИСМ для обеспечения безопасности объекта

Предлагается ввести новые параметры оценки на основе общих принципов ФБ, изложенных, например, в IEC 61508 и IEC 61511:

- границы оценки ФБ;
- уровень полноты безопасности и последствия в случае отказа;
- нормативные требования безопасности.

Отдельно следует принять во внимание при определении различных аспектов моделирования «специализацию» СлПО по отраслям и наличие особых требований (в нотации IEC 61511), например, «мешающий» (ложный) отказ (п.

3.2.65), участие человека как части системы (п. 3.2.84), комплексные (интегральные) испытания (п. 3.2.92). Отметим непосредственное влияние отраслевых аспектов ФБ на частную задачу обеспечения ИБ, например, защиту от несанкционированного доступа (например, к ключам или паролям, п. 11.7.1.3), защиту конфигурации и обеспечение целостности (п. 11.5.5.5), обнаружение отказов (п. 12.7.2.3). С учетом применения риск-ориентированных стандартов в ИСМ важным представляется гарантирование «замыкания» цикла PDCA при управлении ИБ СлПО и формирование контекста для управления СлПО как «открытой системы» в терминах И. Пригожина [150].

1.4.6 Оценка размерностей сложных объектов

В частности, для АСУ ТП могут быть применены следующие оценки размерности[26]. Например, в состав современных АСУ ТП могут входить более 40 типов SCADA систем, более 800 сетевых протоколов и пр. Отметим, что перечень СрЗИ весьма разнообразен в собственной иерархии, например: SOC, SIEM, СрЗИ от НСД, СКЗИ, антивирусное ПО, IDS для SCADA-систем на основе сетей Modbus/TCP, средства проверки и фильтрации сетевых пакетов по их содержимому, средства контроля безопасности, специализированного ПО для тестирования на проникновение (например, PunkSPIDER, Shodan, VPN Hunter, Exploit Search, OpenVAS) и пр.

В 2003 г. представлено «Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства» (далее – «Руководство») [182]. Отметим, что в «Руководстве» приведено важное положение касательно необходимости интеллектуальных сетей. Дополнительные материалы по данному вопросу, подтверждающие тезис о множестве существенных ограничений в муниципальных системах управления водоснабжением и водоотведением представлены в работе Старченко С.В.[27]

---

[26] www.inside-zi, 2016 г., № 2 Петренко С.А. «Практика применения ГОСТ Р 61508 с. 2-9

[27] www.inside-zi, 2016 г., № 2 Старченко С.В., Е.Н. Чемоданов, А.К. Кинебас "Обеспечение защиты информации в Ключевых системах информационной инфраструктуры предприятия" с. 60 - 71.

В работе М. Месаровича, Д. Мако и И. Такахара [127] отмечено, что при решении проблем управления сложными (организационными) системами при условии применения ЭВМ «*неизбежно приходится*» рассматривать вопросы, связанные с совершенствованием СУ. Соответственно, необходимо при изучении таких сложных систем оперировать моделями, структура которых отражает такую сложность ([127], стр. 12). Применение моделей приводит к значительным экономическим преимуществам (например, при повышении непрерывности и доступности систем управления СлПО). Далее в процессе отработки требований заинтересованных сторон (примем во внимание, что это могут быть и злоумышленники [211], [142]) необходимо обеспечить получение результатов измерений, предоставление метрик результативности ИСМ напрямую ЛПР и выдачу адекватных управленческих решений для обеспечения заданного уровня ИБ.

Необходимо принять во внимание, что определенные условия реализации моделей (например – полезность, обеспечение ресурсами, согласование с культурной средой, как показано в [151], стр. 45) учтены в полной мере в представленной выше общей модели ИСМ (см. рисунок 1.7). Также рекомендуется при дальнейшей детализации модели (см. Главу 1 и Главу 2) принять во внимание обязанность аудитора выполнить работу надлежащим образом и предоставить свои выводы (как наилучшую альтернативу, в частном случае) для различных ЛПР (как показано на примере в [151], стр. 78) – для директора, начальника службы охраны и пр. В работе Р. Кини и Х. Райфа отмечается, что метод применения функций полезности более предпочтителен для работы в условиях неопределенности (обязанности ЛПР учитывать риски самой различной природы), чем известные экономические методы «стоимость-эффективность» и /или «затраты-прибыль» ([64], стр. 36). В дополнение данного тезиса обратим внимание, что в работе М. Месаровича, Д. Мако и И. Такахара [127] отмечены примеры управления различными типами СлПО (нефтехимическое производство, сталелитейный завод), для которых

рекомендуется вводить различные временные оценки для соответствующих уровней СУ (от режимов, близких к РРВ до часов и даже суток [127], стр. 25).

Современные направления исследований в области противодействия атакам на СлПО лежат в русле дальнейшего совершенствования СУ рисками, в том числе с учетом современных международных стандартов ([182]). Отметим, что реализация атак возможна и посредством компонентов ИБ, ранее считавшихся надежными, например, токенов двухфакторной аутентификации[28].

1.4.7 Порядок категорирования сложных объектов на примере ТЭК

В ФЗ-256 [247] в ст. 3 определены цели и задачи обеспечения безопасности объектов ТЭК, например: информационное обеспечение безопасности объектов ТЭК. Выделим далее проблему обеспечения ИБ сложных объектов на примере объектов ТЭК. Для изучения проблемы соответствия ФЗ-256 [247] применим следующие требования стандарта ISO 27001 [317]:

— «*высшее руководство должно демонстрировать лидерство*» ([317], п.5.1);
— «*организация должна выполнять планы по достижению целей ИБ, как определено в п. 6.2.*» ([317], п. 8.1);
— «*система менеджмента ИБ организации должна включать документированную информацию*» ([317], 7.5.1);
— «*организация должна предоставить необходимые ресурсы*» ([317], п. 7.1).

В ФЗ-256 [247] в ст. 5 определены требования к категорированию объектов ТЭК: «*Для установления дифференцированных требований обеспечения безопасности объектов ТЭК с учетом степени потенциальной опасности совершения акта незаконного вмешательства и его возможных последствий проводится категорирование объектов*». Для выполнения этой нормы ФЗ-256 [247] применимы следующие требования стандарта ISO серии 27001 [317]:

— «*активам, приведенным в реестре активов, должны быть определены владельцы*» ([317], A.8.1.2);

---

28 https://motherboard.vice.com/en_us/article/8xazek/hackers-show-proof-of-concepts-to-beat-hardware-based-2fa

— «*правила допустимого использования информации и активов, связанных с информацией и средствами для обработки информации, должны быть определены, документированы и внедрены*» ([317], A.8.1.3);

— «*изменения в организации, средствах и системах обработки информации, влияющих на ИБ, должны контролироваться*» ([317], A.12.1.2);

— «*использование ресурсов должно быть контролируемым*» ([317], A.12.1.3).

1.4.8 Требования по обеспечению безопасности ИС на примере ТЭК

В ФЗ-256 [247] в ст. 11 определены требования по обеспечению безопасности ИС объектов ТЭК. Для выполнения этой нормы ФЗ-256 [247] сопоставим следующие требования стандарта ISO серии 27001 [317]:

— «*организация должна определить и внедрить процесс оценки рисков ИБ*» ([317], п. 6.1.2);

— «*организация должна определить и внедрить процесс обработки рисков ИБ*» ([317], п. 6.1.3);

— «*организация должна проводить внутренние аудиты ИБ через запланированные промежутки времени*» ([317], п. 9.2).

1.5 Примеры воздействия на объекты критичной инфраструктуры

За последние несколько лет в мире произошло несколько техногенных катастроф, которые с определенным основанием исследователи относят к результатам вредоносных программных воздействий (ВПВ). В частности, авария летом 1982 г. на отрезке газопровода Уренгой-Сургут-Челябинск [15], авария в 2005 г. на гидроэлектростанции Taum Sauk, в результате которой за 12 минут произошел выброс 4 млн. куб. метров воды [16]. Также известны несколько операций («Лунный лабиринт», «Титановый дождь», «Аврора», «Suter»), имеющих отношение к вредоносным программным воздействиям (ВПВ) [211]. Некоторые подробности приводятся в книгах (например, бывший секретарь Министерства обороны США и советник Р. Рейгана Томас Рид опубликовал книгу «At the Abyss: An Insider’s History of the Cold War»). В работе И.Ю. Жукова «Вопросы управления комплексами программно-технических средств, обеспечивающих безопасность функционирования АСУ ТП» (АО «Концерн

Радиоэлектронные технологии») приводятся следующие известные примеры успешных атак:

- В 2014 г. атака на металлургический завод в Германии[29];
- 12.12.2014 Компьютерный сбой в центре управления воздушным движением в Сванвике[30];
- 17.01.2013 Вирусная атака на электростанцию в США[31];
- 15.08.2012 Хакерская атака на компьютерную сеть Saudi Aramco;
- 10.11.2011 Атака на SCADA-систему компании, обеспечивающей водоснабжение штата Иллинойс в США;
- 10.06.2010 Атака вируса Stuxnet на Иранскую станцию в Натанзе по обогащению урана, разрушившая ее инфраструктуру;
- В 2008 г. польский инженер при использовании пульта управления телевизором спровоцировал сход с рельсов поезда[32].
- В 2000 г. австралийский инженер спровоцировал через систему SCADA разлив 800 тыс. литров сточных вод в отеле Hyatt Regency[33].
- В 1997 г. тинейджер из Массачусетса «уронил» аэропорт Вустер посредством вывода из строя основного и запасного радиопередатчика[34].
- 20.03.1995 Газовая атака в Токийском метрополитене.

В 2018 г. США четыре компании, занимающиеся обслуживанием газопроводов, стали жертвами кибератаки на свои электронные системы для обмена данными с клиентами (EDI)[35]. Об этом сообщило информагентство Bloomberg. Кибератака была нацелена на подразделение Latitude Technologies компании Energy Services Group, предоставляющей технологические услуги EDI более чем 100 газотранспортным компаниям по всему миру[36].

---

29 http://blogs.wsj.com/cio/2014/12/18/cyberattack-on-german-iron-plant-causes-widespread-damage-report/
30 http://dailynewslight.ru/?u=121220142659
31 http://www.securitylab.ru/analytics/487977.php
32 https://www.wired.com/2008/01/polish-teen-hac/
33 http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf
34 http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html
35 https://www.securitylab.ru/news/492454.php
36 http://latitudestatus.com

В «Руководстве» ([182]) приведены примеры успешных атак на объекты СлПО по всему миру. В феврале 2011 г. китайские хакеры атаковали ИС нефтяных и газовых компаний, похитив конфиденциальные данные[37]. Эти атаки были направлены на компьютеры нефтяных и газовых компаний в США. В августе 2012 г. более 30.000 компьютеров, принадлежащих нефтяной компании Saudi Aramco, были парализованы и выведены из строя вредоносной программой "Shamoon". Тот же вирус был использован против ИС катарской компании RasGas[38]. В ноябре 2012 г. была осуществлена DDoS-атака на веб-сайты компании 50Hertz[39]. Также известно о серьезном инциденте 12.05.2017 на автозаводе Dacia, которая привела к сбою ряда ИС на предприятии и часть процессов были остановлены[40]. Аналогичный инцидент произошел в июне 2017 г. на заводе автоконцерна Honda Motor Co в городе Саяма в Японии[41]. Работу завода остановили из-за атаки вируса, похожего на WannaCry.

Необходимо принять во внимание, что мощность DDoS-атак постоянно возрастает. Например, согласно опубликованному отчету экспертов WISR в 2015 г. рекордной стала атака мощностью 500 Гбит/сек[42], а в 2018 г. мощность атак превысила уже 1,6 Тбит/сек[43]. Кроме того, анализ переписки на подпольных форумах позволяет сделать предположение, что в преступном киберсообществе принято использовать сайты ИБ-компаний в качестве испытательных целей, для тестирования новых методов и инструментов. Если существующая статистика по DDoS-атакам в мире показывает срез ситуации на настоящее время, атаки на ИБ-компании позволяют оценить будущее DDoS[44]. Очевидно, что повышение компьютерной интеграции упрощает эксплуатацию инфраструктуры СлПО, но приводит к росту целевых кибератак.

---

37 http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf
38 http://securityaffairs.co/wordpress/8332/malware/rasgas-new-cyber-attack-against-an-energy-company.html
39 http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541
40 http://tass.ru/ekonomika/4249459
41 http://www.rbc.ru/rbcfreenews/594a11b59a79475204ef01f4
42 http://www.infosecurity-magazine.com/news/ddos-attacks-hit-record-500-gbps/
43 https://www.securitylab.ru/news/491821.php
44 https://securelist.ru/analysis/malware-quarterly/28429/ddos-ataki-v-pervom-kvartale-2016-goda/

1.6 Структура и информационные процессы объекта управления

1.6.1 Определение целей управления для сложных объектов

Для обеспечения функционирования сложных объектов применяются различные современные СУ (как показано выше на рисунке 1.4), в состав которых также входят СМ, соответствующие международным стандартам (ISAGO, ISO, IEC). Обеспечение комплексной безопасности (в т.ч. процессов ИБ) для сложных объектов предлагается выполнять на основе полученных оценок (метрик) в единой ИСМ ([88], [90], [96]). Цели управления сложными объектами, таким образом, должны включать на любом уровне иерархической СУ и цели ИБ так, как это принято в практике ИСМ.

Для решения проблемы обеспечения комплексной безопасности сложных объектов необходимо получение оценок уровня обеспечения безопасности (текущих и, в том числе, в режиме, близком к РРВ и/или прогнозов). Для этого необходимо оперировать численными оценками (метриками) ИБ. Соответственно, для указанных целей необходимо, во-первых, проектировать ИСМ на базе современных риск-ориентированных стандартов, во-вторых, сформировать требования к процессам СлПО в четких измеримых метриках и, в-третьих – обеспечить комплексный аудит сложных объектов (в терминах стандартов 19011 и 17021 [20], [21]). В качестве основного направления решения данной проблемы предлагается реализация в составе ИСМ наряду с «целевым» стандартом ISO/IEC 27001 [317] дополнительно стандарт по измерениям ISO/IEC 27004 [318]. В стандарте предложены определения терминов: «мера» (*measure*) и «измерение» (*measurement*), соответственно, п.п. 3.9 и 3.10 ([318]). Приведем примеры объектов измерений в различных СМ:

— результативность реализованных мер и средств контроля ИБ;

— состояние активов, защищенных мерами и средствами контроля ИБ;

— степень удовлетворения заинтересованных сторон.

Для целей обеспечения комплексной безопасности сложных объектов могут использоваться различные источники данных, например:

— результаты анализа и оценки риска;

— отчеты о внутренних и / или внешних аудитах;

— результаты тестирования функциональных подсистем.

Таким образом, формирование модели ИСМ для проведения аудита ИБ для сложных объектов позволит достигать цели измерения и получения оценок уровня обеспечения безопасности (текущих и/или прогнозов). Численная оценка результативности по модели ИСМ соответствует численной оценке уровня обеспечения безопасности (практические примеры будут представлены далее в Главе 4 и Главе 6).

В работе М. Месаровича, Д. Мако и И. Такахара [127] отмечены два важных понятия, актуальность которых со временем только возрастает: «*управление в большом*» и «*управление в малом*». Подразумевается, что «*управление в большом*» затрагивает координацию (управление) в части установления операционных правил в организации ([127], стр. 41). Для рассмотрения предложенных моделей применительно к ИБ это может означать формирование предпочтений для выбора функций оценки эффективности ИСМ (СМИБ). Если говорить более точно, эти функции должны позволять контролировать эффективность процессов ИБ в общей структуре ИСМ (СМИБ). Наилучшей функцией для этой цели экспертами в мире объективно считается функция аудита. В свою очередь, «*управление в малом*» подразумевает координацию (управление) в части практического обеспечения установленного порядка выполнения операционных правил в организации ([127], стр. 41). В ряде случаев эксперты могут предложить конкретные значения для оценки такого порядка, в данном случае – метрик ИБ. Если говорить более точно, при реализации функций аудита ИБ для ИСМ (СМИБ) для высшего руководства (ЛПР) должны быть предложены конкретные числовые метрики для обеспечения управления ИБ.

1.6.2 Формирование критериев для выполнения аудита ИБ

В последние несколько лет на научно-практических конференциях и в различных изданиях предлагаются новые подходы для определения правил выполнения аудита ИБ. Однако, как правило, не рассматривается одна из центральных проблем – формирование подхода к определению критериев для

выполнения аудита ИБ сложных объектов. Например, в обзоре Ю. Тимофеева о деятельности ИСО/МЭК СТК1/ПК27[45] даны ссылки на международные стандарты ISO серии 27001. Следует признать, что это предложение соответствует общему направлению гармонизации международных стандартов и, возможно, будет способствовать повышению качества аудита ИБ для сложных объектов. В докладе А.И. Костогрызова[46] «Научно-методические основы для прогнозирования рисков, обоснования уровней допустимых рисков и обеспечения комплексной безопасности критически важных объектов» также упомянут широкий спектр современных стандартов ISO серий 15288, 27000, 20000, 31000. В докладе Г.Г. Петросюка и С.А. Козленка[47] «Обеспечение ИБ объектов ТЭК» рассмотрены вопросы применения международных стандартов ИСО и отмечаются юридически необязательные рекомендации ФСТЭК по КСИИ [142] – [145], и приказа ФСТЭК России № 31 [167].

1.6.3 Дополнительные требования по специфике объекта аудита

Для проведения аудита сложных объектов могут быть дополнительно рассмотрены в качестве критериев национальные стандарты в области интегрированных систем безопасности – ГОСТ Р серии 52551, 52447, 53893 и 53704 ([47], [48], [49], [50]). ГОСТ Р 52551 [47] вводит дополнительно следующие полезные термины: «*объект защищаемый», «значимость защищаемого объекта»* и важнейший термин: *«оценка соответствия системы безопасности защищаемого объекта»*. Таким образом, обобщенное понятие «оценки соответствия» точно применимо для аудита сложных объектов, и схоже по своему функциональному назначению с любой стандартизированной проверкой соответствия, например, ISO 19011 или ISO 17021 ([20], [21]).

Дополнительно рассмотрим ГОСТ Р 53704 [50], в котором также приводятся требования подтверждения соответствия системы безопасности защищаемого объекта и введен важный термин для обеспечения безопасности сложных

---

45 http://www.ибкво.рф/wp-content/uploads/2015/02/7_Timofeev.pdf
46 http://www.ибкво.рф/wp-content/uploads/2015/02/8_Kostogryzov-A.I..pdf
47 http://www.ибкво.рф/wp-content/uploads/2015/02/23_Petrosyuk-Kozlenok..pdf

объектов – «*латентность*» (подробнее будет рассмотрено в Главе 2). Также в приложении Б [50] указано, что должны быть установлены:

— факторы латентности объекта;

— характер, стоимость и латентные свойства защищаемых ценностей;

— факторы, определяющие экономическую ответственность объекта.

Данные положения коррелируют с требованиями как стандартов ISO серии 27000, так и нормативных документов ФСТЭК России [142] – [145] в части, касающейся безопасности СлПО, обеспечивая методическую базу для эффективной защиты ценных для бизнеса (критически важных) активов. Отметим, что применительно к отраслям (ТЭК или АК), данные требования должны учитываться при создании ИСМ ([105], [96], [258], [256], [147]).

Вопросы ответственности объекта СлПО очень важны, и актуальная позиция ФСТЭК была представлена на конференции в 2018 г. В частности, рассматривался вопрос, насколько эффективно работает механизм оперативного исправления критически важных ошибок в сертифицированном ПО в РФ. Массовое заражение WannaCry произошло потому, что не были установлены выпущенные Microsoft патчи для ведомственных сетей. Отвечая на данный вопрос, представитель ФСТЭК В.Лютиков возложил ответственность за подобную ситуацию на пользователей[48]. Позиция регулятора такова, что существующие правила поддержки сертифицированного ПО в случаях критически опасных ошибок допускают параллельное проведение фактического обновления и проверки патчей в ФСТЭК. Скорость проверки ФСТЭК и сертификацию выпущенных вендором патчей не регулируется.

1.6.4 Область аудита для сложных объектов

Для формирования области аудита любого типа (первой, второй или третьей стороной) сложных объектов необходимо принять во внимание множество факторов, которые специфицированы в стандартах ISO серии 19011 [20], 17021 [21] и ISO серии 27004 [315]. В ряде отраслей для крупных сложных объектов бывает затруднительно разделить такие понятия, как границы (физические),

[48] https://www.itweek.ru/security/article/detail.php?ID=195710

места оказания услуг, центры управления, размещения серверов и ИТ-инфраструктуры. Соответственно, для сложных и пространственно распределенных объектов возможны проблемы с определением комплексных трансграничных рисков. Например, для международной платежной системы (МПлС) MasterCard в 2014 г. серьезно обсуждались риски прекращения деятельности в РФ. Глава MasterCard в России Илья Рябый пояснил в интервью, что «*нельзя вообще вести речь о существовании границ при обработке транзакций*», а также «*никаких физических границ при обработке транзакций не существует. Когда клиент российского банка снимает зарплату в банкомате этого банка, транзакция пролетает через сервера в Сингапуре, Японии, США или другой страны*»[49].

Со временем, как показала практика, эти риски только усилились, например, уже в 2018 г. Oracle предупредила российских партнеров о соблюдении новых санкционных требований США, направленных на заказчиков нефтегазового сектора, в том числе «Газпром», «Роснефть», ЛУКОЙЛ и «Сургутнефтегаз»[50]. Таким образом, при определении области аудита требуется учитывать множество самых важных аспектов, поскольку источники рисков прерывания нормального функционирования сложных объектов могут находиться практически везде и их долгосрочное влияние оценить крайне сложно.

1.6.5 Существующие методы аудита сложных объектов

Метод на основе национального ГОСТ Р 53893

Для целей совместного управления нескольких СМ в составе единой ИСМ разработан национальный стандарт ГОСТ Р 53893, который учитывает рекомендации PAS 99 [46]. Данный стандарт также поддерживает цикл PDCA и должен использоваться вместе со стандартами ГОСТ Р серии 9001, 20000, 27001. Рассматриваемый стандарт ГОСТ Р 53893 уделяет достаточное внимание рискам, что следует признать удачной новацией в РФ по сравнению с риск-ориентированными стандартами ISO на базе Annex SL, появившихся только

---

49 http://www.rfinance.ru/society/interviu/?id=16210

50 https://www.kommersant.ru/doc/3541874

после 2012 г. Понятие риска подробно рассмотрено в приложении А.3 (приложение справочное), оценка степени рисков подробно рассмотрена в приложении А.4 (приложение справочное). Применимость данного стандарта для управления аудитом в ИСМ рассматривается в разделе 4.5.3. и дополнительно – в «Приложении В» дается пример совместного управления для стандартов серии 20000 ([311] – [313]) и 27001 ([316] – [319]).

В ГОСТ Р 51901 рассматриваются вопросы анализа риска технологических систем [46] и приводятся ссылки на международные стандарты IEC (МЭК) серии 60812, 61025 и 61078. В приложении А описываются методы анализа риска (например, FMEA, HAZOP и пр.). Важным преимуществом данного стандарта является требование выполнения аудита процесса анализа риска (раздел 5). При этом установлено, что аудит должен проводиться лицами, непосредственно не привлеченными к участию в выполнении конкретного процесса. Это требование аналогично требованиям о непредвзятости аудиторов в соответствии с требованиями стандартов ISO 19011 и 17021 ([20], [21]).

В работе[51] показано, что согласно ГОСТ Р МЭК 61508–2012, под ФБ понимается «*способность программно-аппаратной системы, связанной с безопасностью, выполнять все предусмотренные в системе функции безопасности с сохранением остаточного риска возникновения опасных событий на допустимом уровне*». ГОСТ Р МЭК 61508-2012 устанавливает 4 интегральных уровня безопасности (Safety Integrity Level, SIL) от минимального SIL1 до максимального SIL4 (см. рисунок 1.8). Для каждого из указанных уровней безопасности определены соответствующие значения показателей PFD (*Probability of Failure on Demand* – средняя вероятность отказа на запрос выполнения ФБ).

Отметим, что при разработке систем безопасности наряду с требованиями ГОСТ Р МЭК 61508-2012, применяются требования и других известных стандартов (например, МЭК 61496 и МЭК 62061). Подобные оценки широко встречаются в обзорах и аналитических отчетах для разных отраслей.

---

[51] www.inside-zi.ru, № 2, 2016 г. Петренко С.А. «Практика применения ГОСТ Р МЭК 61508» С. 2 - 9

ISO EN 13849-1	IEC 62061	IEC 61805 ГОСТ Р МЭК 61508	IEC 62061
PL (*performance level*) Уровень производительности	***PFHd*** (*probability of failure per hour, dangerous*) Вероятность опасного сбоя в течение часа	***SIL*** (safety integrity level) Уровень безопасности	***SIL CL*** (safety integrity level, claim level) Уровень безопасности, заявленный уровень
a	10^{-5}–10^{-4}	–	–
b	3×10^{-6}–10^{-5}	1	1
c	10^{-6}–3×10^{-6}	2	2
d	10^{-7}–10^{-6}	3	3
e	10^{-7}–10^{-8} и более	4	4

Рисунок 1.8 – Сопоставление уровней безопасности SIL

В отчете «Satellite-derived Time and Position: A Study of Critical Dependencies»[52] приведены требования к точности и даны оценки риска для энергетического сектора (см. рисунок 1.9), к которому отнесены добыча нефти и газа.

Рисунок 1.9 – Требование точности и риска для энергетического сектора

Далее приведены требования к точности и даны оценки сопоставимого риска для авиационного сектора (см. рисунок 1.10), к которому отнесены операторы, производители, регуляторы, провайдеры навигационных сервисов и контроля трафика. Обратим внимание, насколько оценки риска в авиации жестче, чем в иных секторах экономики.

[52] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf

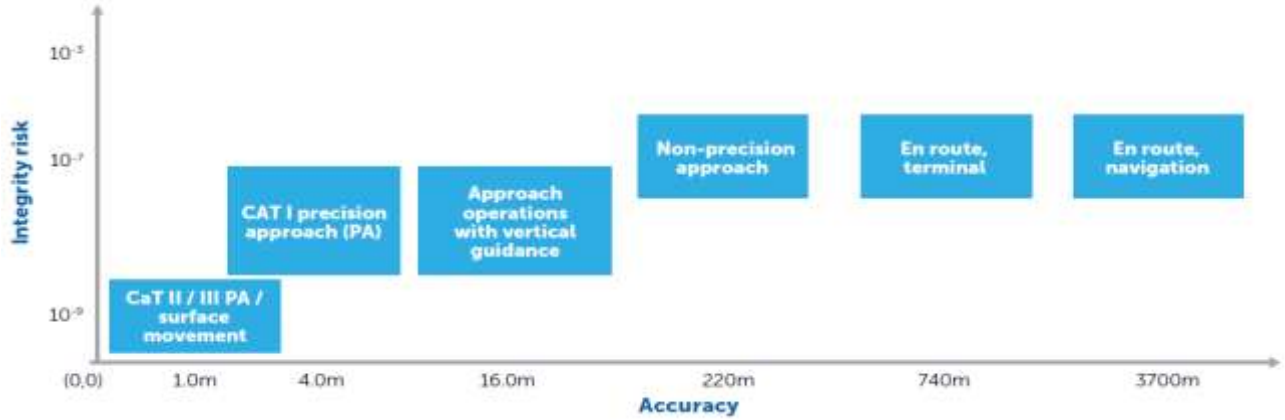


Рисунок 1.10 – Требование точности и риска для авиационного сектора

Метод на основе международного стандарта ISO/IEC 15408

Стандарты ISO/IEC серии 15408 «Общие критерии оценки безопасности ИТ» (широко известные как «Общие критерии») определяют функциональные требования безопасности (*security functional requirements*) и требования к адекватности реализации функций безопасности (*security assurance requirements*) [23], [24], [25]. При проведении работ по анализу защищенности ИС представляется целесообразным использовать «Общие критерии» в качестве основных оценочных критериев, позволяющих оценить уровень защищенности ИС с точки зрения полноты реализованных в ней ФБ и надежности реализации этих функций. Часть 3 «Общих критериев» («Требования доверия к безопасности») содержит оценочные уровни доверия (ОУД) [25]. Минимальный уровень ОУД 1 предусматривает анализ функциональной спецификации, спецификации интерфейсов и эксплуатационной документации, а также независимое тестирование. Максимальный уровень ОУД 7 требует формальную верификацию проекта объекта оценки. Необходимо отметить, что в стандартах ISO/IEC серии 15408 не представлено исчерпывающих конкретных спецификаций для реализации оценки требований:

— организационных мер по защите информации;

— методологии оценки;

— административных и правовых аспектов применения.

Отметим, что действительно высокие уровни ОУД (EAL), начиная с 5 означают, что выполнены проверки всеми возможными математическими

методами. Например, Integrity-178B RTOS[53], система уровня EAL6+ — военная операционная система (использовалась в ВВС для управления автоматикой истребителей, а также в космических «челноках» NASA), первая в мире получившая столь высокий рейтинг[54]. Также отметим микроконтроллер SmarX2, имеющий сертификат Common Criteria EAL6+ для защищенных микроконтроллеров с бесконтактным интерфейсом на базе 90-нм технологии (испытания проводило Федеральное ведомство по информационной безопасности (BSI) Германии)[55]. Отметим, что уровень EAL6 предусматривает доскональное тестирование всей архитектуры безопасности на устойчивость к разнообразным агрессивным, полуагрессивным и неагрессивным атакам, то есть формальную проверку самой концепции обеспечения безопасности. Такие же результаты демонстрирует и компания Samsung[56], которая провела успешно тестирование новой карты T9MF на соответствие Common Criteria Evaluation Assurance Level 6+.

Требования содержат события, потенциально подвергаемые аудиту, и для их отбора разработчиками задания по безопасности при условии включения в требования из класса FAU «Аудит безопасности». Эти требования включают в себя события, относящиеся к безопасности, применительно к различным уровням детализации [24]. Рассмотрим пример сопоставления требований ISO/IEC 15408 для класса безопасности FAU «Аудит безопасности» и некоторых мер (средств) обеспечения ИБ в соответствии с требованиями ISO 27001. Результаты представлены в таблице 1.1.

---

53 https://www.ghs.com/products/safety_critical/integrity-do-178b.html

54 http://www.integrityglobalsecurity.com/

55 http://www.mskit.ru/news20/no129942/

56 http://www.samsung.com/semiconductor/insights/article/25226/new-cc-eal6-level-combi-smart-card

Таблица 1.1 – Сопоставление требований ISO/IEC 15408 и ISO 27001 (выборка)

Семейство		**Мера (средства) обеспечения ИБ**
FAU_ARP	Автоматическая реакция аудита безопасности	A.9.1.2
FAU_ARP	Автоматическая реакция аудита безопасности	A.10.3.1
FAU_ARP	Автоматическая реакция аудита безопасности	A.10.10.2
FAU_GEN	Формирование данных аудита безопасности	A.10.10.1
FAU_GEN	Формирование данных аудита безопасности	A.10.10.5
FAU_SAA	Анализ данных аудита безопасности	A.8.3.3
FAU_SAA	Анализ данных аудита безопасности	A.10.9.3
FAU_SAA	Анализ данных аудита безопасности	A.10.10.3
FAU_SAA	Анализ данных аудита безопасности	A.11.5.2

Метод на основе стандарта NIST 800-53

В США и ряде стран для целей аудита ИБ (в том числе – сложных объектов) используются стандарты NIST, например:

— NIST SP 800-26 Security Self-Assessment Guide for IT Systems

— NIST SP 800-30 Risk Management Guide for IT Systems

— NIST SP 800-53 Recommended Security Controls for Federal IT Systems

В частности, стандарт NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations (Rev.4) разработан в апреле 2013 г. [378]. В данном стандарте рассмотрены меры и средства обеспечения ИБ, сгруппированные в категорию «*Audit and accountability controls*» (шифр AU). Перечень всех «контролей», применяемых для выполнения аудита ИБ приведен в таблице D-5 [378].

Метод на основе стандартов CIP NERC

Североамериканская корпорация по обеспечению надежности электросистем (NERC) разработала стандарты кибербезопасности «Защита важнейших объектов инфраструктуры (CIP) NERC» ([182]). Отдельные стандарты построения комплексной системы кибербезопасности именуются CIP-002 – CIP-009. В CIP также используется подход, основанный на оценке рисков, в соответствии с которым особое внимание уделяется «*важнейшим активам киберпространства*». Перечисленные в таблице 1.2 стандарты

особенно актуальны при обеспечении кибербезопасности на важнейших объектах неядерной энергетической инфраструктуры[57].

Таблица 1.2 – Спецификация стандартов (CIP) NERC (фрагмент)

CIP-002	Выявление важнейших кибератривов
CIP-003	Меры контроля над управлением безопасностью
CIP-004	Персонал и профессиональная подготовка
CIP-005	Электронный периметр безопасности
CIP-006	Физическая безопасность киберсистем
CIP-007	Управление безопасностью систем
CIP-008	Представление информации об инцидентах и планирование ответных мер
CIP-009	Планы восстановления деятельности для киберсистем BES

Отметим, что единый подход в специализированных стандартах (IEC 62433, ISO 27001, NERC CIP и пр.) заключается в том, что все они используются для определения комплекса мер, которые будут применяться независимо от оценки риска. Эта концепция схожа с подходом, лежащим в основе немецкой системы каталогов IT-Grundschutz[58] и предназначена для получения соизмеримых результатов вместо разрозненных отчетов, к которым иногда приводит использование подхода, основанного только на управлении рисками ([182]). Хотя выбор применимых стандартов может зависеть от территориальных ограничений США или Европы, перечень актуальных стандартов (ISO 27001, NIST IR 7638, NERC CIP и IEC 62433) свидетельствует о едином общем подходе, основанном на управлении рисками, применимых к активам (NERC CIP включает предварительный шаг выявления кибератривов).

Метод на основе COBIT

Предложенная IT Governance Institute и ISACA методология CobiT впервые была представлена в 1996 г. Она содержит «лучшие практики» и ссылки на внешние нормативные документы (в том числе ISO – 38500, 31000, 20000, 15504, 9001 и пр.), а также на известные отраслевые руководства – ITIL, TOGAF, CMMI,

---

57 http://www.nerc.net/standardsreports/standardssummary.aspx (02/13/2013)

58 Каталоги IT-Grundschutz, Федеральное управление по информационной безопасности Германии (BSI)

PMBOK и пр. [109]. Ряд экспертов полагает, что CobiT помогает «заполнить разрывы» между бизнесом, рисками, требуемыми мерами контроля и техническими проблемами для ИТ.

Вместе с тем, CobiT не является стандартом и носит больше рекомендательный характер, основываясь, отчасти, на признанных стандартах (например, ISO). В новой версии CobiT5 существенно изменилась собственная процессная модель – она заменена на общеизвестную модель ISO/IEC 15504. Применительно к структуре процессов обеспечения ИБ важно отметить, что выполнено разделение (условное) для процессов управления ИБ:

— управление безопасностью, процесс AP013 (Acquire and Implement);

— управление безопасностью, процесс DSS05 (Deliver and Support).

Рассмотрим пример сопоставления требований Cobit и некоторых мер (средств) обеспечения ИБ в соответствии с требованиями ISO 27001. Результаты представлены в таблице 1.3.

Таблица 1.3 – сопоставление требований Cobit5 и ISO 27001 (выборка)

COBIT 5 для ИБ		**ISO/IEC 27001**	
EDM01	Гарантировать внедрение и поддержку методологии руководства	A.5	Политика в области безопасности
EDM04	Гарантировать оптимизацию ресурсов	A.6	Организация ИБ
APO01	Управлять методологией управления ИТ	A.6	Организация ИБ
APO07	Управлять человеческими ресурсами	A.8	Безопасность человеческих ресурсов
APO08	Управлять взаимоотношениями	A.6.1	Внутренняя организация ИБ
APO10	Управлять поставщиками	A.6.2	Внешние стороны
BAI09	Управлять активами	A.7	Менеджмент активов
DSS04	Управлять непрерывностью	A.14	Менеджмент непрерывности бизнеса
MEA02	Осуществлять мониторинг	A.15.2	Соответствие политикам и стандартам ИБ

Метод на основе международного стандарта ISO/EC серии 20000

Стандарты ISO/IEC серии 20000 были впервые разработаны BSI в Великобритании, «базовый» стандарт назывался BS 15000 и определял требования, предъявляемые Правительством Великобритании к поставляемым ИТ-услугам со стороны внешних организаций. В настоящее время разработаны несколько стандартов ISO/IEC серии 20000, для обеспечения ИБ сложных объектов рассмотрим 3 основные ([311], [312], [313]). Представляется интересным сопоставить некоторые термины из ISO 27001 [317] и [311], в частности, термин «*инцидент ИБ*». Поскольку стандарт [311] определяет требования, важно принять во внимание два существенных аспекта: часть требований предъявляются к системным процессам, а часть – к процессам системы управления ИТ-услугами (СУУ).

Применительно к вопросам ИБ в стандарте [311] выделен отдельный процесс – «*Управление информационной безопасностью*» (раздел 6.6), который определяет основные требования к обеспечению ИБ в организации: выявлению, учету и категорированию активов, а также управлению рисками ИБ (применительно к выявленным значимым активам организации). Не раскрывая все детали реализации требований ИБ, в стандарте [311] дана прямая ссылка на стандарт [317], который является «целевым», как было показано выше, применительно к процессу обеспечения ИБ. Применение процессного подхода в [311], а также в [317], позволяет также использовать методы оценки процессов, поскольку ISO/IEC серии 27000 и 20000 содержат требования постоянного повышения результативности. Для справки – сертификацию по требованиям стандарта [311] в РФ по данным портала[59] прошли всего 29 компаний (данные на 12.03.2018).

Метод на основе библиотеки ITIL

ITIL (IT Infrastructure Library) — библиотека, описывающая лучшие из применяемых на практике способов организации работы ИТ подразделений для

---

59 http://www.realitsm.ru

организаций, занимающихся предоставлением ИТ-услуг. В актуальной версии ITIL v3.1 содержится 5 книг:

- Стратегия услуг (Service Strategy)
- Проектирование услуг (Service Design)
- Преобразование услуг (Service Transition)
- Эксплуатация услуг (Service Operation)
- Постоянное улучшение услуг (Continual Service Improvement)

В книге «Service Operation» приведены ссылки не только на стандарты ISO, но и на отраслевые рекомендации: COBIT, CMMI, eSCM-SP, PRINCE2, ISO серии 9000, 20000 и 27001, которые могут быть применены для учета внешних требований при управлении ИТ-услугами. С другой стороны, в стандарте ISO/IEC [311] или [317] не содержится ссылок на ITIL, т.е. подчеркивается статус стандарта ISO в отличие от ресурса ИТ-отрасли, который содержит «лучшие практики» для реализации определенных требований при управлении предоставляемых ИТ-услуг.

Среди специалистов нет единого мнения о «единственности» и «универсальности» ITIL для обеспечения ИБ как частной задачи. Действительно, в ITIL нет такого отдельного «целевого» процесса как «Управление (обеспечение) ИБ». Несмотря на это, действующая версия стандарта ISO/IEC серии 20000 поддерживает требования в виде отдельного «целевого» процесса ИБ. Однако, на практике не всегда SLA может дать 100% гарантию защиты от критических инцидентов. В частности, в мае 2017 г. «МегаФон» в результате значимого инцидента прекратил предоставлять услуги связи, но юристы полагают, что «обрушение» компонента Hewlett Packard Enterprise позволяет все же рассчитывать на компенсацию[60].

В рекомендациях ITIL также содержатся полезные примеры применения метрик ИБ и общих подходов к обеспечению достаточного уровня ИБ в

---

60 http://www.rbc.ru/technology_and_media/21/05/2017/592185989a79476dca8dc8b4?from=detailed

организации. Например, в книге «Service Design» в разделе 4.6 *Information Security Management* содержатся подробные рекомендации:

— по возможным мерам управления рисками (например, «4Т»);

— по «триггерам ИБ» (*triggers*) для мониторинга и событий ИБ (например, изменение Политики ИБ, изменений в SLA, OLA или контрактах);

— по метрикам ИБ: (например, снижение количества инцидентов ИБ).

В книге «Service Operation» в разделе 5.13 *Information Security Management and Service Operation* также содержатся подробные рекомендации:

— по мерам ИБ (например, порядок проверки персонала провайдера (*Screening*), заключение NDA до начала доступа к информации);

— метрики процессов (например, определение и разрешение инцидентов ИБ, количество инцидентов, связанных с ИБ).

Сравнительные характеристики методов оценки ИБ

Отметим, что стандарты ISO часто получают национальное признание. Например, в работе В. Анищенко[61] приведен удачный пример сопоставления стандартов Белоруссии (СТБ) и их требований (см. рисунок 1.11).

Класс СТБ ISO 15408 (Common Criteria)	СТБ ISO 27001 (средства управления)											
	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	Всего
FAU "Аудит безопасности"				1	1	8	7	3	1		3	24
FCO "Связь"						3		1				4
FCS "Криптографическая поддержка"								1				1
FDP "Защита данных пользователя"			1			13	8	6		1	2	31
FIA "Идентификация и аутентификация"			1	1		3	9					14
FMT "Управление безопасностью"			1	1		11	10	3	2		3	31
FPR "Тайна"												0
FPT "Защита ФВБО"			1		4	14	9	5	1	1		35
FRU "Использование ресурсов"										1		1
FTA "Доступ к ОО"		1		1		1	9				1	13
FTP "Доверенный путь/канал"						5	2	1				8
Итого F		1	4	4	5	58	54	20	4	3	9	162
ASE "Оценка ЗБ"		1				1		2				4
ADV "Разработка"						3		2				5
AGD "Руководящие документы"						2			1		1	4
ALC "Поддержка жизненного цикла"	2	4	2	1	2	7		8			2	28
ATE "Тестирование"		2				1		1	1		2	7
AVA "Оценка уязвимостей"		3				1		2	1	1	2	10
ACO "Составной объект"		3				1		2	1	1	2	10
Итого A	2	13	2	1	2	16		17	4	2	9	68
Всего: F + A	**2**	**14**	**6**	**5**	**7**	**74**	**54**	**37**	**8**	**5**	**18**	**230**

Рисунок 1.11 – Сопоставление требований стандартов СТБ 15408 и 27001

61 http://www.bankit.by/files/2014/presentations/zashhita-informacii/prezentacii/9-40-proektirovanie-i-attestacija-sistem-zashhity-informacii-anishhenko.pdf

1.6.6 Методы аудита ИСМ и сложных систем

Обзор практики в области аудита ИСМ

С помощью методов аудита не только познается объект аудита, но, в ряде случаев, отмечается, как возможно упорядочить процессы его организации. В ряде публикаций отмечается, что, к сожалению, в настоящее время неизвестны факты проведения специальных исследований по вопросам методов аудита, не говоря о методах внутреннего аудита [56]. Известно, что выборочная проверка основывается на законах теории вероятностей, в соответствии с которыми можно получить объективные данные о проверяемой «генеральной совокупности» по ее относительно малой части – «выборке». Согласно требованиям Федерального правила (стандарта) № 16 «Аудиторская выборка», утвержденного Постановлением Правительства РФ от 07.10.02 № 532, все элементы изучаемой совокупности должны иметь равную вероятность быть отобранными в выборку. Такие же требования содержатся в стандарте аудита ГОСТ Р ИСО 19011 [20], [56].

В истории известны примеры количественной оценки в процессе проведения аудита. По данным Геродота на пирамиде Хеопса вырезано, сколько чеснока, редиски, лука и других продуктов было выдано занятым на строительстве пирамиды людям, общая стоимость проекта составила 1500 талантов. Также сохранился отчет, вырезанный на стене Парфенона, согласно которому стоимость строительства составила 469 талантов [216]. Известно, что Петр I внес существенный вклад и в развитие бухгалтерского дела и аудита, особенно с целью обеспечения доказательной силы документа. Приводится факт определения роли документа, который был сформулирован Петром I в письме к А.Меншикову: «*Перед важным делом у господ генералов мнение испрашивай письменно. Дабы при проигрыше баталии не говорили, что советовали инако*» [4]. По данным историков, первая ревизия по правилам, сформулированным лично Петром I, была проведена в 1719 г. [217].

В начале XX века вышла книга Р. Монтгомери «Аудит: теория и практика», которая считается классической, и при последующих переизданиях получила

название «Аудит Монтгомери» [53]. Но американский опыт должен перениматься с определенными допущениями, т.к. предлагаются различные термины, означающие процесс аудита. Например, Американский институт присяжных бухгалтеров и Комитет Американской ассоциации бухгалтеров представляют различные определения аудита [217]. Во второй половине XX века произошло смещение от формального аудита – т.е. проверки документации, подтверждающей записанные денежные операции, и группировку этих операций в финансовых отчетах к внешнему независимому финансовому контролю деятельности экономических субъектов [15]. Появился термин «*системно-ориентированный аудит*» против ранее применявшегося термина «*подтверждающий аудит*».

В последнее время в связи с широким развитием риск-ориентированных стандартов (не только ISO) появился новый термин – «*аудит, ориентированный на риск*». Именно это понятие приводится в двух основных стандартах для аудита – ISO серии 19011 и 17021 [21], [20].

Критерии для выполнения сложного аудита

Для выполнения любого сложного аудита необходимо формировать критерии, что является известной проблемой. Рассмотрим пример: «Стандарт качества организации по управлению бизнес-процессами в КО»[62], который содержит несколько степеней зрелости. В то же время следует отметить, что прямое применение любого типового решения не приводит к появлению «автоматического» соответствия (*compliance*).

Для подтверждения данного тезиса рассмотрим функционал решения RSA Archer GRC по процессу «Управление внутренними аудитами»[63]. Заявлено, что автоматизация данного процесса с использованием систем GRC позволяет осуществлять:

— формирование плана аудита в условиях изменения уровней рисков;

— представление полной картины активов;

---

62 http://www.cbr.ru/publ/moneyandcredit/radchenko_03_11.pdf

63 https://www.rsa.com/en-us/products-services/governance-risk-compliance

— отслеживание загрузки аудиторов.

Для сопоставления моделей зрелости могут быть применены, например, стандарт ISO 15504, методика CMM или отраслевой стандарт АКФОРБ[64]. Детальное описание возможности применения RSA Archer eGRC для соответствия требованиям «Стандарта качества организации работы по управлению бизнес-процессами в кредитных организациях» было представлено на банковском форуме[65].

Критерии интегрированности систем менеджмента в составе ИСМ

Как было показано выше, при переходе от отдельных СМ к ИСМ необходимо принимать во внимание общие требования (PAS-99 [362]) и учитывать уникальность требований иных СМ (например, ISO 27001 [317]). Известно несколько публикаций по данной теме, например: «Формирование критериев оценки ИСМ», Зубкова К.С., Шабанова Е.Н., Малахова Ю.Г.[66], «Подходы и критерии Русского Регистра при оценке степени интеграции системы менеджмента организации»[67], «Оценка результативности интегрированной системы менеджмента», Титова В.А., Колочева В.В.[68]

Для решения проблемы предлагается более простой вариант, который характеризуется определением критериев интегрированности СМ (определяемых, в общем случае, в соответствии со спецификой конкретного стандарта в ИСМ), набора весовых коэффициентов (определяемых, в общем случае матрицей парных сравнений – МПС) и количественной шкалой для определения уровня ИСМ. Представленный метод соответствует, в отличие от рассмотренных выше вариантов, формальным требованиям современных риск-ориентированных стандартов (Annex SL), численным представлениям результатов и объективными средствами математической самопроверки (МПС).

Рассмотрим примеры критериев интегрированности:

1. Единый принцип формирования контекста (внешнего и внутреннего),

---

64 http://akorb.ru/

65 http://npk.akforb.ru/upload/doc/2015/Черников.pptx

66 http://cyberleninka.ru/article/n/formirovanie-kriteriev-proverki-integrirovannoy-sistemy-menedzhmenta

67 http://www.rusregister.ru/upload/medialibrary/8da/Integration_level_Criteria.pdf

68 http://www.ria-stk.ru/stq/adetail.php?ID=10233

2. Единый принцип идентификации требований регуляторов,
3. Единый принцип постановки целей и планирования ресурсов,
4. Единый подход к управлению рисками для всех систем,
5. Единый принцип формирования группы внутренних аудиторов.

Для каждого критерия определяется оценка (в баллах), которая затем оценивается МПС группой экспертов, утвержденной ЛПР. Например, рассмотрим расчет уровня интегрированности ИСМ:

$$R = \frac{1}{k}\sum_{i}^{k}\frac{\lambda_i}{m_i}\ \alpha \qquad (1.3)$$

где:

R – уровень интегрированности;

k – количество критериев интегрированности ИСМ;

m – максимальный балл каждого критерия интегрированности;

λ – текущая оценка каждого критерия интегрированности;

α – весовой коэффициент критерия интегрированности.

Пример количественной шкалы для определения уровня ИСМ по формуле (1.3) представлен в таблице 1.4:

Таблица 1.4 – Уровень интегрированности СМ в составе ИСМ:

№	Уровень	Значение R	Примечание
1.	Начальный	0 < R ≤ 0,2	Не все СМ соответствуют Annex SL
2.	Низкий	0,2 < R ≤ 0,5	
3.	Средний	0,5 < R ≤ 0,8	
4.	Высокий	R > 0, 8	

1.7 Оценивание уровня обеспечения ИБ в ИСМ

1.7.1 Подходы при оценивании уровня обеспечения ИБ в ИСМ

Для оценивания уровня обеспечения ИБ в современных организациях применяются различные подходы. Кратко рассмотрим несколько основных:

— международные стандарты ISO, содержащие требования к ИБ (например, СМИБ), позволяющие выполнять любой аудит (1-й, 2-й и 3-й стороной),

— комплекс СТО БР ИББС, позволяющий КО выполнять самооценку и/или внешнюю оценку по единой количественной методике,

— аттестация по руководящим документам ФСТЭК РФ (общая оценка объектов автоматизации по установленным классам),

— оценки по отраслевым стандартам (PCI DSS), рекомендациям (CobiT5), позволяющим получать оценки по специфическим требованиям.

Очевидно, что для целей формирования объективных (и независимо воспроизводимых) оценок уровня обеспечения ИБ в ИСМ (минимально – СМИБ, а целевая задача – ИСМ), могут быть применены только стандарты ISO, т.к. все прочие методы содержат неформализованные отраслевые требования. Эти специфические требования, в частном конкретном случае, не могут быть оценены (например, требование «*Банковский платежный технологический процесс*» в СТО БР ИББС). Важно обратить внимание, что общие подходы к интеграции для рассмотренных СМ могут быть дополнительно взяты из специализированного стандарта ISO/IEC 27013:2012 [320].

1.7.2 Требования к модели оценивания защищённости ИСМ

К модели СМИБ, пригодной для оценивания защищённости ИСМ, как показывает статистика выполненных аудитов, целесообразно предъявлять следующие требования (см. [96], [102], [103], [106]):

— Соответствия области сертификации (*Scope*) ИСМ;

— Соответствия требованиям к точности;

— Соответствия требованиям к адекватности модели;

— Соответствия целям ИСМ.

1.7.3 Проблема «интегрального соответствия»

При создании ИСМ, состоящих минимально из 2-х и более СМ (например, СМИБ, СМК и СУУ, как определено в PAS-99 [362]), во внимание принимается широкий спектр требований, важнейшими из которых являются требования непрерывности и устойчивости бизнес-процессов организации ([119] – [121]). Известно, что при создании современных ИСМ, помимо проблем кооперации требований различных стандартов ISO серии 9000, ISO/IEC серии 27000 и серии 20000, необходимо обеспечить «*интегральное соответствие*» требованиям бизнеса – прежде всего экономической эффективности по целевой функции

достижения прибыли и минимизации издержек [114], [116]. Также важна и не менее значима вложенная задача – формальное соответствие (*compliance*) законодательным требованиям различных регуляторов (например, ФЗ-63 «Об электронной подписи» [236], ФЗ-152 «О персональных данных» [240], ФЗ-161 «О национальной платежной системе» [241]). Пример соответствия формальным требованиям (с определенным бюджетом на приведение инфраструктуры в соответствие требованиям регуляторов: разработку документов и внедрение средств защиты) показан в обзоре[69].

1.7.4 Парадигма формирования оценки уровня обеспечения ИБ в ИСМ

Современную оценку защищённости ИСМ предлагается формировать на чёткой парадигме «целевого» стандарта ISO/IEC 27001 ([317]): «Бизнес» - «Контекст» - «Активы» - «Уязвимости» - «Угрозы» - «Риски» - «Средства защиты». Для полноты комплексной оценки ИСМ в качестве сущностей иерархической модели могут быть востребованы также стандарты ISO/IEC серии 20000 – устанавливающие требования к СУУ [311] и стандарты ISO серии 22301 – устанавливающие требования к системам менеджмента непрерывности бизнеса (СМНБ) [315]. С учетом сказанного выше, основная методологическая роль в оценке защищённости ИСМ возлагается на СМИБ.

Кратко рассмотрим несколько основополагающих понятий СМИБ, которые будут полезны для корректного восприятия предложенной модели и методов оценки защищённости ИСМ, применительно к исследуемому вопросу. По представленной постановке задачи необходимо дать краткие комментарии:

- в любой организации используются активы, т.е. экономические сущности, которые вовлечены в процесс создании продукции (услуг);
- любые активы имеют уязвимости, следовательно, существуют угрозы и риски утраты целостности, доступности и / или конфиденциальности;
- на практике ценные активы организации не всегда должным образом определены, категорированы, оценены и защищены;

---

69 https://www.kommersant.ru/doc/3494853?from=four_tech

— одна из ключевых проблем – оценка защищённости активов, которая дает высшему руководству (ЛПР) сопоставимые и достоверные данные.

Представляется важным внимательно изучать исследовательские отчеты, в частности, «Сравнение эффективности средств защиты информации от несанкционированного доступа», опубликованный в 2017 г. исследователями Р.Алферовым и А.Гороховым, в котором дается анализ двух СрЗИ: Dallas Lock 8.0-С (сборка 8.0.347.4) и Secret Net (сборка 7.6.604.0). Оба СрЗИ функционируют под ОС Windows 7 Service Pack 1 (сборка 7601). В отчете указано, что для Dallas Lock 8.0-С возможно реализовать несколько успешных атак, несмотря на декларируемый дискреционный и мандатный доступ. В частности, показаны успешные атаки на известные уязвимости (например, MS15-010), получение доступа к защищаемым файлам, разные виды организации утечек. Для Secret Net показаны разные виды успешных атак, в том числе показано, как нарушитель, не имеющий административных привилегий, может получить любой доступ к защищаемым файлам и, более того – просматривать историю их изменений. Кроме того, показано, что в безопасном режиме не функционирует мандатное разграничение доступа. В общей таблице данного отчета показано, что для каждого из исследуемых СрЗИ НСД более 50% проверок не прошли.

Соответственно, возникает вопрос к степени доверия к системе ФСТЭК и испытаний СрЗИ НСД, которая не учитывает и не проверяет при испытаниях по РД (выпуска еще 1992 г.) многие неявные механизмы современных ОС Windows и доступные уязвимости. Необходимо отметить, что «базовые» испытания ФСТЭК могли быть дополнены автоматизированными проверками отечественными сканерами, в частности, «Сканер-ВС», который за десятки минут может «прогнать» около 60 тыс. проверок[70], в том числе и для СрЗИ[71].

---

[70] https://www.metasploit.com/

[71] https://habrahabr.ru/company/echelon/blog/347702/

1.7.5 Менеджмент рисков в ИСМ

В работе Р. Кини и Х. Райфа отражено положение, что для оценки «желательности» какой-либо альтернативы, ЛПР должен принять во внимание все риски с тем, чтобы осуществлять выбор «рискованных альтернатив» ([64], стр. 9). В процессе разработки, внедрения, эксплуатации и постоянного улучшения ИСМ должны быть приняты во внимание следующие риски:

- неправильное выделение критичных бизнес-процессов, что повышает затраты на реализацию средств защиты в СМИБ;
- некорректное определение активов, подлежащих защите;
- неосведомленность о ценности нематериальных активов (НМА), в т.ч. SLA, лицензий ПО, что особенно критично для ИТ-услуг);
- формально разработанные процедуры ИБ (например, регламент аудита ИБ «для галочки» по устаревшим шаблонам чек-листов консультантов);
- непринятие во внимание требований обеспечения безопасности (например, в соответствии с требованиями ФЗ-256 или ФЗ-187).

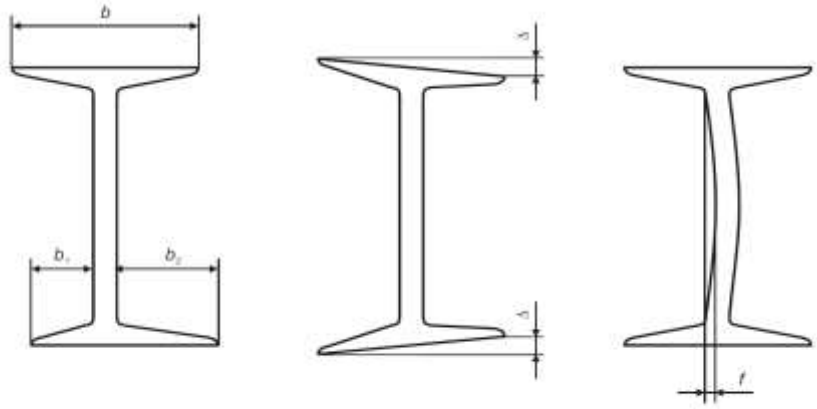
При анализе рисков должны быть приняты во внимание практические ситуации, при которых «желательная» альтернатива формируется на базе действующего законодательства (в частности, ФЗ-187). Например, при создании СМИБ (ИСМ) необходимо выполнить закупку мер (средств) обеспечения ИБ, и у ЛПР есть логичное желание перевести эту информацию в режим коммерческой тайны, тем самым снизить риск осведомленности потенциальных нарушителей. Рассмотрим пример закупочной деятельности, которая осуществляется в соответствии с федеральным законом от 18.07.2011 № 223-ФЗ «О закупках…». ЛПР вправе самостоятельно определить применяемые способы закупки, если информация о закупке содержит коммерческую тайну, а также иную информацию, доступ к которой ограничен федеральными законами. Например, приказом Министерства энергетики России от 13.12.2011 № 587 разработка, монтаж и эксплуатация ИС и систем защиты информации ТЭК отнесены к работам, непосредственно связанным с обеспечением безопасности объектов ТЭК. Соответственно, такую практику защиты «чувствительной» информации и

снижения рисков ИБ применяют многие крупные компании. В частности, при организации конкурса ЦОД «Транснефти»[72] технические решения (в том числе средства защиты информации) были «закрыты» с формулировкой, цитата: «*предоставление доступа к указанным сведениям неограниченному количеству третьих лиц создаст значительную угрозу информационной безопасности*».

1.8 Методологические основы аудита ИБ для сложных объектов

1.8.1 Классические принципы измерения объектов

Из механики хорошо известны (например, ГОСТ 8239-89 Двутавры стальные горячекатаные. Сортамент[73]) способы измерений, например, предельных отклонений по размерам поперечного сечения (см. рисунок 1.12).



b_1 — ширина укороченного фланца; b_2 — ширина удлиненного фланца;
Δ — перекос полки; f — прогиб стенки.

Рисунок 1.12 – Пример измерений отклонений двутавров ГОСТ 8239-89

К сожалению, при аудите ИБ, тем более при аудите СлПО, в существующей нормативной документации не всегда доступны способы и метрики проведения простых и ясных измерений. В частности, нельзя сказать, что «система А» более безопасна, чем «система Б», не приведя достаточных объективных свидетельств аудита. Далее будет предложен подход к формированию метрик ИБ, основанный на стандарте ISO 27004 и дополненный рядом **новых** важных ключевых элементов.

---

72 http://www.cnews.ru/news/top/2017-07-27_rossijskaya_neftyanaya_monopoliya_zasekretila_tehdokumentatsiyu

73 http://sanc.spb.ru/gost/gost8239-89.pdf

1.8.2 Существующие практики мониторинга и управления ИБ

В работах ряда известных ученых приведены различные методические подходы для выполнения мониторинга и управления сложными объектами ([253] – [255], [259], [261]). В частности, отмечается, что «*в подавляющем большинстве случаев на практике мониторинг, прогнозирование и управление состояниями СлО автоматизирован, в лучшем случае, лишь частично*» [177]. Это положение, изложенное еще в 2006 г., поясняет задачу оперативного измерения и управления процессами ИБ в сложных системах. В «Доктрине информационной безопасности Российской Федерации» — опыт количественного моделирования» отмечается, что представляется целесообразным формировать вектор наиболее существенных оценок как показателей влияния всех выделенных в модели факторов на оценку уровня обеспечения ИБ объекта [255]. В работе «Аналитический обзор докладов Международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (2010 г.) отмечается, что «п*о сути дела, большие информационные системы, как правило, собраны из нескольких систем, каждая из которых исторически создавалась в разных условиях и по различным требованиям»* [68]. Отмечается необходимость применения не только международных стандартов серии 27000, но и «*сквозных механизмов обеспечения безопасности*», например: управление инцидентами, управление непрерывностью [68]. Следует отметить, что данное положение достаточно точно коррелирует с современными риск-ориентированными стандартами ISO (в частности, серии 27001 [317] и серии 55001 [322]). Понимание, что СМИБ (ИСМ) должна строиться «*от собственника актива*» до сих пор наблюдается, к сожалению, не всегда. Возможно, новый стандарт по управлению активами ISO 55001 внесет определенную ясность в данную проблему. Необходимо пояснить, что указанные процессы ИБ могут быть реализованы и на базе существующих в настоящее время в РФ национальных стандартов ([28], [30]).

1.9 Разработка обобщенной базовой модели аудита ИБ

1.9.1 Новая модель проблемной ситуации

В соответствии с нотацией [138] определим новую модель проблемной ситуации. На основании имеющейся информации θ'_N и результатов «контрольного» оценивания (аудита) ИБ СлПО необходимо определить модель предпочтений ЛПР – Ω ([138], стр. 59), приведенную в (1.3). Отметим, что наличие **A** в (1.3) означает, что часть значений неопределенных факторов будет обязательно установлена (например, требования проведения аудита ИБ могут быть заданы регуляторами), а другая часть будет определена в процессе решения новых самостоятельных задач (например, формирования переченя средств (мер) обеспечения ИБ, рекомендованных ЛПР к внедрению в процессе аудита ИБ). Как показано в работе [138], во многих практических случаях априорное значение коэффициента эффективности **K** приводит к формированию множества «нехудших альтернатив», что может означать в конкретном случае для СлПО факт, что по результатам аудита ИБ могут быть сформированы несколько достойных альтернатив. При этом мера выбора из «нехудших» единственной – задача решается ЛПР посредством модели Ω (модели предпочтений ЛПР).

Общая постановка задачи моделирования предпочтений может быть представлена в виде:

$$\langle D, \theta'_N ; \Omega_D \rangle \qquad (1.4)$$

где:

$D = \{U, A, G, Y, W, K\}$

θ'_N – дополнительная уточненная информация о проблемной ситуации.

Предлагается расширить перечень требований к аудиту ИБ и расширить и уточнить состав дополнительной информации о проблемной ситуации θ'_N за счет новых факторов и представить задачу формирования множества стратегий ЛПР в новом виде:

$$\langle \theta_{A0}, \theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, A_N, U_N \rangle \qquad (1.5)$$

где:

- θ_{A0} – информация о начальной (исходной) цели операции;

- θ_1 – информация о результативности «мгновенных аудитов» ИБ;
- θ_2 – информация о результативности аудита всех типов (1-й, 2-й и 3-й стороной);
- θ_3 – информация об инцидентах ИБ (например, Security Operation Center);
- θ_4 – информация о новом «контексте» СМИБ (ИСМ);
- θ_5 – информация о новых предпочтениях ЛПР;
- θ_6 – информация об изменениях ФЗ (например, ФЗ-187 «ГосСОПКА»).

1.9.2 Базовая модель для аудита ИСМ

На основании постановленной задачи необходимо предложить модель ИСМ, которая содержит все базовые сущности для выполнения аудита ИБ (критерии, объект, наблюдения аудита) и позволяет генерировать оценки уровня обеспечения безопасности. Важное замечание – любая СМ содержит обязательное требование проведения внутреннего аудита ([315], [317], [321], [323]). Процесс аудита ИБ дает важную составляющую общей (интегрированной) оценки результативности ИСМ, т.е. насколько запланированные цели были достигнуты. Представляется рациональным выполнять декомпозицию «общих» целей ИСМ на специфические цели – например, оценки уровня обеспечения комплексной (интегральной) безопасности, и специфическая цель тоже может быть агрегированной, например, содержать интегральную оценку иных подцелей.

В конкретной ситуации применяется выбранная нотация для формирования базовой модели для аудита ИБ в ИСМ для СлПО ([138], стр. 73). Кроме того, отметим, что переход от обобщенной модели к модели «конкретной ситуации» является очень сложным, особенно, когда речь идет об анализе больших и сложных ТС (в том числе – СлПО) ([138], стр. 74). В ряде случаев вынужденно применяются только эвристики, т.к. многие компоненты явно не заданы ([138], стр. 55). В работе ([138], стр. 75) даются пояснения о сложностях в процедурах получения дополнительной информации, однако, есть основание предложить к применению известные и более простые процедуры «мгновенных аудитов» ИБ. Кроме того, новацией в развитии базовой модели аудита ИБ является постоянная

оценка адекватности, конкретные механизмы которой (например, циклы оптимизации) рассмотрены ранее ([79] – [87], [96]). Принимая во внимание обобщенную модель ИСМ для обеспечения безопасности СлПО (см. рисунок 1.7) и основные ограничения, которые должны быть учтены при решении поставленной задачи, предлагается базовая модель аудита ИСМ (см. рисунок 1.13).

В этой модели, как части общей модели ИСМ (рисунок 1.7), детально отражена возможность сопоставлять планируемые и реальные состояния СУ для СлПО (как объекта оценки – ОО), реализуется «замкнутый» цикл аудита (в смысле выполнения всех обязательных процедур аудита ИБ согласно [32]). На рисунке 1.13 представлена базовая модель для аудита ИСМ, необходимая как концептуальная база для описания подходов к поставленной задаче.

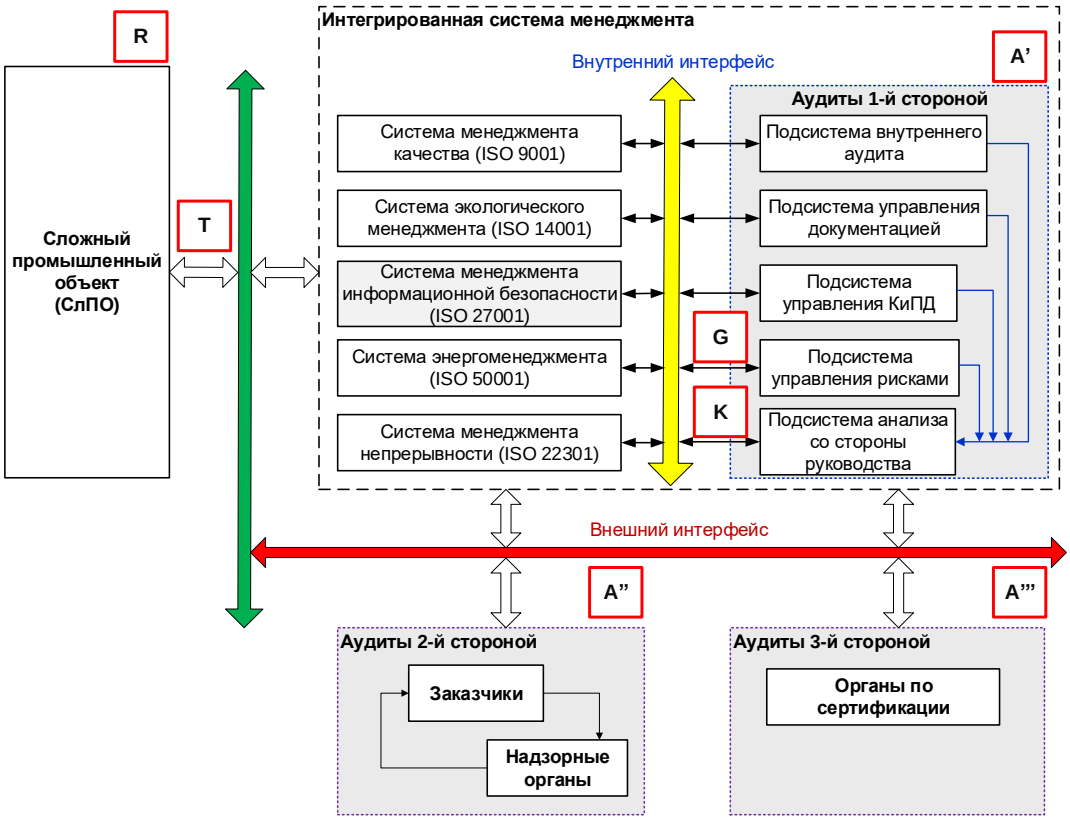


Рисунок 1.13 – Базовая модель аудита ИБ в ИСМ

Необходимо предоставить общие пояснения к базовой модели ИСМ:

1. Аудит ИСМ предполагает использование единого множества метрик, но на разных интерфейсах: для обмена «чувствительной» информацией для внутреннего и для внешних аудитов;

2. Внутренний аудит обязательно учитывают данные внешних аудитов, справедливо и обратное утверждение;
3. Воздействие на объект оценки реализуется через подсистему анализа со стороны руководства (в соответствии с циклом PDCA), являющимся требованием всех СМ).

1.9.3 Формальное описание базовой модели для аудита ИСМ

В работе Н.Винера отмечается, что ценность управления (в соответствии с древнегреческим понятием «χυβερνητίχη» - «кибернетика) еще в 1834 г. была отмечена французским физиком А.-М. Ампером в издании «Essai sur la philosophie des sciences» ([13], стр. 81). Для управления СлПО рекомендуется не только определить цели, но и точно описать существующий и требуемый определенный порядок перехода различных состояний. В частности, Н. Винер предполагал существование цепей управления (обратной связи), в которых человек «*совершенно не участвует*» ([13], стр. 164). С учетом современных специфических особенностей управления СлПО говорить о применении паровых регуляторов (регуляторов Максвелла) уже не приходится, необходимо обеспечить управление, адекватно скоростям протекающих процессов.

1.9.4 Оценка риска ИБ по базовой модели для аудита ИСМ

Объективные результаты любого аудита ИСМ, равно как статистика инцидентов ИБ, являются достоверными и объективными данными, которые могут быть приняты как апостериорные оценки свойств фактически реализованной системы безопасности для СлПО [79], [80]. При этом ЛПР имеет возможность сколь угодно уточнять (на основе полученных данных) оценки фактического состояния безопасности СлПО как по отдельным функциональным подсистемам, так и по отдельным процессам, в том числе, сопоставляя затраты на эти компоненты и величину ущерба (если имел место инцидент ИБ). Таким образом, может быть предложена следующая математическая оценка риска ИБ для СлПО как математическое ожидание двух компонент (прямого и косвенного ущерба соответственно):

$$\boldsymbol{R_t = M_t\left(R_t^1 + R_t^2\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} S^1{}_{ij} \cdot V^1{}_{ij} + \sum_{i=1}^{n}\sum_{j=1}^{m} S^2{}_{ij} \cdot V^2{}_{ij}}$$

где:

i – возможные ДД для СлПО (с учетом возможности реализации),

j – возможные сценарии реализации ДД для конкретного СлПО,

S^1_{ij} *– величина прямого ущерба при реализации риска возможных ДД,*

S^2_{ij} *– величина косвенного ущерба при реализации риска возможных ДД,*

V_{ij} *– вероятность реализации риска возможных ДД.*

На основании рассмотренных практик аудита СлПО представлен новый метод определения численных показателей (метрик) ИБ. Далее в диссертации отмечается, что с целью снижения издержек (это одна из приоритетных задач бизнеса и форма оценки результативности службы ИБ) могут быть применены метрики, например, на базе ISO/IEC (ГОСТ Р ИСО/МЭК) серии 27004 [318].

ЛПР может получать необходимые данные для принятия эффективных управленческих решений для обеспечения требуемого уровня безопасности СлПО только при наличии СМИБ (ИСМ), оперирующих достоверными оценками. Критериями результативности СМИБ (ИСМ) выступают показатели степени соответствия процессов ИБ установленным требованиям, а также результаты оперативного оценивания ЛПР (*management review*) заданных и фактических показателей деятельности. Рассмотрим ИСМ в известной нотации «сущности – связи» (*Entity – Relationship*), определим $\mathbf{Z = \{E_n ; R_m\}}$ как множество, состоящее из $\mathbf{E_n}$ – множество сущностей (например, технических систем) и $\mathbf{R_m}$ – множество связей конкретного объекта (например, данных аудита ИБ в СлПО). С учетом базовой модели аудита ИСМ (см. рисунок 1.13) $\mathbf{Z_{base} = \{E_{n\ base} ; R_{m\ base}\}}$. Показатели степени соответствия процессов ИБ установленным требованиям обозначим как $\mathbf{Z_q = \{E_q ; R_q\}}$. При этом $\mathbf{Z_q}$ может включать ограниченное множество показателей, необходимых для оценки определенных процессов ИБ (например, внутренний аудит ИБ) или только определенных метрик (например, количество инцидентов ИБ), это множество обозначим как

$\mathbf{Z'_q}$. Тогда ЛПР может формализовать математическую постановку задачи применения метрик ИБ как:

$$\mathbf{Q} = \frac{\mathbf{Z_q} \cap \mathbf{Z_{base}}}{\mathbf{S}} \; ; \; \left(\mathbf{R_q} = \mathbf{R_{m\,base}}\right)$$

где:

S – затраты для применения метрик ИБ с учетом применимых требований.

Множество **Q** может быть формализовано в различных представлениях современных ТС (удобных для получения оперативных значений применяемых метрик, например, из систем DLP, SIEM, IDS/IPS и пр.). В определенном смысле, получение формализованного множества **Q** позволяет уйти от субъективного (экспертного) подхода или, минимально, дополнить предположения экспертов подтверждающими объективными достоверными данными для конкретного объекта. Кроме того, **Q** позволяет сопоставить не только степень соответствия текущих оценок базовой модели аудита ИСМ $\mathbf{Z_{base}}$, но и выявить степень соответствия заданным (установленным или перспективным) требованиям ИБ $\mathbf{Z_q}$, например, заблаговременно проверить формальное соответствие реализованной СМИБ (ИСМ) предполагаемым требованиям (например, GDPR или ФЗ-187). Для оценки степени достижения целей ИБ (т.е. оценки результативности) рекомендуется применять метрики ИБ, которые обеспечивают поддержку принятия решений ЛПР на соответствующих уровнях иерархии.

1.10 Метод определения численных показателей (метрик) ИБ

1.10.1 Сопоставление целей бизнеса и метрик ИБ

В настоящее время опубликовано достаточно материалов как в поддержку внедрения (сертификации) СМ (в т.ч. СМИБ), так и противоположных консервативных оценок. Очевидно, что успех ряда стандартов (например, ISO серий 9001 и 27001) вызван определенными факторами, реализация которых представляется целесообразным в экономическом, техническом и социальном аспектах [309]. Помимо анализа статистики, разумно рассмотреть мнение представителей крупного бизнеса, тем более, специализирующегося в вопросах ИБ. В частности, Наталья Касперская полагает, что «*…для каждого предприятия*

в силу его индивидуальной специфики управление ИБ всегда будет не типовым, а уникальным. … InfoWatch является примером предприятия, на котором не имеет смысла внедрять стандарты ISO — прежде всего, потому, что объем затрат на их внедрение не оправдается возможными выгодами»[74]. Такое же мнение высказал в 2017 г. замначальника ГУБиЗИ ЦБ РФ А.Сычев[75].

Для целей бизнеса реализация требований ИБ наилучшим образом изложена в стандартах ISO серии 27000 ([315] – [319]). Очевидно, система метрик ИБ должна соответствовать терминологии бизнеса и позволять объективно оценивать предлагаемые проекты заинтересованными сторонами (не только ЛПР). Для процесса формирования, анализа и сравнения метрик ИБ стандартным подходом представляется применение «целевого» стандарта ISO 27004 [318]. Ниже будет представлен метод оценки результативности СМИБ и пример формирования численных (количественных) показателей.

1.10.2 Базовые требования к формированию метрик ИБ

С целью снижения издержек (это одна из приоритетных задач любого бизнеса и наиболее «презентабельная» форма оценки результативности службы ИБ) могут быть применены метрики, показывающие степень достижения возможного максимума (например, выполнения в срок проектов) ([98], [105]). В стандарте ISO 27004 установлена необходимость определения соответствующих заинтересованных сторон, которым следует принимать участие в формировании области применения измерений ИБ. Специфические результаты измерений результативности отдельных мер (средств) обеспечения ИБ следует определять и доводить до сведения заинтересованных сторон, которые могут быть внутренними или внешними по отношению к подразделениям организации (п. 7.2 стандарта [318]). Для этого требуется надежный механизм контроля передачи информации на разные интерфейсы. Модель такой системы представлена в публикации [105].

---

74 http://bis-expert.ru/articles/45301

75 http://www.rbc.ru/finances/14/02/2017/58a1ed4c9a794774d2272578

1.10.3 Постановка задачи формирования метрик ИБ

Проект внедрения и постоянной оценки СМИБ (ИСМ) необходимо рассматривать с учетом ожидаемых выгод – экономической и неэкономической природы. В этих условиях постановка задачи формулируется следующим образом: разработка методологии формирования численных (количественных) метрик ИБ, соответствующих в целом иерархической системе бизнес-целей организации, для оценки результативности СМИБ (ИСМ) и обеспечения безопасности жизненно значимых активов организации ([317], [323]).

Стандарт ISO 27001 требует от организации «*проводить регулярные проверки результативности СМИБ*», а также определять, «*каким образом проводить измерение результативности выбранных мер и средств контроля и управления и их групп*» [317]. В ISO 27004 рекомендуется, чтобы на СМИБ не выделялись ресурсы в ущерб другой (основной) деятельности, и, в идеальном случае, деятельность, связанная с измерениями, была бы интегрирована в плановую деятельность организации (п. 8.2 стандарта [318]). Дополнительно требуется обеспечить интеграцию анализа данных в соответствующие процессы для обеспечения регулярного функционирования этих процессов. Следовательно, возрастает роль внутреннего аудита в масштабе всей организации. Очевидно, что экономия ресурсов на обеспечение измерений СМИБ должна приводить к выполнению целей измерений, связанных с ИБ, и получению оценки результативности в реализованной СМИБ (п. 5.1. b) [317]). Меры и средства обеспечения ИБ, выбранные в рамках программы измерений, следует непосредственно связывать с функционированием СМИБ, а также процессами основной деятельности организации. Измерения могут быть интегрированы в обычные процессы функционирования организации, что обеспечивает решение поставленной задачи. В аспекте постановки задачи важно, что в стандарте ISO 27004 определены требования к программе измерений (п. 5.2 [318]). В стандарте ISO 27004 определены факторы успеха, непрерывного совершенствования СМИБ, среди которых отметим [318]:

— количественную оценку мер безопасности;

— оценку результативности программы и полезности измерений;

— оценивание результатов измерений.

1.10.4 Подходы к формированию системы метрик ИБ

Метод формирования системы численных (количественных) метрик ИБ, должен соответствовать иерархической системе бизнес-целей организации, формируемых для оценки результативности СМИБ. С позиции требований бизнеса важны следующие параметры: входные величины экономической природы, выбор активов, анализ соответствующих данных и распространение отчетов. В качестве входных величин для формирования системы метрик ИБ на основании поставленных бизнесом целей на разных уровнях иерархии управления организации могут рассматриваться следующие показатели:

— объем затрат на обеспечение бизнеса (в т.ч. управленческий персонал),

— период окупаемости проектов (в т.ч. связанных с безопасностью),

—длительность допустимых простоев для бизнеса (в т.ч. основных активов).

Отчеты с результатами измерений, подлежащие распространению на «внешнем интерфейсе» (см. рисунок 1.13), должны содержать только данные для внешнего использования и должны утверждаться перед выпуском (п. 9.3 [318]). Дополнительно рекомендуется организовать проверку «утечки» данных в конкретном «мини-цикле» PDCA[76].

1.10.5 Метод оценки результативности ИБ

Метод измерений должен основываться на атрибутах выбранных объектов измерений (п. 5.4.2. [318]). Примерами объектов измерений могут служить:

— результативность мер и средств обеспечения ИБ, реализованных в СМИБ,

— результативность процессов ИБ (в т.ч. реализованных в СМИБ),

— степень удовлетворенности уровнем ИБ заинтересованных сторон.

Метод измерений может использовать объекты измерений и атрибуты из разнообразных источников, например:

— результаты анализа риска, оценки риска и обработки рисков ИБ,

---

[76] Журнал «Автоматизация в промышленности», 2017 г., № 7, стр. 33-62

— отчеты о внутренних и/или внешних аудитах,

— результаты тестирования, например, полученные в результате тестирования на проникновение (*penetration test*).

Отметим, что практика *penetration test* все чаще становится одним из обязательных инструментов, в частности, это указано в отчете «New Regulations Increase The Risk And Compliance Burden»[77]. В работе Р.Кини и Х.Райфы определено, что для формирования оценки (и объективного выбора альтернатив) должны быть определены и шкалы измерений, критерии и числовые характеристики ([64], стр. 47). В той же работе показаны примеры «неизмеримых» целей. Проблема может быть поставлена шире – как достижение одной цели (оценка результативности СМИБ) за счет гарантированного достижения другой цели – результативного выполнения аудита ИБ. Примеры «*каузального эмпиризма*» (см. ([64], стр. 48) могут привести к сокращению издержек для решения проблем обеспечения заданного уровня ИБ для СлПО, в частности, приводятся примеры неудачного формирования «дерева целей» NASA (1030 целей). Очевидно, что ЛПР для реального СлПО сложно обеспечить «обсчет» такого «дерева целей» в режиме, близком к РРВ, при известных ресурсных ограничениях.

Для примера выберем ряд мер и средств обеспечения ИБ в соответствии с требованиями стандарта ISO 27001 [317]. Выбор данного множества обоснован, во-первых, акцентом на контроле жизненно важных активов и, во-вторых, применением практически в любой СМИБ с малой вероятностью исключения. Результаты представлены в таблице 1.5.

В дополнение к требованиям ISO 27004 представленный метод включает набор этапов для обеспечения «связи» целей бизнеса и целей ИБ посредством перечня активов, подлежащих защите.

---

77 http://www.infosecisland.com/blogview/25054-2020-Vision-How-to-Prepare-for-the-Future-of-Information-Security-Threats.html

Таблица 1.5 – Выбор мер (средств) обеспечения ИБ (выборка)

№ п.п.	Мера и средство контроля и управления	Пункт стандарта	Назначение
1.	Должны проводиться проверки всех кандидатов на работу, с учетом классификации информации, к которой будет осуществляться доступ	A.7.1.1	Предварительная проверка
2.	Учтенные активы должны иметь своих владельцев	A.8.1.2	Владение активами
3.	Должны быть разработаны и применены процедуры для работы в зонах безопасности	A.11.1.5	Работа в зонах безопасности

Описание шагов представленного метода формирования метрик ИБ представлено в таблице 1.6.

Таблица 1.6 – Метод формирования метрик ИБ

№ п.п.	Шаг метода формирования метрик ИБ	Префикс по ISO 27004
1.	Определение области сертификации СМИБ (scope) исходя из поставленной задачи и дополнительной информации θ_N	– (новый)
2.	Обеспечение максимальной полноты перечня активов (asset), в аспекте дополнительной информации θ_N	– (новый)
3.	Определение мер (средств) обеспечения ИБ (controls) (из «Заявления о применимости»)	– (новый)
4.	Определение реализации меры (средства) обеспечения ИБ	– (новый)
5.	Определение объектов измерения	О
6.	Определение атрибутов	А
7.	Определение метода измерения	МИ
8.	Определение основной меры	ОМ
9.	Определение функции измерения	Ф
10.	Определение производной меры измерения	Пр
11.	Определение аналитической модели	АМ
12.	Определение показателей	П
13.	Определение критериев принятия решения	Кр
14.	Определение результатов измерения	РИ

Пример расчета метрик ИБ для 4 выбранных мер (средств) обеспечения ИБ в соответствии с требованиями современных стандартов ISO серии 27000 ([317], [319]) показан далее на рисунке 1.14

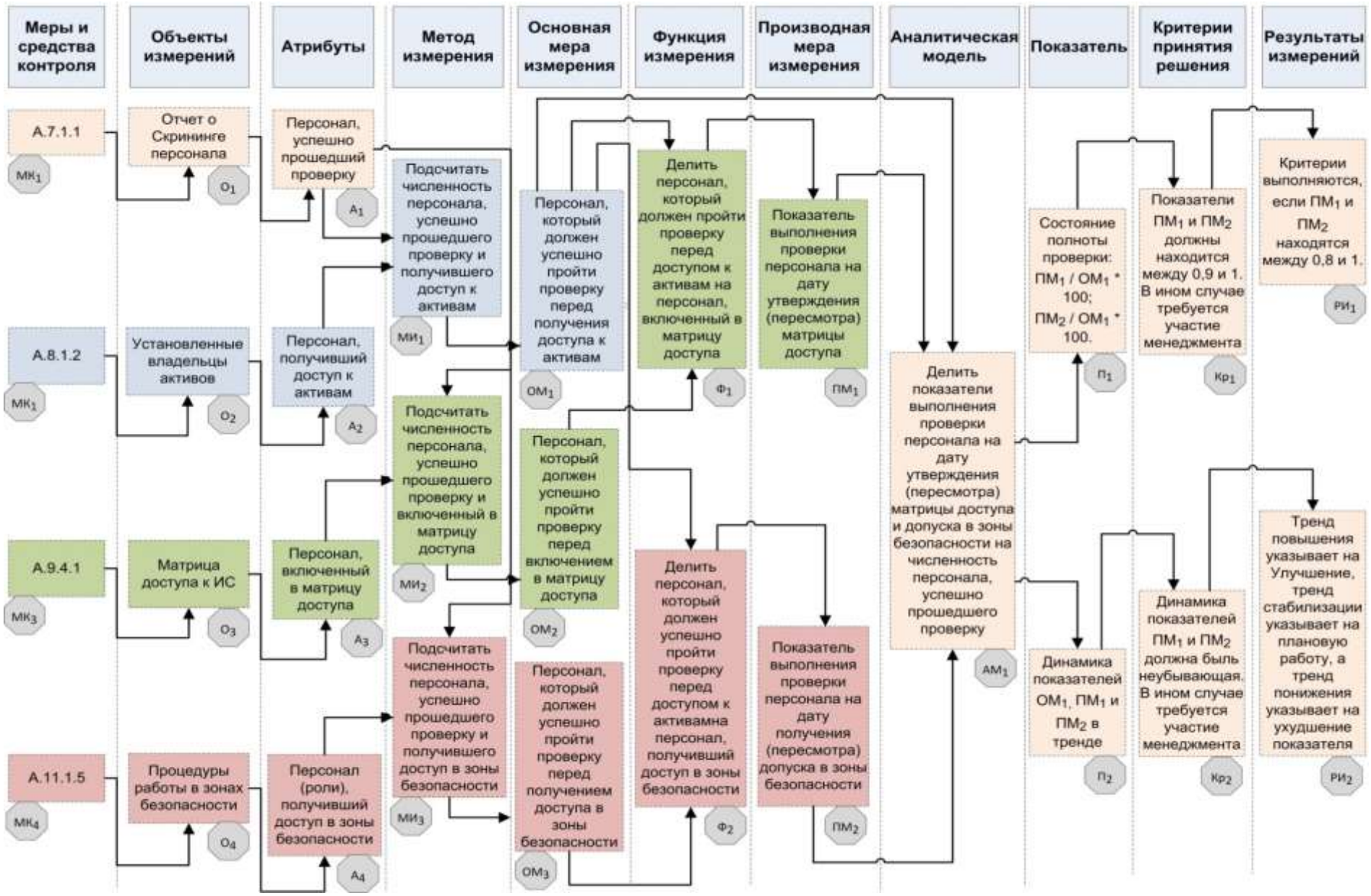


Рисунок 1.14 – Пример расчета метрик ИБ

1.11 Выводы к Главе 1

1. Требования к моделям выполнения аудита ИБ в ИСМ для СлПО должны включать независимость получения оценок, численные метрики степени зрелости и уровня адекватности подсистем ИБ в составе ИСМ. Кроме того, модели выполнения аудита ИБ должны позволять практическое применение с учетом как актуальных угроз, так и противодействия новым вызовам в области ИБ.
2. Представленый метод на основе стандарта ISO 27004 позволяет получать оценки результативности внедрения СМИБ (ИСМ), пригодные для анализа и принятия управленческих решений ЛПР, используя систему метрик ИБ, как «рабочий элемент» в существующей СУ для СлПО.
3. Полученные оценки могут рассматриваться применительно к СМИБ (ИСМ) на всех стадиях ЖЦ ИС. Для формирования оценки уровня безопасности СлПО необходимо формировать «сквозную» систему метрик ИБ, образуя оптимальную (иерархическую) структуру (по процессам, подразделениям или продуктам/услугам) с обязательным учетом жизненно важных активов.
4. Представляется рациональным при выполнении анализа СМИБ (ИСМ) со стороны ЛПР оперировать метриками бизнеса, выбранными таким образом, чтобы демонстрировать добавленную стоимость внедренных СМ и отражение конкретного вклада в повышение конкурентоспособности организации. Необходимо контролировать и обеспечить гарантирование замыкания «мини-циклов» PDCA на соответствующих уровнях иерархии СМИБ (ИСМ).

2 Глава. Методы и модели проведения аудита ИСМ для СлПО

2.1 Проблемы определения сущностей модели

2.1.1 Современные законодательные определения объекта аудита

Одной из важнейших задач является точное определение объекта аудита – СлПО. Только на основании полученного достоверного и объективного описания объекта аудита возможно создание и применение моделей и методов аудита ИСМ для СлПО. Прежде всего, необходимо рассмотреть существующее законодательство (помимо указанного в Главе 1) для определения важнейшего класса требований, предъявляемых к СлПО – законодательных требований. Применимое законодательство включает в себя: Федеральные законы [170], [238], [240], [242], [244], [246] – [251], а также постановления и распоряжения Правительства РФ: [156] – [161], [168], [178], [211]. В настоящее время на законодательном уровне не в полной мере определены механизмы взаимодействия и ответственность субъектов, прямо или косвенно участвующих в обеспечении безопасности критически важных объектов (КВО): органов государственной власти всех уровней, государственных структур, частных охранных структур, служб безопасности, разработчиков, производителей и поставщиков СрЗИ. В частности, в случае с уязвимостью в программе Cisco Smart Install Client (апрель 2018 г.) логичным было бы обвинить разработчика. Однако разработчик еще в марте 2018 г. выявил эту уязвимость и создал патч. Но большинство пользователей его не установили, также как и в случае с эпидемией шифровальщика WannaCry, и по рынку прокатилась волна увольнений[78].

Механизмы государственного лицензирования, надзора и контроля в этой сфере не в полном объеме закреплены законодательными актами, в результате чего эти функции малоэффективны. На данный момент можно констатировать отсутствие единых норм и системного подхода при построении системы защиты КВО, исключение составляет 187-ФЗ от 26 июля 2017 г. "О безопасности критической информационной инфраструктуры Российской Федерации". В

[78] http://spb.rbcplus.ru/news/5ad708107a8aa906b7e8cd0c

диссертации Кузьмина В.В. отмечается: *«обеспечение защиты критически важных объектов включает в себя и защиту объекта и систему информационной безопасности»* [73]. В работах проф. Молдовяна А.А. содержатся важнейшие положения обеспечения безопасности АСУ ТП, в том числе – выполняющих важные (критичные) приложения ([133]– [137]).

В настоящий момент известны различные определения КВО:
1. «Критически важный объект – это объект, нарушение или прекращение функционирования которого приведет к потере управления экономикой РФ, субъекта РФ или административно-территориальной единицы субъекта РФ, ее необратимому негативному изменению (разрушению), либо существенному снижению безопасности жизнедеятельности населения» (68-ФЗ [237]);
2. «*Критически важные объекты – объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению (или разрушению) или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени*» ([178]);
3. «*Критически важный объект инфраструктуры РФ – объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта РФ либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок*» ([174]).

Следует отметить также, что существует направление защиты КСИИ, предложенное ФСТЭК России ([142] – [145]) еще в 2007 г., но так и не прошедшее регистрацию в Минюсте РФ. Важно, что в мае 2018 г. ФСТЭК России разместила на своем сайте информационное сообщение N 240/22/2339 об отмене

документов КСИИ[79]. В документе ФСТЭК приводится свое определение КСИИ ([142], стр. 15). В ФЗ-256 [247] также приведено свое определение КВО ТЭК. Необходимо отметить, что в тексте ФЗ-256 нет упоминания о рисках, что не позволяет применять этот ФЗ в полной мере как базу для создания современной СМИБ (ИСМ) и проведения аудита ИБ для СлПО на базе современных риск-ориентированных стандартов. В Приказе ФСТЭК России № 31 [167] содержатся требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами (АСУ ТП) на КВО, а также объектах, представляющих повышенную опасность для жизни и здоровья людей.

2.1.2 Определение нового термина СлПО

Известно определение МЧС «*Объект инфраструктуры, критически важный для национальной безопасности*» (см. «Методические рекомендации по проведению инвентаризации критически важных и / или потенциально опасных объектов Российской Федерации и формированию перечня критически важных объектов на региональном уровне», утв. 19.06.2008 № 2-4-60-10-14[80]). Согласно 116-ФЗ, к СлПО могут относиться не только здания и сооружения, но также предприятия, их участки или иные производственные объекты [238]. Но в письме Госстроя «О разъяснении нормативно-правовых и нормативно-технических документов в области проектирования особо опасных производственных объектов» сложные объекты трактуются только в категории «*особо опасные, технически сложные и уникальные объекты*», в отношении только зданий и сооружений [217]. Известна норма ст. 48.1 Градостроительного кодекса РФ [16], где указано, что к особо опасным и технически сложным объектам относятся, например:

- объекты использования атомной энергии;
- объекты космической инфраструктуры;
- аэропорты и иные объекты авиационной инфраструктуры.

---

79 https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1585-informatsionnoe-soobshchenie-fstek-rossii-ot-4-maya-2018-g-n-240-22-2339

80 75.mchs.gov.ru

Соответственно, СлПО должен рассматриваться не только в техническом, но и в административном аспекте. Предлагается далее применять следующее **новое** определение: «**СлПО** – это технический объект, имеющий систему управления, несанкционированное изменение штатного режима функционирования которого, связанное с нарушением свойств ИБ, может привести к угрозе техногенных катастроф с необратимыми последствиями». В дальнейшем будет использоваться введенный выше термин СлПО, т.к. предложенные методы и модели аудита ИСМ не ограничиваются только объектами ТЭК или только какими-либо иными отраслевыми приложениями.

2.1.3 Современные стандартизированные определения объекта аудита

Определенное значение на развитие теоретических и методических подходов к обеспечению ИБ для СлПО оказало создание структурированной системы мониторинга и управления инженерными системами зданий и сооружений (СМИС) [186], [187]. Основным назначением СМИС является обеспечение автоматического мониторинга инженерных систем, технологических процессов, сооружений инженерной защиты, а также передача в РРВ информации об угрозе и возникновении ЧС. Представляется важным отметить, что СМИС, помимо ведомственных приказов (№ 612 МЧС от 27.10.2009), также опирается на ГОСТ Р ([41] – [43]). Отдельно необходимо рассмотреть специальную серию стандартов ПАО «Газпром» «Система обеспечения информационной безопасности» СОИБ ([222] – [229]).

Кроме того, представляется целесообразным рассматривать для создания системы управления ИБ для СлПО зарубежные отраслевые стандарты: NIST серии SP 800, ISA серии 99, стандарты American Petroleum Institute (API), стандарты American Gas Association (AGA) [188], [192] – [198]. В частности, новый стандарт ISA/IEC 62443-4-1-2018 определяет требования к процессу безопасной разработки и поддержки продуктов, используемых в АСУ ТП[81]. Стандарт также определяет безопасный ЖЦ разработки с учетом безопасной реализации (в том числе рекомендации по программированию), верификации и

[81] https://www.securitylab.ru/news/492355.php

проверке подлинности, управлению дефектами, управлению исправлениями и окончанию срока службы продукта[82]. В Европе широко известны стандарты IEC [199] – [203]. Представляется необходимым отметить ГОСТ РО 0043-002-2012 «Защита информации. Аттестация объектов информатизации. Общие положения» [44], который предназначен, в том числе, для аттестации ОИ. Вместе с тем, к этому документу экспертами предъявляются претензии, в частности, из-за возможности ошибок при проведении аттестации (поиск ошибок в ПО, анализ установленных патчей безопасности и пр.) [189] – [191].

2.1.4 Определение категорий объектов аудита

В ряде источников приводятся различные подходы к категорированию (отнесению) объектов различной природы к КСИИ ([2], [184], [185]). Принимая во внимание, что к СлПО приоритетно могут быть отнесены системы, нарушение штатного режима функционирования которых может нарушить управление чувствительными процессами, с учетом практики выполненных проектов, предлагается следующее обобщение:

– СУ транспортом (наземным, воздушным, морским);
– СУ энергоснабжением;
– СУ добычей и транспортировкой нефти и газа;
– СУ финансово-кредитной и банковской деятельности;
– СУ предупреждения и ликвидации ЧС.

Соответственно, в категорию СлПО для решения конкретной рассматриваемой задачи включены приоритетные КСИИ (например, АСУ ТП объектов ТЭК), а также ИС, относящиеся к юрисдикции МЧС или Банка России. Отметим, что инциденты прерывания нормальной деятельности КО БС в РФ, к сожалению, хорошо известны ([100], [108]).

2.1.5 Определение значимости последствий для объекта аудита

Для определения значимости последствий для объекта аудита (СлПО) могут применяться различные подходы. В частности, известен подход Сломянского,

---

82 https://www.automation.com/automation-news/industry/isa-announces-newly-published-isaiec-62443-4-1-2018-security-standard

Глебова и Галкина к категорированию КВО, при котором для определения значимости показателей используется МПС. Указанные авторы провели экспертный опрос специалистов федеральных органов исполнительной власти, специалистов МЧС, всего к опросу было привлечено 30 специалистов. В результате были определены соответствующие коэффициенты значимости показателей (см. таблицу 2.1).

Таблица 2.1 – Значимость факторов при оценке важности объекта

№№ п/п	Факторы	Коэффициент значимости
1	Значимость объекта для экономики страны	0,3729
2	Нанесение ущерба престижу государства	0,1141
3	Возможные угрозы населению и территориям	0,5130
Итого		1,0

В работе Национальной академии наук Белоруссии «Классификация критически важных объектов информатизации по требованиям физической защиты с использованием методов кластерного анализа» (см. «Искусственный интеллект» 2010, Вып. 4, С. 677) отмечается, что «*Непременным условием нормального функционирования с позиции физической защиты ОИ КВО является своевременное пресечение возможных акций нарушителей*». Также в указанной работе приводятся количественные оценки экономического ущерба (к сожалению, только на день инцидента) как процент от стоимости активов КВО (например, катастрофический ущерб предложено считать свыше 15%).

Представляется необходимым до начала формирования современных риск-ориентированных моделей определить негативные последствия, возможные при нарушении функционирования СлПО. Эти негативные последствия рассчитываются по-разному (Hirshmann ([207]), Yokogawa ([376]), методические документы МЧС (указанные выше), постановление Правительства № 304 [155]). Отметим два подхода оценки последствий ЧС: предложенные компанией Hirshmann и изложенные в постановлении Правительства № 304 [155] (соответственно, таблица 2.2 и таблица 2.3).

Таблица 2.2 – Оценка последствий ЧС по методике Hirshmann

Уровень	**Описание**	**Люди**	**Окружающая среда**	**Производство и оборудование**
5	Катастрофа	Смертельный исход	Пагубные последствия вне зоны производства	Потери более 1 млн.
4	Тяжелые	Несчастный случай с потерей трудоспособности	Пагубные последствия в зоне производства	Потери более 500 тыс.
3	Серьезные	Лечение	Все утечки в зоне производства не сразу устраняются	Потери более 100 тыс.
2	Малые	Первая помощь	Все утечки в зоне производства устранены	Потери более 10 тыс.
1	Незначительные	Без травм	Без утечек	Потери менее 10 тыс.

Таблица 2.3 – Оценка характера ЧС ситуаций ТЭК по постановлению Правительства № 304

Характер ЧС	**Территория**	**Пострадавшие**	**Материальные потери, руб.**
Локальный	Не выходит за пределы территории объекта	не более 10 чел.	не более 100 тыс.
Муниципальный	Не выходит за пределы территории одного поселения или внутригородской территории города федерального значения	не более 50 чел.	не более 5 млн.
Межмуниципальный	Не выходит за территорию двух и более поселений, внутригородских территорий города федерального значения или межселенную территорию	не более 50 чел.	не более 5 млн.
Региональный	Не выходит за пределы территории одного субъекта Российской Федерации	свыше 50 чел., но не более 500 чел.	свыше 5 млн., но не более 500 млн.
Межрегиональный	Затрагивает территорию двух и более субъектов Российской Федерации	свыше 50 чел., но не более 500 чел.	свыше 5 млн., но не более 500 млн.
Федеральный	-	свыше 500 чел.	составляет свыше 500 млн.

2.1.6 Актуальные проблемы терминологии объекта аудита

В качестве недостатков существующего статического подхода рассмотрим пример противодействия известному вирусу WannaCry[83]. Начало эпидемии определено 12.05.2017, распространение происходит через эксплоит EthernalBlue. Патч для этого вируса был выпущен заблаговременно (14.03.2017) и далее, как правило, штатные IPS/IDS уже его определяли вполне успешно. Однако, успешность атаки WannaCry (500 тыс. компьютеров в 150 странах) показала, что даже статические меры «*сделал и забыл*» не всегда выполняются.

Актуальный ГОСТ Р 51583-2014 [45], к сожалению, повторяет все ранее существовавшие ограничения на создание современных систем защиты – сохранения «фокуса» на формирование моделей (статических) УБИ, даже несмотря на ссылку на ISO 27005 по управлению рисками ИБ [319], сохранения порядка разработки на основании ТЗ, упоминание стандартов ГОСТ Р ИСО/МЭК серии 15408 (не указано применение «Задания по безопасности»). Кроме того, достаточно спорным выглядит требование обеспечения защиты информации проведением аттестации на соответствие требованиям безопасности информации: ФСТЭК России дало официальное разъяснение по данному вопросу, что решение об аттестации может быть принято заказчиком самостоятельно [62]. Сожаление также вызывает общая небрежность документа. Например, Приложение А содержит описание стадии 4 «Эскизный проект», которая не имеет ни одного входа и ни одного выхода, а также приведены требования по управлению проектом (ГОСТ Р 54869), которые далее нигде не применяются (см. рисунок 2.1).

В общем случае, современные актуальные ГОСТ Р в настоящее время не позволяют однозначно оперировать специальной терминологией применительно к рассматриваемой задаче.

---

83 http://reply-to-all.blogspot.ru/2017/07/blog-post.html

Примерный перечень и содержание нормативной информации национальных стандартов, рекомендуемых к применению при создании автоматизированных систем в защищенном исполнении

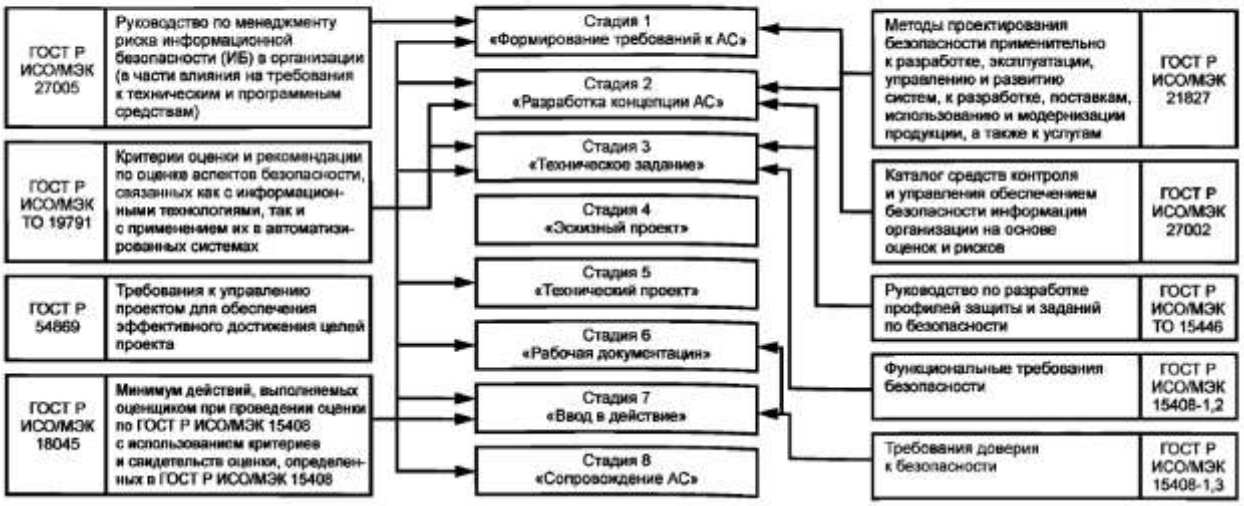


Рисунок 2.1 – Приложение А к стандарту ГОСТ Р 51583-2014

Рассмотрим 4 наиболее показательных примеров явных «нестыковок» действующих в РФ нормативных документов:

1. «Контролируемая зона» обозначена как «*пространство (территория, здание, часть здания и т.п.), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового пропуска, и посторонних транспортных средств*» [142] и также как *«пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств»* [5].

2. «Доступность информации» обозначена как «*состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно*» [142] и также как «*свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта»* [22].

3. Целостность информации обозначена как «состояние *информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право»* [5] и также как «*способность средств вычислительной техники или автоматизированной*

системы обеспечить неизменность информации в условиях случайного и / или преднамеренного искажения (разрушения)» [142].

4. Угроза безопасности информации – «*совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и / или несанкционированными и / или непреднамеренными воздействиями на нее*» (ФСТЭК КСИИ) [142] и также как *«совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации»* [49]. Даже на отраслевых конференциях, таких как Positive Hack Days 8, экспертами отмечаются нестыковки требований законодательства в области КИИ (выполнять обязаны уже сейчас, но подзаконных актов от ФСБ и ФСТЭК нет). Отдельно снова отмечена проблема несоответствия терминологии и определений в документах у ФСТЭК и ФСБ[84].

Достаточно интересно анализировать «корень» терминологических казусов, которые можно проследить с общих и неконкретных формулировок еще 20-летней давности. Например, в ст.2 ФЗ 5485-1 «О государственной тайне» 21.06.1993 г. (в редакции в ред. Федерального закона от 06.10.1997 № 131-ФЗ) изложено: «*средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации*»[85]. Эта формулировка дает основание во многих проектах ФЗ и Постановлений Правительства в области ИБ повторять эту обтекаемую конструкцию: «*средство – это средство…*». Примерно такие же дискуссии возникают при обсуждении терминов в законе «О безопасности КИИ»[86]. Однако необходимо признать, что данная проблема вообще весьма распространена и в мире [85], [86]. В частности, в США на уровне двух крупнейших государственных организаций National

84 https://www.securitylab.ru/blog/personal/valerykomarov/343982.php?R=1
85 http://www.securitylab.ru/blog/personal/Business_without_danger/341970.php
86 http://lukatsky.blogspot.ru/2017/08/blog-post_9.html

Institute of Standards and Technology (NIST) и Department of Homeland Security (DHS) происходят дискуссии о применяемых терминах, в частности, насколько различаются трактовки для термина «*cybersecurity incidents*»[87].

2.2 Проблемы при оценке уязвимостей при моделировании СлПО

В настоящее время известно несколько систем оценки уязвимостей, которые с различной частотой и практическим успехом используются в процессе обеспечения ИБ для СлПО. Известные следующие системы:

- CWE[88] (Common Weakness Enumeration).
- CVSS[89] (Common Vulnerability Scoring System).
- NIAC[90] (National Infrastructure Advisory Council).
- OWASP[91] (Open Web Application Security Project).
- Microsoft Rating System[92]
- Korea Internet & Security Agency[93]

2.2.1 Microsoft Rating System

Система Microsoft Rating System характеризуется структурированием уязвимостей по 4 классам (в порядке снижения критичности): Critical, Important, Moderate, Low. Обратим внимание, что оценки уязвимостей предоставляются по различным продуктам компании Microsoft, эти оценки привязаны к численной шкале, но не всегда соответствуют иным системам оценки, как будет показано на примере далее.

2.2.2 Оценка уязвимостей OWASP Top 10 – 2017

Система оценки уязвимостей OWASP Top 10 – 2017, открытый проект, который разработан международным сообществом OWASP[94]. База содержит более 500 тыс. уязвимостей[95]. Проект OWASP не является официальным стандартом, это информационный документ, который широко используется

---

87 https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
88 http://cwe.mitre.org
89 https://en.wikipedia.org/wiki/CVSS#External_links
90 https://www.dhs.gov/national-infrastructure-advisory-council
91 https://www.owasp.org/index.php/Main_Page
92 https://www.cs.colostate.edu/~malaiya/p/cvssMicrosoft15.pdf
93 https://www.researchgate.net/institution/Korea_Internet_Security_Agency
94 https://www.securitylab.ru/news/489784.php
95 https://www.owasp.org/index.php/Top_10_2013-Top_10

многими организациями и экспертами в области кибербезопасности для классификации уровня опасности уязвимостей. За последние годы рейтинг обновлялся несколько раз: в 2004, 2007, 2010, 2013 и 2017 годах. В новом рейтинге появились две новые позиции[96]:

– A8:2017 – Insecure Deserialization, which permits remote code execution or sensitive object manipulation on affected platforms.
– A10:2017 – Insufficient Logging and Monitoring, the lack of which can prevent or significantly delay malicious activity and breach detection, incident response, and digital forensics.

2.2.3 Система оценки уязвимостей CVSS

Общая система оценки уязвимостей CVSS разработана некоммерческой организацией FIRST (Forum of Incident Response and Security Teams). С 2012 г. действует CVSS версии 3, которая является открытой схемой, позволяющей обмениваться информацией об уязвимостях ИС[97], актуальный релиз – июнь 2015 г. Цель системы CVSS состоит в том, чтобы предоставить менеджерам по ИТ, разработчикам СрЗИ, разработчикам ПО и иным исследователям возможность общаться на языке оценки уязвимостей ИТ. В качестве примера рассмотрим патчи, устраняющие серьезную уязвимость в Oracle Identity Manager, опасность которой оценена в максимальные 10 баллов по шкале CVSSv3[98]. Обратим внимание, что Oracle Identity Manager сама по себе содержит чувствительные данные, доступ к которым должен строго контролироваться. Уязвимость CVE-2017-10151 представляет собой «установленную по умолчанию учетную запись» без пароля и может быть проэксплуатирована удаленно без аутентификации[99].

2.2.4 Сравнение систем оценки уязвимостей

Рассмотрим два примера сравнения различных систем оценки уязвимостей: CVSS и Microsoft Exploitability Index (см. рисунок 2.2 и рисунок 2.3), а также CVSS с OWASP (см. таблицу 2.4). На рисунке 2.2 представлено

96 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
97 http://www.first.org/cvss
98 http://www.securitylab.ru/news/489422.php
99 http://www.oracle.com/technetwork/security-advisory/-cve-2017-10151-4016513.html

сравнение систем оценки CVSS и Microsoft для двух продуктов Microsoft: Internet Explorer и ОС Windows 7. Отметим, насколько разнятся оценки, особенно для двух основных метрик ошибок – False Positive и False Nagative.

Software	Performance Measures	CVSS Exploitability Metrics		MS-Exploitability Index	
		Whole Sample (%)	*Balanced Sample (%)*	*Whole Sample (%)*	*Balanced Sample (%)*
IE	Sensitivity	97	97	85	85
	Precision	7	**50**	7	**57**
	F1-Measure	13	33	12	34
	F2-Measure	27	**82**	25	**77**
	False Positive Rate	99.30	97	92.70	**64**
Windows 7	Sensitivity	65.38	65	82.69	82
	Precision	19.43	**50**	14.53	**50**
	F1-Measure	29.96	29	24.71	31
	F2-Measure	44.39	**62**	42.66	**73**
	False Positive Rate	46.69	**62**	83.77	81

Рисунок 2.2 – Сравнение систем оценки CVSS и Microsoft

На рисунке 2.3 представлено сравнение систем оценки CVSS и Microsoft для Windows 7, которые тоже имеют существенные различия.

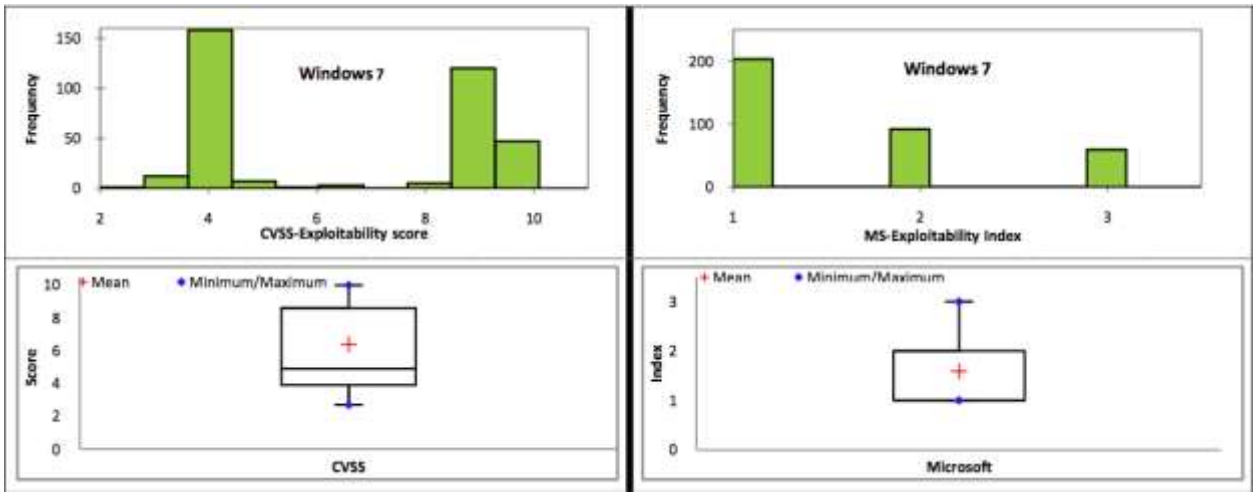


Рисунок 2.3 – Сравнение систем оценки CVSS и Microsoft для Windows 7

Отметим, что представители Open Bug Bounty заявили в 2018 г. о начале перехода на стандарт ISO 29147:2014, утвержденный ISO (International Organization for Standardization), в котором задокументированы нормы, правила и рекомендации по публикации информации об обнаруженных уязвимостях[100].

2.2.5 Проблемы моделирования угроз ИБ для СлПО

Проблемам моделирования УБИ, прежде всего в АСУ и АСУТП в СлПО на объектах ТЭК, уделяется достаточное внимание (работы Липатникова В.А. [123] – [125]). В частности, в работе [122] рассмотрены вопросы обеспечения ИБ в

100 https://www.securitylab.ru/news/491712.php

АСУ предприятий ТЭК. Предложена оригинальная методология построения модели угроз и приведена схема алгоритма формирования модели УБИ в АСУ ТП для объектов ТЭК. В работе [65] систематизированы наиболее характерные внутренние производственные, технические и финансовые риски, имеющие место в работе предприятий ТЭК. С учетом того, что в настоящее время риск кибернетических атак значительно возрос и современные компьютерные вирусы способны вывести из строя практически любые объекты, этот сценарий может привести к катастрофическим последствиям.

Отметим, что производители не всегда уделяют должное внимание безопасности АСУ ТП. Из-за требования обеспечения непрерывности технологических процессов базовые компоненты СУ (протоколы, ОС, СУБД) не обновляются годами и эти факторы в совокупности приводят к развитию новых угроз. В частности, в 2016 г. было опубликовано более 100 уязвимостей в компонентах АСУ ТП основных производителей и больше всего их найдено в продуктах Siemens, Advantech, Schneider Electric и Moxa[101]. Основная доля опубликованных уязвимостей имеет критическую и высокую степень риска (свыше 60%), наиболее распространенные из них: «удаленное выполнение кода» и «отказ в обслуживании». При этом большая часть уязвимостей приходится на устройства диспетчеризации и мониторинга (SCADA). В целом предложения в указанных выше публикациях, наряду с докладами на конференциях («Комплексная защита информации»[102], «Код Информационной безопасности»[103], «InfoSecurity Russia»[104] др.) имеют хорошую проработку.

Настройки по умолчанию многих систем SCADA рекомендуют обеспечивать анонимный доступ к DCOM в Microsoft Windows, что порождает бреши в безопасности. Также многие промышленные протоколы по ряду причин (сложность реализации на оборудовании телеметрии, увеличение объема трафика) не поддерживают шифрование[105]. В работе «SCADA под прицелом:

---

101 https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-rus.pdf
102 http://kzi.su/
103 http://codeib.ru/program
104 http://www.infosecurityrussia.ru
105 https://xakep.ru/2011/08/09/56432/

анализ защищенности АСУТП» (еще в 2011 г.) отмечается, что в существующей нормативной базе нет ясных требований к таким критически важным системам как АСУ ТП и, в частности, SCADA. Требования по защите от НСД, согласно ФСТЭК России, не учитывали множество вопросов, таких как сигнализация попыток нарушения защиты, контроль доступа субъектов к программам, узлам сети, каналам связи и пр. [85], [86]

2.2.6 Проблемы управления рисками в СлПО

Как было показано выше, в отношении определения актуальности УБИ в настоящее время существует весьма обширная практика, прежде всего, ФСТЭК ([142] – [145], [169], [211]) и ФСБ ([129]). В то же время необходимо признать, что этот подход не является единственным эффективным средством противодействия ВПВ. Очевидно, что наибольшее внимание следует уделять вопросам применения современных риск-ориентированных стандартов, прежде всего: ISO (ISO/IEC) серии 27001, 55001, 20000, 22301 ([317], [321], [323], [315]). Данные стандарты по сложившейся практике являются национальными стандартами, соответственно, ГОСТ Р ИСО (ГОСТ Р ИСО/МЭК) ([22], [30], [34]). Кроме того, отметим практику применения отраслевых стандартов: СТО БР ИББС (Банка России) [217] – [220] и СТО ПАО «Газпром» [221] – [229]. Важно принять во внимание, что в РФ некоторые промышленные сообщества (например, «Интер РАО»[106]) создают свои отраслевые системы и «переводят» их в ГОСТ, пройдя формальную процедуру экспертизы.

Примером могут служить два стандарта, разработанные ОАО "ВНИИС":

- ГОСТ Р 54336-2011 Системы экологического менеджмента в организациях, выпускающих нанопродукцию. Требования;
- ГОСТ Р 54338-2011 Системы менеджмента качества в организациях, выпускающих нанопродукцию. Требования.

В последнее время в публикациях на тему обеспечения безопасности СлПО недостаточное внимание уделяется вопросу управления рисками на всех фазах ЖЦ. Заметим, что большинство публикаций и докладов на научно-практических

[106] https://www.securitylab.ru/blog/personal/plutsik/343983.php?R=1

конференциях (Минск, Астана, Уфа, Москва, Санкт-Петербург) относятся, в соответствии с известным циклом PDCA, к области «*Chec*k» и, отчасти, «*Act*». При этом единичные публикации (например, работы Зикратова И.А. [59], [60]) освещали решение практических задач в фазе «*Plan*», а применение риск-ориентированных стандартов по всем фазам ЖЦ СлПО остается недостаточно раскрытым ([317], [311], [323]).

Новые вызовы для применения риск-ориентированных стандартов

В условиях экономического кризиса всегда наблюдается повышенное внимание к проблеме управляемого сокращения издержек, которое в ситуации уменьшения спроса может предотвратить значительное падение прибыли. Таким образом, растет «чувствительность» ЛПР к любым проявлениям неожиданных и незапланированных потерь. Сокращение потерь достигается за счет комплексного управления рисками (работы Кустова В.Н. [74] – [76]).

В статье В. Щербины [258] показано, что предыдущие версии (не риск-ориентированные стандарты) имеют ряд недостатков. В новых редакциях указанных выше стандартов ISO сказано, что управление рисками должно осуществляться комплексно на всем предприятии, затрагивая различные области его деятельности. Достаточно интересный подход предложен в обзоре, посвященном новым европейским требованиям по формированию ИТ-компетенций – European e-Competence Framework 3.0 [69]. Четкая иерархия требований, фокус на постоянное обучение, в том числе, в области безопасности – все это может поддержать обеспечение экономически эффективной комплексной безопасности СлПО, поскольку вариант «локального» противодействия неприменим.

Современный риск-ориентированный подход ISO 31000

Согласно ГОСТ Р ИСО 31000 [33] термин «Риск» означает «*влияние неопределенности на цели*», при этом в примечаниях уточняется, что:

- влияние может быть положительное и/или отрицательное;
- цели организации могут иметь различные аспекты (например, финансовые, вопросы безопасности, экологические и т.д.);

– риск выражается комбинацией последствий событий и вероятностью их наступления.

ГОСТ Р ИСО 31000 также содержит схему процесса управления рисками, которая отражает замкнутый цикл, состоящий из основных процедур или этапов, таких как определение контекста («ситуации»), оценка риска, обработка («воздействие на риск»), мониторинг и пересмотр, обмен информацией и консультирование (см. рисунок 2.4). Отметим, что серия стандартов 31000 непрерывно совершенствуется, например в 2018 г. вышел новый стандарт BS 31111:2018. Cyber risk and resilience. Guidance for the governing body and executive management[107].

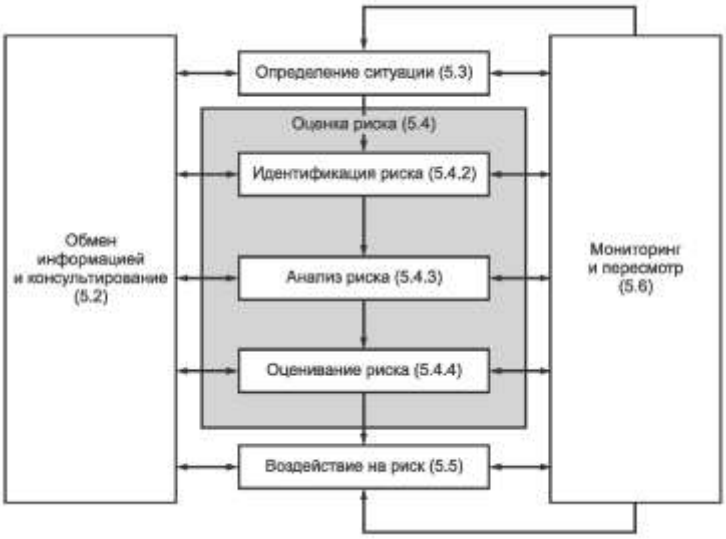


Рисунок 2.4 – Процесс управления рисками согласно ГОСТ Р ИСО 31000

Цель идентификации рисков – определить, что вызывает потенциальный ущерб, место и причину возможного ущерба, в частности:

– активы предприятия;
– угрозы и уязвимости, которые могут быть использованы и их последствия;
– существующие или запланированные защитные меры.

Современный риск-ориентированный подход NIST

Современный риск-ориентированный подход NIST представлен в одном из наиболее удачных и широко применяемом на практике стандарте NIST SP 800-

[107] https://shop.bsigroup.com/ProductDetail?pid=000000000030342527https://cloudblogs.microsoft.com/microsoftsecure/2018/04/04/announcing-new-british-standard-for-cyber-risk-and-resilience/

53[108]. Общая схема процесса оценки рисков представлена на рисунке 2.5. Обратим внимание на четкость и ясную выраженную последовательность каждого этапа в процессе оценки рисков.

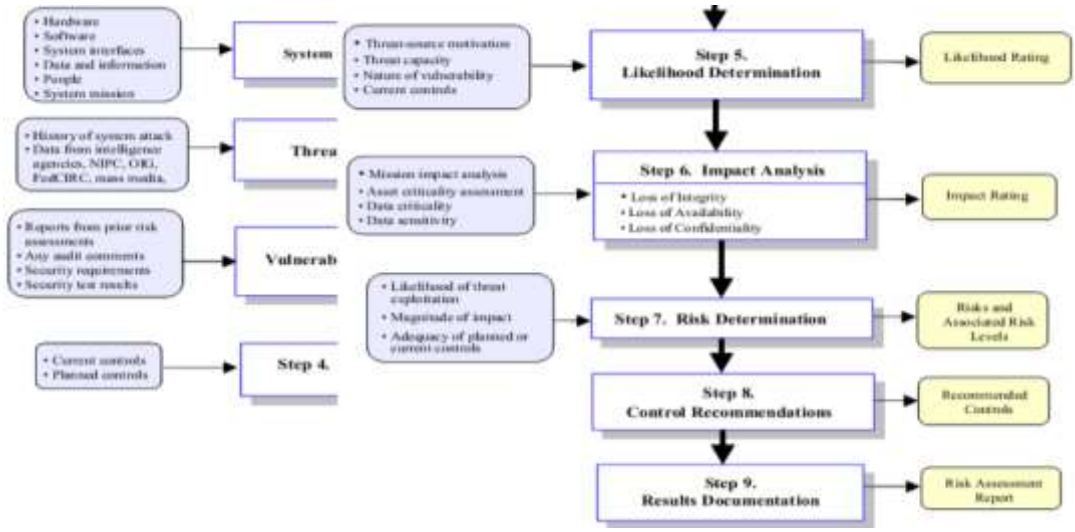


Рисунок 2.5 – Процесс управления рисками согласно NIST SP 800-53

Современный риск-ориентированный подход OCTAVE

Методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) подразумевает активное участие владельцев процессов (*stakeholders*) при определении наиболее незащищённых активов и наиболее вероятных рисков[109] (см. рисунок 2.6).

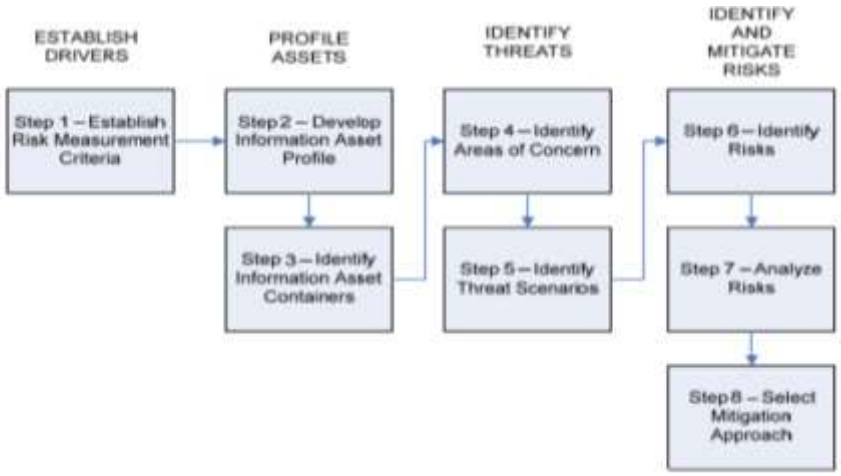


Рисунок 2.6 – Процесс управления рисками согласно OCTAVE

OCTAVE предлагает 3 фазы анализа рисков и логика процесса оценки рисков заключается в выполнении этапов только сотрудниками предприятия без

108 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/Nist.SP.800-53r4.pdf

109 http://www.science-education.ru/ru/article/view?id=12197

помощи внешних консультантов, что снижает риски утечки «чувствительной информации».

Современный риск-ориентированный подход FAIR

Рассмотрим подход к оценке рисков FIRE, предложенный The European Union Agency for Network and Information Security (ENISA)[110], который предоставляет качественные оценки рисков, удобные только для первого быстрого высокоуровнего анализа (см. рисунок 2.7).

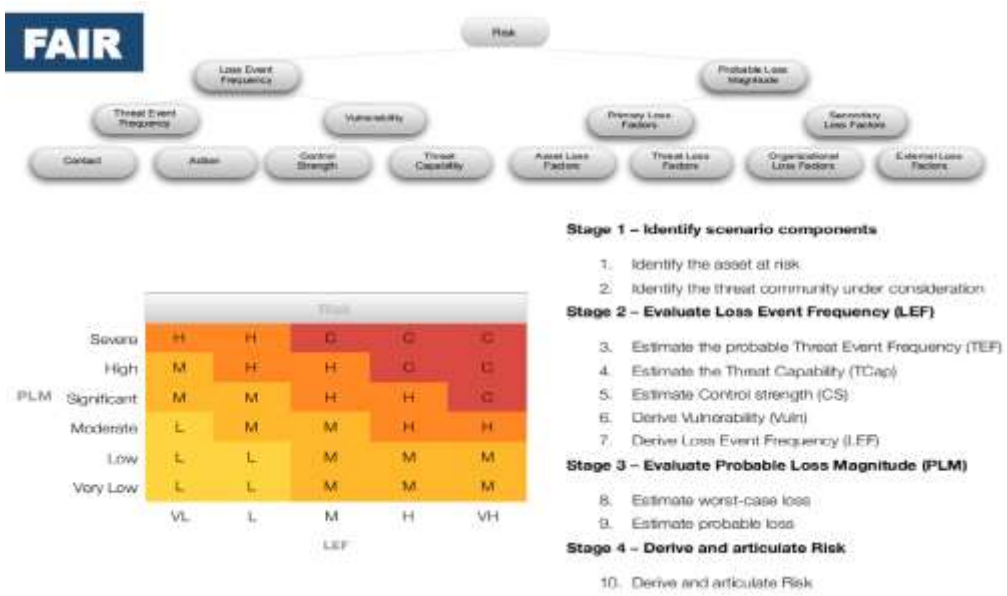


Рисунок 2.7 – Процесс управления рисками согласно FAIR

Далее в таблице 2.4 приведен сравнительный анализ различных стандартов и методов оценки рисков в части идентификации активов. Сравнительный анализ различных стандартов и методов оценки рисков представлен в таблице 2.5 уже в части процедуры анализа рисков. В ГОСТ Р ИСО 31000 представлены варианты обработки рисков: снижение, сохранение, избежание и передача (метод «4Т») [141]. В настоящее время внимание к риск-ориентированному подходу уже не является «областью интересов» только аудиторов. Эта проблема получает поддержку на уровне Правительства РФ, о чем свидетельствует поручение вице-премьера Игоря Шувалова[111].

110 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

111 http://open.gov.ru/events/5511232/

Таблица 2.4 – Сравнительный анализ стандартов и методов идентификации активов

Стандарт / метод	**Типы активов**										**Проводимые мероприятия**						
	Информация	Бизнес-процессы	Технические средства	Программное обеспечение	Каналы и сети	Персонал	Помещения	Организационная структура	Обеспечивающие системы	Третьи стороны	Интервьюирование	Опросные листы	Анализ документации	Физический осмотр	Анализ инцидентов	Использование инструментальных средств	Мозговой штурм
ISO/IEC серий 27000 и 31000	+	+	+	+	+	+	+	+	–	–	+	+	+	+	+	+	–
NIST SP 800 серии	+	+	+	+	+	+	–	–	–	–	+	+	+	–	+	+	–
РС БР ИББС-2.2-2009	+	+	+	+	+	–	+	–	–	–	+	+	–	–	–	–	–
Р Газпром 4.2-3-003-2015	+	+	+	+	–	–	–	–	–	–	+	+	+	+	+	+	–
MAGERIT	+	+	+	+	+	+	+	–	+	+	+	+	–	–	+	–	+
EBIOS	+	–	+	+	+	+	+	–	–	+	+	+	+	+	–	+	–
PCI DSS	+	+	+	+	+	+	–	–	–	–	+	+	–	–	+	–	–
OCTAVE	+	–	+	+	+	+	+	–	–	–	+	+	–	–	–	+	+
CRAMM	+	+	+	+	–	+	–	–	–	–	+	+	–	–	–	–	–
ГРИФ	+	+	+	+	+	+	–	+	–	–	+	+	–	–	–	–	–
RiskWatch	+	–	+	+	+	+	–	–	–	–	+	+	–	–	+	+	–
Microsoft	+	–	+	+	+	–	–	–	–	–	+	+	–	–	–	+	–

Таблица 2.5 – Сравнительный анализ стандартов и методов анализа рисков

Стандарт / метод	**Виды оценки**		**Оценка вероятности события**								**Категории последствий**					
			Параметры			**Учитываемые факторы**										
	Качественная	Количественная	Вероятность	Частота	Актуальность	Мотивация источника угроз	Возможности источника угроз	Осведомленность	Уязвимости	Реализованные защитные меры	Прямые материальные	Косвенные	Правовые	Репутационные	Ущерб жизни и здоровью	Ущерб окружающей среде
ISO/IEC серий 27000 и 31000	+	+	+	–	–	+	+	–	+	+	+	+	+	+	+	+
NIST SP 800 серии	+	+	+	–	–	+	+	–	+	+	+	+	–	+	+	–
РС БР ИББС-2.2-2009	+	+	+	–	–	+	+	–	–	+	+	+	+	+	–	–
Р Газпром 4.2-3-003-2015	+	+	+	–	–	+	+	+	+	+	+	+	+	+	+	+
BSI-Standard 100-3	+	–	–	–	+	–	–	–	–	+	–	–	–	–	–	–
MAGERIT	+	–	+	+	–	–	–	–	–	+	+	+	+	+	+	+
EBIOS	+	–	+	–	–	+	+	–	+	+	+	+	–	–	–	–
PCI DSS	+	+	+	–	–	+	+	–	+	+	+	–	–	–	–	–
OCTAVE	+	–	+	–	–	+	–	–	+	+	+	+	+	+	+	–
CRAMM	+	+	–	+	–	–	–	–	+	+	+	+	+	+	+	–
ГРИФ	+	+	+	–	–	–	–	–	+	+	+	–	–	–	–	–
RiskWatch	–	+	–	+	–	–	–	–	+	+	+	+	–	+	+	–
Microsoft	+	+	–	+	–	–	–	–	+	+	+	+	+	+	–	–

2.2.7 Современный риск-ориентированный подход IATA

Интегрированная система управления риском ICAO Doc 9859

В документах IATA представлены нормативы для создания интегрированной системы управления рисками. В частности, документ ICAO Doc 9859[112] описывает структуру Руководства по управлению безопасности полетов (РУБП) и устанавливает следующие определения и требования:

– «Риск» (п. 6.3.2);

– «Оценка риска» (п. 6.3.3);

– «Интегрированная система управления риском» (п. 9.2.10).

Оценка рисков по требованиям ICAO Doc 9859

В РУБП (Doc 9859 AN/460) введено определение «*безопасности*», и в соответствии с положениями РУБП государства должны требовать от предприятий внедрения систем управления БП (СУБП). Такие СУБП должны, как минимум, выявлять фактические и потенциальные угрозы безопасности, способствовать принятию мер по уменьшению факторов риска.

Рассмотрим процесс оценки рисков в соответствии с требованиями ИКАО Doc 9859 AN/460. В таблице 2.6 представлена шкала вероятностей, в таблице 2.7 представлена шкала серьезности (степени тяжести последствий).

Таблица 2.6 – Вероятность (возможность) наступления события

Цифра	**Характеристика**	**Описание характеристики при постоянном производстве полетов обслуживании ВС**
5	часто	может происходить многократно: каждые 2-3 полета или обслуживания ВС
4	периодически	может происходить время от времени: 2-3 раза в неделю ÷ месяц
3	редко	может произойти, но вероятность небольшая: 1 раз в месяц ÷ год
2	маловероятно	очень малая вероятность события, но такие события бывали в прошлом при выполнении полетов или обслуживании ВС
1	Практически невозможно	Вероятность события крайне мала (согласно стандартов RTCA $P = 5 \times 10^{-9}$)

112 http://www.icao.int/safety/SafetyManagement/Documents/Doc.9859.3rd%20Edition.alltext.en.pdf

Таблица 2.7 – Серьезность (степень тяжести последствий)

Буква	**Характеристика события**	**Описание характеристики при постоянном производстве полетов / техническом обслуживании / наземном обслуживании ВС**
A	Катастрофическое	Разрушение ВС, многочисленные человеческие жертвы
B	Опасное	Серьезное уменьшение “запаса прочности”. Серьезные травмы или смерть большого числа людей. Крупные повреждения ВС или его оборудования
C	Значительное	Существенное уменьшение “запаса прочности”. Серьезный инцидент. Телесные повреждения людей
D	Незначительное	Помехи. Эксплуатационные ограничения. Использование аварийных процедур. Незначительный инцидент
E	Ничтожное	Малозначительные последствия: дополнительное ТО и НО ВС, отмена или задержка вылета, повторный заход на посадку и т.п.

Соответственно, оценка рисков в соответствии с требованиями ИКАО Doc 9859 выполняется по матрице (см. рисунок 2.8):

Вероятность (частота) наступления события	Серьезность – характеристика возможных неблагоприятных последствий				
	A Катастрофич	**B** Опасная	**C** Значительная	**D** Незначитель-ная	**E** Ничтожная
5 часто	5A	5B	5C	5D	5E
4 периодически	4A	4B	4C	4D	4E
3 маловероятно	3A	3B	3C	3D	3E
2 незначительная	2A	2B	2C	2D	2E
1 ничтожная	1A	1B	1C	1D	1E

Рисунок 2.8 – Матрица оценки рисков в соответствии с Doc 9859

Модель Ризона

В области управления безопасностью полетов известна модель концепции авиационных происшествий, разработанная проф. Джеймсом Ризоном[113]. Эта концепция дает в простой графической форме оценку направления функционирования сложного объекта (не только авиационного) – в область

[113] http://docs.cntd.ru/document/1200107984

устойчивого функционирования или в область аварий (сбоев). Например, для анализа авиационного происшествия необходимо оценить одновременное воздействие нескольких факторов (см. рисунок 2.9). При этом подразумевается, что воздействия одного фактора недостаточно для нарушения системы защиты и появления ущерба. Важным преимуществом концепции Дж. Ризона является учет явных и скрытых (латентных) факторов, что крайне важно и для обеспечения требуемого уровня ИБ в СлПО.

Рисунок 2.9 – Модель Джеймса Ризона для оценки рисков

В качестве примера необходимости тщательного анализа рассмотрим исследование результатов аварии разгонного блока «Фрегат»[114] в 2017 г. Проявились проблемы, не встречавшиеся ранее: сочетание азимута стартового стола с азимутами стрельбы ракеты-носителя и разгонного блока выявило ошибку (угол рассогласования «Фрегата» должен был составить 349 градусов, а достиг лишь 10 градусов). При расследовании комиссия обратила внимание на факт, что ОКР по «Фрегату» были начаты в 1998 г. и тогда же был разработан алгоритм работы разгонного блока, который ни разу не корректировался.

В докладе проф. Д. Кэмпбелла (конференция IT-QM-IS, Нальчик, 2016 г.) даны примеры метрик в системах управления рисками (см. рисунок 2.10).

114 https://www.kommersant.ru/doc/3494314

Category	Indicators
LOC-I: Loss of control - inflight	• Stick shaker • Increased roll attitude or rate • High pitch angle • Overspeed (vertical or configuration) • Failure of primary flight instruments
CFIT: Controlled flight into or toward terrain	• EGPWS hard warnings • Descent below MSA • Navigation errors
RE: Runway excursion	• Abnormal runway contact • Loss of control on ground • Long or fast landings • Occurrences with crosswind conditions • High speed rejected take-offs • ATA32 related occurrences

Рисунок 2.10 – Примеры численных метрик для оценки рисков

Метод упреждающего управления безопасностью

В работе Г.Н. Матвеева «Метод упреждающего управления безопасностью полетов воздушных судов в авиационных предприятиях» приводится пример классов событий, которые могут затрагивать 3 аспекта: людей, отказы и имущество (см. рисунок 2.11).

КЛАСС СОБЫТИЙ	АСПЕКТЫ, НА КОТОРЫЕ ОКАЗЫВАЕТСЯ ВЛИЯНИЕ		
	Люди	Отказы нарушения отклонения	Имущество
1	Легкие травмы	Не влияющее на БП	Легкие повреждения
2	Незначительные травмы	Усложнение условий полета	Незначительные повреждения
3	Значительные травмы	Сложная ситуация	Значительные повреждения
4	Единичный смертельный случай	Аварийная ситуация	Обширные повреждения
5	Многочисленные смертельные случаи	Катастрофическая ситуация	Крупные повреждения

Рисунок 2.11 – Аспекты влияния метода упреждающего управления

Однако, в работе Г.Н. Матвеева подчеркивается, что понятие вероятности появления риска – недопустимо. Также введено понятие риска 1-го рода μR_1,

применяемое при описании единичного риска, ведущего к отказу – как индикаторная или частотная мера.

$$\mu R_1 = PR \text{ или } \mu = f(\{\mu R_1, HR \mid \sum 0\})$$

где:

PR – вероятность ущерба,

HR – значение ущерба

Предложено формировать интегральный показатель вида:

$$S(\%) = (1 - Н_{ууп} * К_{ууп} + Н_{сс} * К_{сс} + Н_{ас} * К_{ас}) / Н$$

где:

Н – число событий типа возникновения особых ситуаций (УУП, АА, АС),

К – коэффициент доли влияния каждого вида событий особой ситуации.

Важно, что в отрасли каждому событию присваивают экспертный (весьма субъективный фактор) коэффициент опасности:

$К_{ууп}$ – 1

$К_{сс}$ – 10

$К_{ас}$ – 1000

Метод управления кибербезопасностью Doc 8973/8

В РУБП (Doc 8973/8 ICAO) в Главе 18 отмечаются требования защиты критических авиационных систем, ИС и связанных технологий, например:

– Эксплуатанты авиационной техники должны определить КИИ (п. 18.1.2);

– Защита КИИ должна включаться в процессы оценки угроз (п. 18.1.7);

– Эксплуатанты должны установить меры снижения риска (п. 18.1.8).

Методы категорирования и прогнозирования рисков СлПО

В работе А.И. Костогрызова «Научно-методические основы для прогнозирования рисков, обоснования уровней допустимых рисков и обеспечения комплексной безопасности критически важных объектов и систем» приводится сопоставление моделей и выводы по их использованию (см. таблицу 2.8).

Таблица 2.8 – Сравнение моделей для прогнозирования рисков (фрагмент)

Сравниваемые модели	Выводы по использованию для прогнозирования рисков
ГОСТ Р ИСО серии 9000 и ГОСТ Р ИСО серии 15288	▪ рекомендации к управлению рисками даны на уровне требований и вербальных моделей, ▪ возможно использование на уровне принципов.
ГОСТ Р ИСО серии 31000	▪ рекомендации даны на уровне требований к экспертным и формализованным моделям, в т.ч. ▪ вероятностным. Даны ссылки на модели, опубликованные в научно-технической литературе, ▪ возможно использование различных моделей.
ГОСТ 27.301 «Основные положения по расчету надежности» и ГОСТ Р 51901 «Управление надежностью. Анализ риска технологических систем»	▪ к качественным методам относят: метод анализа опасности и работоспособности, метод «что будет, если…?» и др., ▪ к количественным показателям рисков отнесены частота возникновения угроз (по травматизму, аварийным ситуациям и пр.), вероятность отказа в течение заданного периода прогноза. Рекомендуемые модели не содержат рекомендаций по учету мер контроля и мониторинга.
Методы SWOT анализа	▪ экспертная оценка сильных и слабых сторон, возможностей и угроз, ▪ высокая степень субъективности.
РД 08-120-96 и РД 03-418-2001	▪ изложены общие указания по мерам обеспечения безопасности, порядку анализа рисков, ▪ разработка или выбор конкретных моделей прогнозирования рисков отдан на откуп экспертам.

Некоторые методики категорирования КВО представлены О. Паниным в работе «Категорирование объектов для создания эффективных систем физической защиты»[115]:

— Методика категорирования опасных производственных объектов (представлена ФГУП «НТЦ «Промышленная безопасность»);

— Методика общегосударственного категорирования объектов (представлена «НПП «ИСТА-Системс»).

В работе А. Бояринцева, А. Бражника и А. Зуева «Проблемы антитеррористического: Категорирование и анализ уязвимости объектов»[116]

[115] http://mx1.algoritm.org/arch/70/70_5.pdf

[116] http://kurganobl.ru/assets/files/terrorizm/zaschischennost_obektov_promyshlennosti_i_energetiki.pdf

рассматриваются подходы к определению компонента ущерба. Для этого предложено пользоваться существующими методическими рекомендациями по оценке ущерба от ЧС природного и техногенного характера, например:

— «Классификация ЧС природного и техногенного характера» (утв. постановлением Правительства № 1094 от 13.09.1996 г.).

— «Методические рекомендации по оценке ущерба от аварий на опасных производственных объектах» (РД 03–496-02, утв. Постановлением Госгортехнадзора России № 63 от 29.10.2002 г.).

— «Единая межведомственная методика оценки ущерба от ЧС природного, техногенного и террористического характера, а также классификации и учета ЧС» (разраб. ФГУ ВНИИ ГОЧС, утв. приказом МЧС России от 01.12.2004).

Следует иметь в виду, что данные методики предназначены, в первую очередь, для учета и регистрации ЧС по единой системе показателей, т. е. для апостериорных оценок. На этапе прогнозирования последствий ЧС или проектирования СУ точность аналитических оценок будет очень невысока.

Учет факторов, способных оказать влияние на функционирование

Для эффективного управления СлПО, ЛПР должно учитывать множество факторов, способных оказать значительное воздействие на режимы функционирования, например:

- $\boldsymbol{\eta_1}$ – внешние негативные воздействия на СлПО (в том числе, ДД),
- $\boldsymbol{\eta_2}$ – последствия инцидентов ИБ (ремонт или простой компонент АСУТП),
- $\boldsymbol{\eta_3}$ – внутренние события, например, невыполнение мероприятий ИБ,
- $\boldsymbol{\eta_4}$ – непредвиденные события, например, отказ в обслуживании и пр.

Математическая модель такого процесса может быть представлена в виде:

$$\mathbf{R_t}\left(\mathbf{PR_j}\right) = \mathbf{f}\left(\boldsymbol{\alpha}^{\boldsymbol{\eta i}}_{\mathbf{PRj}}, \boldsymbol{\eta}_{\mathbf{i}}(\mathbf{PR_j})\right)$$

где:

- $R_t\,(PR_j)$ – совокупное влияние множества факторов $\boldsymbol{\eta_i}$ на процесс PR_j,
- $\eta_i\,(PR_j)$ – воздействие фактора $\boldsymbol{\eta_i}$ на процесс ИБ PR_j,
- $\alpha^{\eta i}_{PRj}$ – весовой коэффициент воздействия фактора $\boldsymbol{\eta_i}$ на процесс ИБ PR_j

Тогда с учетом требований обеспечения безопасности СлПО на всех этапах ЖЦ можно определить влияние конкретных факторов для аудита каждого процесса ИБ в СМИБ (ИСМ). Пример размещения влияния факторов ($\boldsymbol{\eta_1 - \eta_m}$) с учетом известных процессов ($PR_1 - PR_m$) применительно к фазам цикла PDCA показан в таблице 2.9.

Таблица 2.9 – Влияние факторов для аудита процессов ИБ по фазам PDCA

Фактор	**Фаза PDCA (перечень процессов)**			
	PR_1	**PR_2**	**…**	**PR_m**
η_1	η_1 (PR_1)	η_1 (PR_2)		η_1 (PR_m)
η_2	η_2 (PR_1)	η_2 (PR_2)		η_2 (PR_m)
…	…	…	…	…
η_n	η_n (PR_1)	η_n (PR_2)		η_n (PR_m)

Отметим, что определение $\alpha_{PRj}^{\eta i}$ может выполняться по классическому методу МАИ (Т.Саати) или по модифицированным методам на базе МАИ, например, на основе разработанной модели СМИБ, ранее предложенной автором. Для эффективного управления рисками ИБ необходимо обеспечить поддержку ЛПР внешними заинтересованными сторонами с целью выявления, идентификации, управления и контроля событий ИБ, потенциально способных повлиять на достижение целей организации.

Рекомендации по управлению рисками СлПО в цикле PDCA

Управление рисками – это процесс, осуществляемый на предприятии коллегиальным органом из состава высшего руководства, экспертов, внешних и внутренних заинтересованных сторон с целью выявления, идентификации, управления и контроля событий, потенциально способных повлиять на достижение целей организации.

Пример реализации процесса управления рисками для одной ключевой фазы «Plan» цикла PDCA показан на рисунке 2.12. В предлагаемом подходе учтены все основные сущности: формирование внутренних и внешних аспектов, формирование контекста, формирование системы менеджмента рисков предприятия и основных типов документированной информации – критериев рисков, шкалы оценки, файла рисков, плана обработки рисков.

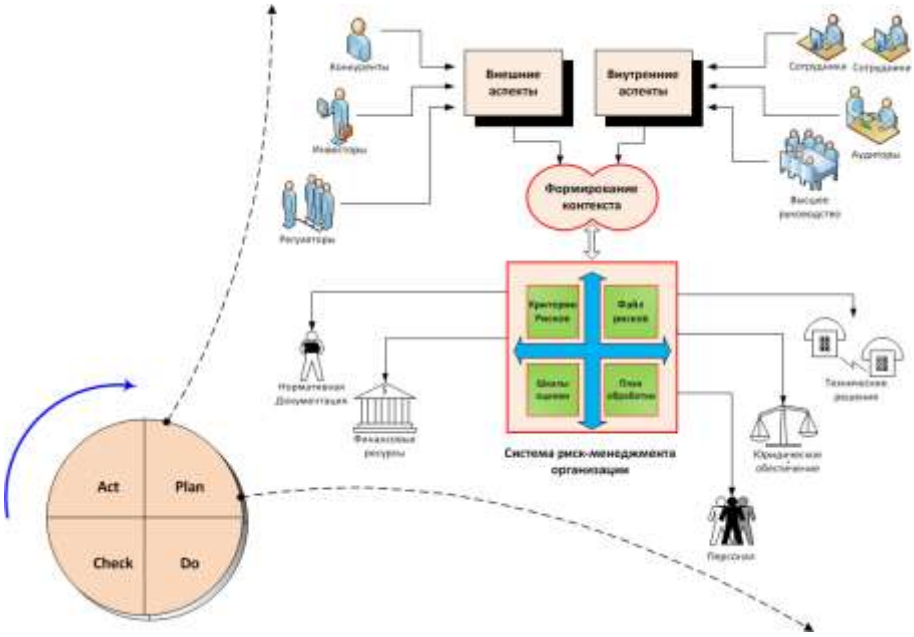


Рисунок 2.12 – Процесс управления рисками для фазы «Plan» цикла PDCA

В качестве аналогичного подхода, предложенного в 2017 г., можно рассмотреть подход Lloyd's of London[117]. В частности, в отчете «Emerging Risks Report 2017 Technology» показано, что общий размер потерь от глобальной кибератаки, способной лишить бизнес доступа к информации в облачных хранилищах, может превысить 121 млрд. долл. При этом отмечается, что даже потери от самого разрушительного в истории торнадо «Катрины» составили лишь около 108 млрд. долларов.

Задачи системы менеджмента рисков для СлПО можно расположить в порядке реализации цикла PDCA ([91], [339] – [349]):

1) «P» (*Plan*) – формирование нормативной базы, разработка регламентов, паспортов риска, определение шкалы оценки рисков, критериев принятия рисков, формирование сводной карта рисков для предприятия;
2) «D» (*Do*) – разработка комплекса мероприятий по снижению вероятности (ослаблению последствий) при возникновении рисков;
3) «C» (*Check*) – контроль полноты, своевременности и эффективности реализации комплекса мероприятий по управлению рисками предприятия;

117 https://www.lloyds.com/news-and-insight/risk-insight/library/technology/countingthecost

4) «A» (*Act*) – анализ результативности комплекса мероприятий по управлению рисками на уровне ЛПР и формирование управленческих решений для оптимизации СМ рисков предприятия.

Следующий важный вопрос касается обеспечения «замыкания» цикла PDCA с учетом предложенного выше риск-ориентированного подхода.

Важно принять во внимание, что СМ рисков формируется именно на фазе «Plan» цикла PDCA во всех типах СМ. Благодаря этому обстоятельству она способна «отработать» не только известные (для самой организации, по информации конкурентов, по данным аналитических служб), но и перспективные риски, реализация которых возможна в будущем.

Представление количественной и качественной оценки рисков СлПО

Рассмотрим примеры наглядного представления результатов качественной и количественной оценки рисков соответственно в виде матрицы оценки рисков (соответственно, см. рисунок 2.13 и рисунок 2.14). Для качественной оценки представлены шкалы: вероятности – от крайне маловероятного до крайне вероятного события наступления риска и последствий реализации событий риска – от несущественного до катастрофического (см. рисунок 2.13).

Вероятность реализации события риска							
	Крайне вероятный		Г-3		Н-4, А-6	С-4	Д-5
	Вероятный		Г-2	А-1		А-3, Б-2	Д-7
	Возможный		Г-1		А-2	Б-1	
	Маловероятный						
	Крайне маловероятный						
		Несущественные	Незначительные	Малые	Средние	Значительные	Катастрофические
	Последствия реализации события риска						

Рисунок 2.13 – Матрица оценки рисков (качественная оценка)

На этом примере показаны разные типы рисков (индексы отражают бизнес-сущности, ответственные за управление каждым конкретным типом риска, например – риски ИТ, риски ИБ, финансовые риски) [78].

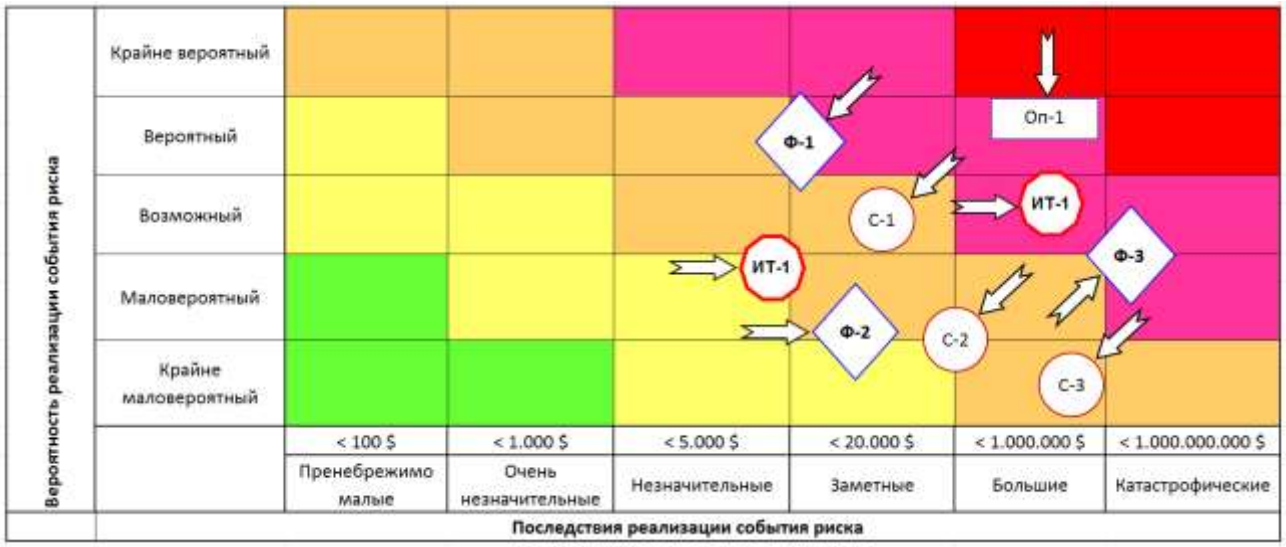


Рисунок 2.14 – Матрица оценки рисков (количественная оценка)

Представляется более полезным предоставлять ЛПР именно количественные (численные) оценки рисков. Для реализации данного решения предлагается принять в качестве методической базы стандарты ([311], [319], [315], [323]), а для оценки последствий использовать данные таблицы С.3 из стандарта ГОСТ Р ИСО/ТО 13569-2007 [22].

Системы управления компании рисками в решениях SAP

На основании специального издания «SAP Security and Risk Management», посвященного проблемам обеспечения ИБ в решениях SAP, представляется возможным отметить ряд принципов и практических решений [354]. Прежде всего, необходимо обратить внимание, что подходы SAP не являются узкоспециализированными, а могут быть применены к различным отраслям и сферам деятельности, например, к электронному документообороту (EDI – Electronic Data Interchange) или построению доверенной третьей стороны (TTP – Third Trusted Part).

В отношении специфических рисков ИБ компания SAP предлагает свой подход, который характеризуется определением целей (IT-Security Objectives). Структура целей обеспечения ИБ представлена на рисунке 2.15. На конференции «Цифровой инфофорум 2017» в докладе «Взгляд SAP на безопасность цифровой экономики» представлены системы управления стандартами и передовые практики безопасности SAP (см. рисунок 2.16).

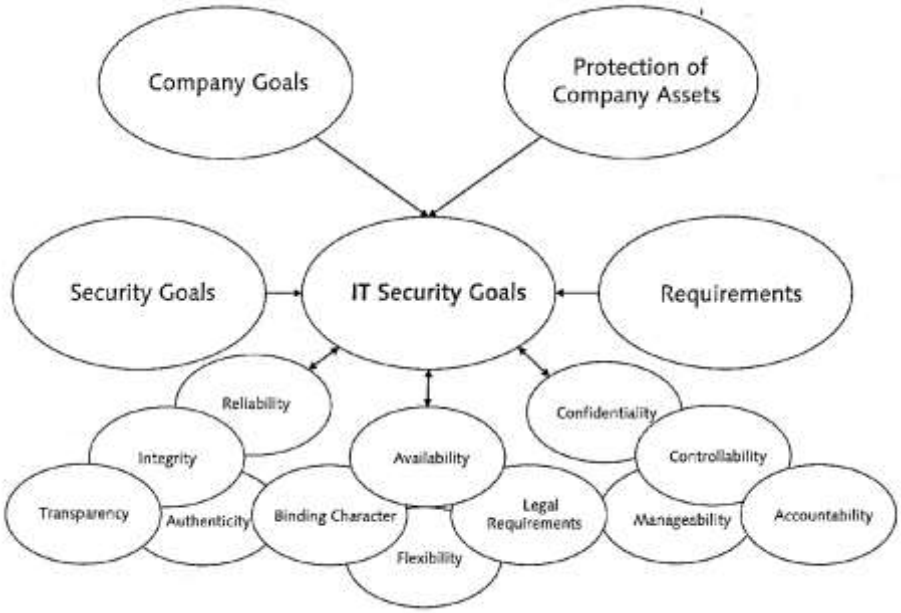


Рисунок 2.15 – Цели обеспечения ИБ

Обратим внимание на значительный перечень стандартов ISO.

Рисунок 2.16 – Системы управления стандартами безопасности в SAP

Рассмотрим декларируемый перечень требований стандартов и методик:

1. SOX – Sarbanes-Oxley Act, особо отмечены секции 302 (ответственность), 402 (внутренний контроль), 404 (управление измерениями), Form 20 (NDA).
2. REACh (стандарт химической промышленности, Финляндия).
3. Basel (стандарт де-факто для финансовой отрасли, в т.ч поддержка ИТ-систем, защита от рисков, осведомленность и управление).
4. COBIT (методика для ИТ-отрасли).
5. ISO (стандарты ИСО различных серий).

6. NIST (стандарты США различных серий).
7. IFRS (стандарт отчетности финансовой отрасли);
8. PIPEDA (стандарта для защиты электронных документов, Канада).
9. ITIL (методика для ИТ-отрасли).
10. COSO (стандарт де-факто для аудита, США).

Системы управления рисками в решениях Yokogawa

В руководстве Yokogawa по системам безопасности [376] указаны основные стандарты безопасности, которыми следует руководствоваться при создании систем промышленной автоматики для объектов ТЭК и, в целом, для СлПО. Это стандарты IEC (МЭК) 61508 и IEC 61511. Стандарты функциональной безопасности IEC 61508, в основном, используется для построения и производства систем безопасности, типа PLC и приборов безопасности, а IEC 61511 обычно используется при построении, запуске и работе со сложными установками. Это направление может иметь определенные перспективы, принимая во внимание, что динамика сертификации по «Общим критериям» в РФ примерно 300 продуктов в год с небольшой вариацией в течение достаточно длительного периода 2006 – 2014 гг. [69].

Также в руководстве [376] содержится важная «привязка» процесса обеспечения ИБ к ЖЦ объекта управления. Вводится понятие «жизненный цикл безопасности» (Safety Life Cycle) – многостадийный процесс, используемый для оценки рисков, связанных с технологическим процессом, определением целевого риска, определением архитектуры и требований к безопасности, ввода в эксплуатацию, работы и технического обслуживания. Применяемые стандарты IEC 61508 и IEC 61511 определяют все виды требований для полного ЖЦ установки от «рождения» до вывода из эксплуатации. В этой связи важно отметить корреляцию с новыми стандартами ISO серии 55001 ([323], [324]), которые содержат требования формирования стратегического плана по управлению активами и иные функциональные требования, применимых к правильному использованию активов. Важный шаг заключается в количественной оценке рисков (применяется только такая методика!) и

определении необходимой степени снижения рисков. Помимо ограничения на применение методов оценки рисков необходимо отметить, что в нотации процессов ЖЦ Yokogawa отсутствуют и методы оценки остаточного риска (которые есть, например, в ISO 27005), что может оказаться критическим фактором при противодействии инцидентам ИБ в СлПО.

2.2.8 Проблемы обеспечения ИБ для СлПО на уровне ОБСЕ

В 2003 г. представлено «Руководство», которое разработано при участии экспертов из Европейского Союза и НАТО, что подчеркивает специальный уровень «*куратора*» данных инициатив [182]. «Руководство» предоставляет структуру для обеспечения управления вопросами кибербезопасности в отношении важнейших объектов неядерной энергетической инфраструктуры на основе комплексного подхода, построенного на рассмотрении рисков, с особым акцентом на готовности к реагированию на инциденты и общей устойчивости инфраструктуры. Отметим, что существуют разные определения «кибертерроризма», которые концентрируются на последствиях, например:

– «*Под кибертерроризмом обычно понимают незаконные атаки и угрозы атаки на компьютеры, сети и на хранящуюся в них информацию в целях устрашения или принуждения государства или его населения и реализации определенных политических или социальных целей*»[118].
– «*Кибертерроризм означает использование инструментов компьютерной сети для нанесения вреда важнейшим объектам национальной инфраструктуры (таких как энергетика, транспорт, государственная деятельность) или прекращения их работы*»[119].

2.3 Проблемы при формировании моделей аудита ИСМ

2.3.1 Актуальные требования для формирования моделей аудита

Обратим внимание, что серия стандартов ISO/IEC «Общие критерии» 15408 ([23] – [25]) не акцентируется на уязвимостях (см. рисунок 2.17).

---

[118] Mehmet Nesip Ogun: Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes, Journal of Applied Security Research (2012), стр. 209
[119] Gabriel Weimann: Cyberterrorism: The Sum of All Fears?: Studies in Conflict & Terrorism, стр. 130

Рисунок 2.17 – Взаимосвязи понятий безопасности ISO/IEC 15408

Эта новация нашла реализацию в новом подходе[120] – «Collaborative Protection Profile» (cPP). В частности, новый подход cPP, в отличие от «классического» подхода «Общих критериев», декларирует следующие решения указанных проблем:

1. Отказ от сертификации на соответствие требованиям заданий по безопасности, которые не декларируют соответствие ни одному из утверждённых профилей защиты.
2. Отказ от использования понятия «оценочный уровень доверия» и понижение требований доверия.
3. Разработка типовых методик проведения испытаний.

В работе Н. Винера отмечен случай, когда «*машина*» явно неисправна ([13], стр. 226). В ряде случаев на нее следует подать «ненормально большой электрический импульс», в надежде, что это запредельное воздействие вернет машину в исходное состояние. Однако, если данный экстремальный способ не дает результата, необходимо предложить надежный способ получения подтверждения того, что «*машина*» - в конкретном случае СМИБ (ИСМ) в СлПО гарантированно находится в одном из определенных состояний.

120 http://s3r.ru/2016/02/novosti/pro-collaborative-protection-profile/

2.3.2 Анализ существующих методик моделирования угроз

Для анализа существующих методик моделирования угроз были выбраны как отечественные, так и зарубежные источники. В зарубежных источниках процесс моделирования угроз является частью процессов по выявлению и оценке рисков. В отечественной практике моделирование угроз является отдельным процессом и, к сожалению, он не всегда связан с рисками ИБ. Даже изменения, вносимые в Постановления Правительства (например, № 676 от 06.07.2015 и № 555 от 11.05.2017), касающиеся требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных ИС, учитывают «статические» требования ФСТЭК и ФСБ[121]. Постановление № 555 требует согласования моделей угроз с ФСТЭК и ФСБ, хотя методику моделирования таких угроз ФСТЭК не приняла (по состоянию на 31.12.2017).

Анализ базовой модели угроз безопасности ПДн ФСТЭК

Базовая модель угроз безопасности ПДн при их обработке в ИСПДн разработана ФСТЭК [5]. Обратим внимание, что есть отдельная Базовая модель угроз для КСИИ [142]. Документ содержит систематизированный перечень угроз безопасности персональных данных (УБПДн) при их обработке в ИСПДн. Данный перечень сформирован на основе факторов и условий, которые создают опасность НСД к ПДн. Соответственно, Базовая модель оперирует только элементами (в которые не включены риски!), например, объект воздействия, уязвимость, источник угрозы.

Анализ модели угроз для УЦ ФСБ

Регулирование вопросов обеспечения ИБ для УЦ осуществляется на основании нормативной базы ФСБ [129], [166]. Для защиты информации ограниченного распространения УЦ применяются стандарты ([34] – [36]), которые введены приказами ФАТРиМ. Принимая во внимание информацию о возможностях нарушителя безопасности информации УЦ в соответствии с методическими документами ФСБ ([129], [166]), необходимо противостоять

---

121 http://lukatsky.blogspot.ru/2017/05/555.html

угрозам, представляющим целенаправленные действия (атаку) с использованием аппаратных и / или программных средств с целью нарушения безопасности защищаемой информации (например):

1. Подготовка и проведение атак извне КЗ.
2. Подготовка и проведение атак на объекты УЦ (например, ЭД).
3. Осуществление создания способов и подготовки атак с привлечением специалистов в области использования недекларированных возможностей (далее – НДВ) прикладного и системного ПО.

На основании возможности реализации перечня угроз могут быть определены УБИ для УЦ (см. таблицу 2.10)

Таблица 2.10 – Актуальные УБИ для УЦ (выборка)

№ п.п.	Угрозы безопасности информации УЦ	Возможность реализации УБИ	Степень возможного ущерба	Актуальность УБИ
1.1	Проведение атаки при нахождении в пределах КЗ	Высокая	Средняя	Актуальная
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ;	Высокая	Низкая	Актуальная
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов, сопровождающих СКЗИ	Высокая	Средняя	Актуальная
4.1	создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак НДВ.	Высокая	Средняя	Актуальная

ФСТЭК КСИИ

Отметим положительную динамику изменений в части обеспеченеия безопасности объектов КИИ в РФ, прежде всего, Приказа ФСТЭК № 239[122] и Приказа ФСТЭК № 235[123]. Например, ст. 18 Приказа ФСТЭК № 235 содежит ссылку на ФЗ-184 в части оценки соответствия применяемых СрЗИ и порядок устранения замечаний, выявленных при внешней оценке (ст. 35).

---

122 http://www.garant.ru/products/ipo/prime/doc/56638278/

123 http://rulaws.ru/acts/Prikaz-FSTEK-Rossii-ot-21.12.2017-N-235/

В документах ФСТЭК КСИИ [142] – [145] рассматривается реализация УБИ только в отношении файлов, определяется вероятность реализации j-й угрозы в отношении r-го файла и возникновение g-го деструктивного действия (ДД), выполняемого в результате реализации УБИ относительно r-го файла. Рассмотрение только УБИ, и только в отношении файлов (например, ОС серверов или АРМ), является недостатком методики ФСТЭК КСИИ, т.к. не позволяет специфицировать риски ИБ по необходимому широкому перечню активов (в частности, как определено в ГОСТ Р ИСО серии 27001). Несмотря на выход в 2009 г. стандарта ISO 31000 и данного стандарта как ГОСТ Р ИСО, дальнейший переход к современным технологиям ИБ так и не был реализован. Этот недостаток частично устранен с выходом приказа ФСТЭК № 31 [235].

Документы ФСТЭК КСИИ содержат особенность, связанную с тем, что практически для каждой УБИ необходимо иметь свою модель расчета. При этом отмечается: «*такие модели в настоящее время отсутствуют, а их разработка представляет собой достаточно длительный процесс*». Соответственно, принимается допущение: относительно r-го файла определяется только вероятность наличия благоприятных условий для реализации j-й угрозы. Отметим еще один недостаток методики ФСТЭК КСИИ – жесткая фиксация «триады» свойств безопасности не соответствует современным требованиям ИБ (например, ISO серии 27001 [32]) и не позволяет расширять свойства ИБ для, например, подотчетности и/или надежности (см. п. 3.4 [32]), что крайне важно при обеспечении шифрования или межсетевой безопасности оборудования (CISCO, Hirschmann, Yokogawa, Siemence) в СлПО.

УБИ реализуются за рассматриваемый период времени t с некоторыми вероятностями, представленными в виде матрицы

$$P^{/}(t) = \left\| p^{/}_{jr}(t) \right\|, j = \overline{1,J}, r = \overline{1,R},$$

где $p^{/}_{jr}(t)$ – вероятность реализации j-й угрозы в отношении r-го файла.

Ущерб от реализации ДД представлен в виде матрицы:

$$D = \left\| d_{rg} \right\|, r = \overline{1,R}, g = \overline{1,G},$$

где d_{rg} – ущерб от реализации g-го деструктивного действия в отношении r-го файла может быть оценен и неприемлемый ущерб D_{np}. Коэффициент опасности j-й угрозы определяется по формуле:

$$\overline{D_j} = \begin{cases} \sum_{r=1}^{R}\sum_{g=1}^{G}\left(\tau_{jg}\cdot\frac{d_{rg}}{D_{np}}\cdot p'_{jr}\right), \text{ если } \sum_{r=1}^{R}\sum_{g=1}^{G}\left(\tau_{jg}\cdot\frac{d_{rg}}{D_{np}}\cdot p'_{jr}\right)<1; \\ 1-\text{в противоположном случае.} \end{cases}.$$

Пример определения актуальности УБИ для АСУ ТП на базе последовательного вычисления вероятности реализации УБИ (Вр), вербальной интерпретации вероятности, коэффициента опасности УБИ (Ко) и вербальной интерпретации опасности представлен в таблице 2.11. Необходимо отметить, что этот фрагмент расчета актуальности УБИ для реального проекта СлПО, выполняемого в течение 2015-2017 гг., в котором владелец каждого r-го файла определил неприемлемый ущерб D_{np}. Именно по этой причине для всех УБИ была подтверждена актуальность.

Таблица 2.11 – Определение актуальности УБИ для АСУ ТП (фрагмент)

Код УБИ	**Вероятность реализации УБИ (Вр)**	**Вербальная интерпретация вероятности**	**Коэффициент опасности УБИ (Ко)**	**Вербальная интерпретация опасности**	**Актуальность УБИ**
УФД2	0,40	Средняя	1	Очень высокая	Актуальная
УФД5	0,40	Средняя	1	Очень высокая	Актуальная
УНД А1	0,40	Средняя	1	Очень высокая	Актуальная
УНД А2.1	0,40	Средняя	1	Очень высокая	Актуальная
УНД А2.3	0,40	Средняя	1	Очень высокая	Актуальная
УНД Б1.2	0,00	Очень низкая	1	Очень высокая	Актуальная
УНД Б2	0,00	Очень низкая	1	Очень высокая	Актуальная
УНД В1	0,40	Средняя	1	Очень высокая	Актуальная
УНД Г1	0,40	Средняя	1	Очень высокая	Актуальная
УУД Б1.2	0,00	Очень низкая	1	Очень высокая	Актуальная
УУД Б2.2	0,86	Очень высокая	1	Очень высокая	Актуальная
УУД Б3.2	0,86	Очень высокая	1	Очень высокая	Актуальная
УУД Б5.1	1,00	Очень высокая	1	Очень высокая	Актуальная
УУД В3	0,40	Средняя	1	Очень высокая	Актуальная
УУД В5.2	0,00	Очень низкая	1	Очень высокая	Актуальная
УУД В10.1	0,86	Очень высокая	1	Очень высокая	Актуальная
УУД В13.1	0,86	Очень высокая	1	Очень высокая	Актуальная
УУД Г.8	1,00	Очень высокая	1	Очень высокая	Актуальная
УУД Г.11	0,86	Очень высокая	1	Очень высокая	Актуальная
УО1	0,86	Очень высокая	1	Очень высокая	Актуальная
УТХ2	0,86	Очень высокая	1	Очень высокая	Актуальная

Анализ РС БР ИББС

В документе РС БР ИББС-2.2-2009 «Обеспечение ИБ организаций банковской системы РФ. Метод оценки рисков нарушения ИБ»[124] учитывает степень возможности реализации угрозы в рамках оценки рисков нарушения ИБ. Для оценки степени вероятности реализации угроз ИБ используется качественная шкала, а риск нарушения ИБ оценивается в количественной (денежной) форме. В целях дополнения рассмотрим материалы, представленные на конференции АКФОРБ[125] (г. Уфа, Национальный Банк Республики Башкортостан, 2016 г.). В частности, в докладе Бондаренко, Тарасова и Горчакова приведена схема сложности управления рисками (см. рисунок 2.18).

Рисунок 2.18 – Сложность управления рисками

Примеры рейтинговой оценки ряда КО БС РФ в системе Moody’s представлены на рисунке 2.19.

---

124 http://www.cbr.ru/credit/Gubzi_docs/st22_09.pdf

125 http://npk.akforb.ru/upload/doc/2015

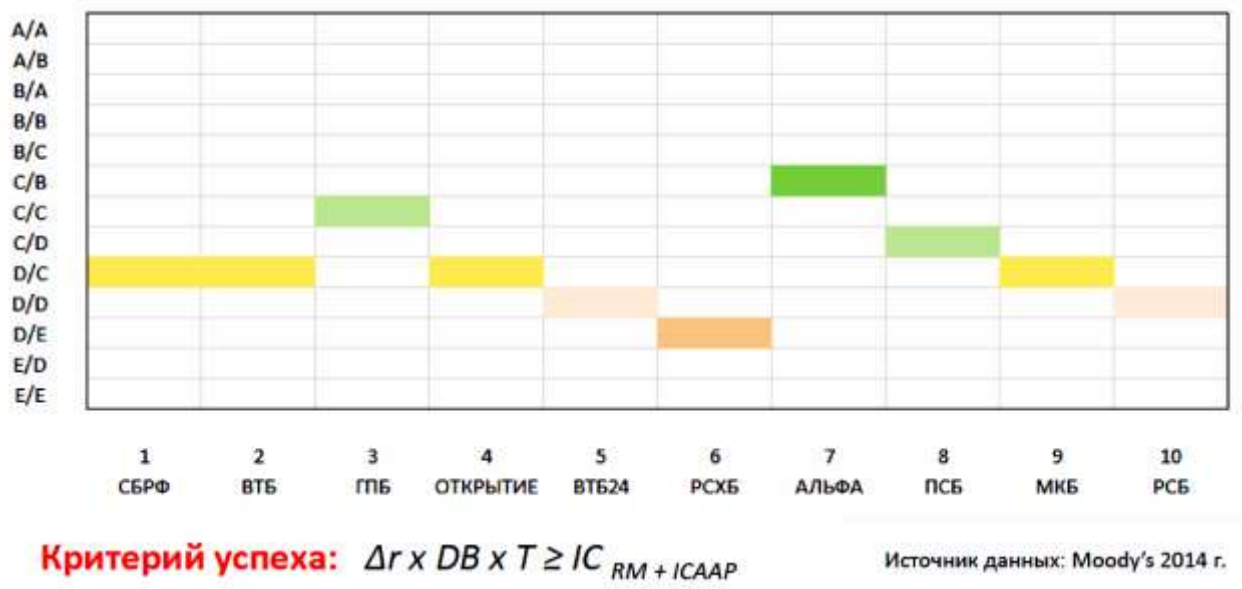


Рисунок 2.19 – Пример расчета критерия успеха при управлении рисками

Анализ модели угроз ПДн, обрабатываемых в ИСПДн отрасли связи

«Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли» (далее – «Модель угроз отрасли связи») подготовлена Министерством связи и массовых коммуникаций РФ для разработки частных моделей УБПДн в отдельных ИСПДн (документ согласован с ФСБ и ФСТЭК в 2010 г.)[126]. В «Модели угроз отрасли связи» описывается модель потенциального нарушителя, а также подход к определению актуальности УБПДн с учетом состава обрабатываемых ПДн и особенностей ИСПДн, для которой разрабатывается модель угроз. Вероятность реализации угрозы определяется экспертным методом и может принимать 4 значения. Оценка опасности УБПДн также носит экспертный характер и может принимать 3 значения. Актуальность УБПДн определяется по матрице расчета, в которой учитываются коэффициент реализуемости угрозы и оценка опасности УБПДн. К сожалению, в «Модели угроз отрасли связи» не рассматриваются риски.

Анализ частной модели угроз ПДн учреждений здравоохранения

В «Методических рекомендациях по составлению частной модели угроз безопасности ПДн учреждений здравоохранения, социальной сферы, труда и

126 http://minsvyaz.ru/common/upload/publication/1410065MC.pdf

занятости» представлен алгоритм построения модели угроз[127]. При определении пользователей ИСПДн составляется матрица доступа, отражающая права каждой категории пользователей ИСПДн. Определение исходного уровня защищенности ИСПДн, вероятности реализации, возможности реализации, опасности и актуальности УБПДн проводится также, как в «Модели угроз отрасли связи».

Анализ СТО Газпром 4.2-0-004-2009

В соответствии с СТО Газпром 4.2-0-004-2009, угроза ИБ реализуется так же, как и Базовой модели ФСТЭК России [5], в результате образования канала реализации между источником угрозы и носителем информации, что создает необходимые условия для нарушения ее безопасности (ДД). Источники угроз ИБ делятся на внутренние и внешние. Источник угроз относится к внешнему, если в ходе реализации угрозы он располагается за пределами контролируемой зоны (КЗ), и к внутреннему, если он находится в пределах КЗ. В зависимости от способа реализации возможностей ДД на критически важную информацию и используемых при этом средств, выделяется 3 класса угроз:

- угрозы специальных воздействий на защищаемую информацию в целях ее уничтожения, искажения и блокирования;
- угрозы утечки информации по техническим каналам;
- угрозы, связанные с НСД к информации в ИС.

В результате реализации УБИ может быть нарушена конфиденциальность (утечка, разглашение), целостность (модификация) и доступность (блокирование) информации. Отметим, что нарушение целостности и / или доступности информации в ИС может привести к нарушению своевременности подачи управляющих команд и, как следствие, к отказу функционирования компонент или полностью СлПО.

---

127 http://docs.cntd.ru/document/902301906

Анализ NIST SP 800-30

В NIST SP 800-30 «Risk Management Guide for Information Technology Systems» определение вероятности реализации угрозы проводится в рамках оценки риска [371]. Пять из девяти этапов оценки рисков можно отнести к определению актуальности УБИ. Согласно подразделу 3.5 стандарта при определении вероятности реализации УБИ учитываются следующие факторы:

- мотивация и возможности источника УБИ;
- характер уязвимости;
- наличие и эффективность применяемых защитных мер.

Для выявления источников угроз и самих УБИ рекомендуется использовать статистику об инцидентах ИБ в организации. В соответствии с пунктом 3.2.1 стандарта все УБИ можно разделить на 3 группы:

- природные угрозы;
- антропогенные угрозы;
- экологические угрозы.

Анализ международного стандарта ISO/IEC 27005

В международном стандарте ISO/IEC 27005 установлены требования к менеджменту рисков ИБ [319]. Согласно стандарту, угрозы ИБ и их источники должны быть определены. Входные данные для определения и оценки вероятности возникновения УБИ могут быть получены от владельцев активов или пользователей, специалистов в сфере ИБ и пр. Опыт, извлеченный из инцидентов ИБ, и предыдущие оценки угроз должны быть учтены.

В качестве примера рассмотрим угрозы природного происхождения с высокой периодичностью – взрывы на химическом заводе Arkema в Техасе в августе 2017 г. Эти взрывы явились прямыми последствиями урагана «Харви»[128], который привел к прекращению подачи электричества на территорию завода, из-за чего охлаждающие установки отключились. Доступ к хранилищу химикатов ограничен из-за наводнения, вся территория затоплена, глубина воды составляет

[128] https://www.arkema.com/en/media/news/news-details/Status-of-Plant-in-Crosby-Texas

более 6 футов[129]. В методе оценки рисков ИБ могут применяться критерии для оценки рисков ИБ (см. таблицу 2.12).

Таблица 2.12 – Критерии оценки рисков ИБ

Уровень возможного ущерба	**Уровень вероятности реализации угрозы**								
	Максимальный (1)			**Средний (2)**			**Минимальный (1)**		
	Уровень уязвимости								
	1	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7

В методе оценки рисков ИБ могут применяться следующие уровни приемлемого и остаточного риска ИБ (см. таблицу 2.13).

Таблица 2.13 – Уровни приемлемого и остаточного рисков ИБ

Уровень риска	**Пороговый уровень (приемлемый риск)**	**Необходима обработка риска**	**Остаточный риск**	**Приемлемость остаточного риска**
1	4	Да	1	Нет
2	4	Да	2	Нет
3	4	Да	3	Нет
4	4	Нет	4	Да
5	4	Нет	5	Да
6	4	Нет	6	Да
7	4	Нет	7	Да

В методе оценки рисков ИБ могут применяться следующие результаты анализа рисков ИБ (см. таблицу 2.14). В методе оценки рисков ИБ могут применяться следующие оценки приемлемого уровня и рекомендации по необходимости обработки рисков ИБ (см. таблицу 2.15).

[129] https://www.wsj.com/amp/articles/arkema-warns-it-cant-prevent-potential-chemical-explosion-in-texas-1504124326?mg=prod/accounts-wsj

Таблица 2.14 – Результаты анализа рисков ИБ (выборка)

№ риска	Наименование риска	Критичность актива	Уровень уязвимости	Уровень вероятности реализации угрозы	Величина риска	Уровень риска
1	Риски нарушения конфиденциальности информации в АС «Альфа»	Средний	Средний	Средний	4	Средний
2	Риски нарушения целостности информации в АС «Альфа»	Средний	Максимальный	Минимальный	4	Средний
3	Риски нарушения доступности информации в АС «Альфа»	Средний	Средний	Минимальный	5	Средний

Таблица 2.15 – Оценка приемлемого уровня и рекомендации по необходимости обработки рисков ИБ (выборка)

№ риска	Наименование риска	Состав актива	Приемлемость риска	Необходимость обработки риска	Приоритетность обработки риска
1.	Риски нарушения конфиденциальности информации в АС «Гамма»	Виртуальный сервер DDD1 VMware vSphere 5.xxx MS SQL 20xx	да	нет	
2.	Риски нарушения целостности информации в АС «Гамма»		да	нет	
3.	Риски нарушения доступности информации в АС «Гамма»		да	нет	

Анализ международного стандарта ISO/IEC 15408

В соответствии с ГОСТ Р ИСО/МЭК серии 15408 ([23] – [25]) предлагается дополнительный перечень УБИ применительно, например, к УЦ (см. таблицу 2.16).

Таблица 2.16 – Перечень угроз безопасности информации УЦ (выборка)

№ п.п.	Обозначение согласно ГОСТ Р ИСО/МЭК 15408	Наименование угрозы
1.	T.SKEY_THEFT	Кража (копирование) злоумышленником секретного ключа владельца сертификата ключа подписи с целью выдачи себя за истинного владельца секретного ключа (присвоение его полномочий).
2.	T.BASE_MISTAKE	Нарушение функционирования УЦ злоумышленником, приводящее к внесению не соответствующих действительности данных в сертификат открытого ключа, реестр выданных сертификатов, список отозванных сертификатов.
3.	T.CASKEY_ATTACK	Обход злоумышленником реализованных в составе УЦ механизмов защиты информации с целью получения доступа к закрытому ключу центра сертификации УЦ.
4.	T.CAADMIN_MASQUERADE	Воздействие злоумышленника на механизм идентификации и аутентификации УЦ с целью получения доступа к УЦ, присвоения полномочий системного Администратора.
5.	T.CRYPTOGRAPHIC_ATTACK	Применение злоумышленником методов и средств криптографического анализа с целью получения доступа к программной и/или информационной части УЦ или осуществления НСД к передаваемой УЦ информации.
6.	T.MALFUNCTION	Сбой и/или отказ отдельного компонента, механизма УЦ, или всего УЦ в процессе его функционирования.

Сравнительный анализ методик построения моделей угроз

В таблице 2.17 приведена обобщенная информация о выявленных элементах моделей угроз в рассмотренных выше стандартах и методиках.

Таблица 2.17 – Сравнительный анализ стандартов и методик моделирования угроз

Стандарты и методики моделирования угроз	**Элементы модели угроз**							
	Объекты воздействия	Уязвимости	Источники угроз	Защитные меры	Характеристики угроз			
					Способ реализации	Исходная защищенность	Вероятность реализации	Опасность
Базовая модель ФСТЭК	+	+	+		+			
РС БР ИББС-2.2-2009	+		+	+	+			
Модель угроз отрасли связи	+	+	+	+		+	+	+
Методические рекомендации (медицина)	+	+	+	+		+	+	+
СТО Газпром 4.2-0-004-2009	+	+	+				+	
NIST 800-30	+	+	+	+			+	
ISO/IEC 27005	+	+	+	+			+	
ISO/IEC 15408	+		+	+			+	

2.3.3 Требования к оценке уровня обеспечения ИБ

Формирование требований к оценке уровня обеспечения ИБ в ИС

Необходимо обратить внимание, что успешное решение проблем обеспечения ИБ (в т.ч. конфиденциальности и доступности) невозможно обеспечить без реализации комплекса мероприятий в отношении ИС. Более того, проблема обеспечения комплексной безопасности СлПО непосредственным образом зависит от уровня ИБ применительно к действующим ИС. Под термином ИС понимается термин «*система (system)*» как комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей (п. 4.17 стандарта ГОСТ Р ИСО/МЭК 15288-2005).

Но остается открытым вопрос о существующих мерах контроля ИБ, об оценке их эффективности и достаточности на всем жизненном цикле ИС – с момента создания, ввода в действие, эксплуатации, сопровождения и вывода из эксплуатации. Известно, что термин «*жизненный цикл системы*» («*system life cycle*») определяется как развитие ИС во времени, начиная от замысла и заканчивая списанием. (см. п. 4.20 стандарта ГОСТ Р ИСО/МЭК 15288-2005).

Требования ФСТЭК к оценке степени защищенности ИС

Во всех рассмотренных выше методиках моделирования УБИ вероятность реализации определяется экспертным методом. Поскольку не всегда возможно автоматизировать мнения различных групп экспертов, то на практике в РФ применяется подход, при котором оценивается степень реализации требований приказов ФСТЭК России, предъявляемых к ИС ([167] – [169]). В таблице 2.18 показано распределение требований по группам для каждого приказа ФСТЭК России. Знак « - » означает, что требования данной группы к ИС не предъявляются. Отметим, что буквальное исполнение требования ОПО (см. выше в таблице 2.18) не всегда реализуется на практике так, как нужно. В частности, в мае 2017 г. от вируса-блокировщика WannaCry пострадали более 500 тыс. компьютеров в 150 странах мира, а по данным экспертов Group-IB[130]

[130] http://www.rbc.ru/technology_and_media/27/06/2017/59528a7a9a7947235dce7803?from=center_1

цитата: «*уроки WannaCry пострадавшими организациями так и не выучены: обновления ПО все так же устанавливаются несвоевременно…*».

Таблица 2.18 – Требования ФСТЭК к ИС (выборка)

Группа требований	**Приказ № 17**	**Приказ № 21**	**Приказ № 31**
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	7	6	8
Управление доступом субъектов доступа к объектам доступа (УПД)	17	17	18
Ограничение программной среды (ОПС)	4	4	5
Защита машинных носителей информации (ЗНИ)	8	8	9
Регистрация событий безопасности (РСБ)	8	7	9
Антивирусная защита (АВЗ)	2	2	3
Обнаружение вторжений (СОВ)	2	2	3
Анализ защищенности информации (АНЗ)	5	5	6
Обеспечение целостности (ОЦЛ)	8	8	9
Обеспечение доступности (ОДТ)	7	5	8
Защита среды виртуализации (ЗСВ)	10	10	11
Защита технических средств (ЗТС)	5	5	6
Защита автоматизированной системы и ее компонентов (ЗИС)	30	20	31
Обеспечение безопасной разработки программного обеспечения (ОБР)	-	-	7
Управление обновлениями программного обеспечения (ОПО)	-	-	4
Планирование мероприятий по обеспечению защиты информации (ПЛН)	-	-	4
Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	-	-	6
Информирование и обучение персонала (ИПО)	-	-	4
Анализ угроз безопасности информации и рисков от их реализации (УБИ)	-	-	3
Выявление инцидентов и реагирование на них (ИНЦ)	-	6	7
Управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ)	-	4	6

2.3.4 Формирование требований к оценке уровня обеспечения ИБ СлПО

Как отмечалось выше, для ЛПР важно унифицировать совокупность требований, принятых на законодательном уровне: Федеральные законы, постановления Правительства ([155], [157], [158]), приказ ФСТЭК России № 31

[167] и дополнительно применять современные стандарты ISO (по ИБ – серии 27001 [317], по энергетике – серии ISO 50001 [321]), которые совместно формируют методологическую основу обеспечения ИБ для СлПО ТЭК.

Отметим, что в классическом труде Н. Винера по теории кибернетики отмечается: «*Для получения приемлемых результатов в приемлемое время необходимо довести до максимума скорость элементарных процессов и добиться, чтобы течение этих процессов не прерывалось существенно более медленными шагами*» [13].

2.4 Модели критериев оценки уровня ИБ на объектах ТЭК

2.4.1 Существующие подходы для оценки уровня ИБ на объектах ТЭК

Представляется важным сконцентрировать усилия на целях формирования достоверных моделей и методов обеспечения внутреннего аудита и оценки уровня ИБ на объектах ТЭК, находящихся под воздействием угроз ИБ. В настоящее время известна СОИБ, разработанная ПАО «Газпром» В ряде источников (например, «Эшелон»[131]) доступны стандарты СОИБ ([221] – [229]), которые содержат и некоторые требования стандартов ГОСТ Р ([19], [22]).

В работе Р.Кини и Х.Райфа показано, что к критериям, применяемым в процессе оценки со стороны ЛПР альтернатив для промышленных объектов, помимо требований измеримости, предъявляются также требования полноты, действенности, разложимости, минимальности и неизбыточности ([64], стр. 63). Для ряда организаций вполне естественно принимать «как есть» отраслевые требования, а внедрение дополнительных стандартов (национальных или международных) требует отдельного решения. Это обстоятельство не является экстраординарным, т.к., во-первых, изложено в преамбуле всех международных стандартов (ISO) и их российских переводов ГОСТ Р, во-вторых, является функцией формирования добавочной стоимости нематериальных активов (*intangible asset*) и, в-третьих, подтверждается мировой статистикой сертификации ISO [309]. Соответственно, в случае принятия такого решения – о внедрении конкретного национального или международного стандарта,

131 www.s3r.ru/2010/10/standarty/Gazprom

организация выполняет сопоставление (*mapping*) своих процессов ИБ, реализованных изначально только лишь под требования конкретных отраслевых стандартов. При этом возможны упущения (неполнота) при выполнении анализа рисков нарушения ИБ и недостаточно полное изучение уязвимостей процессов переработки информации в ИС со стороны ЛПР.

2.4.2 Основные различия в отраслевых подходах к оценке уровня ИБ

Объективно существуют различия в требованиях СОИБ, которые могут препятствовать успешному внедрению СМИБ (например, различия в понятиях «*актив*» и «*объект защиты*») и проведению успешной независимой оценки по требованиям стандарта 27001 [32]. Необходимо принять во внимание, что цели СОИБ (в нотации ПАО «Газпром») и СМИБ не вполне совпадают (в частности, СОИБ не предполагает проведение внешней оценки со стороны независимого органа), но содержат часть процедур СМИБ. В том случае, когда ЛПР принимает решение о подготовке СМИБ к внешнему аудиту, представляется необходимым проанализировать требования СОИБ (оценить уровень, на котором они реализованы) и принять решение о комплексе мероприятий, который следует предпринять для целей обеспечения соответствия СМИБ требованиям стандарта [32]. Далее будут рассмотрены два основных фундаментальных различия, которые могут иметь критичные последствия для целей создания и успешной эксплуатации СМИБ ([78], [93]). Второе негативное последствие выявленных различий, имеющее измеримое значение – дополнительные издержки при приведении СМИБ к уровню, достаточному для адекватного выполнения требований стандарта [32].

Различие 1 – идентификация (классификация) активов

Для анализа первого различия рассмотрим требования стандарта [32] в части управления активами и требования стандарта СОИБ [228] по классификации ОЗ. Известно определение: «*активы (asset): все, что имеет ценность для организации*» (п. 3.1 [32]). Дополнительно рассмотрим Приложение «В» стандарта [319]: «*для установления ценности активов организация должна определить все свои активы на соответствующем уровне*

детализации». Дается пояснение о том, что различаются два вида активов: «*основные активы*» и *«вспомогательные (поддерживающие) активы»*.

В фазе «План» цикла PDCA (п. 4.2.1 [32]) указано, что организация должна, например:

- *a) определить область и границы действия СМИБ с учетом характеристик бизнеса, ее размещения, активов и технологий;*
- *d) идентифицировать риски, для чего необходимо:… идентифицировать активы в пределах области функционирования СМИБ и определить владельцев этих активов;*

В Приложении А (обязательное приложение [32]) даны примеры реализации конкретных мер (средств) обеспечения ИБ (“*controls*”) в части касающейся управления активами, например:

- *A.7.1.1 «Опись всех важных активов организации должна быть составлена и актуализирована»;*
- *A.7.1.2 «Вся информация и активы, связанные со средствами обработки информации, должны иметь назначенного представителя организации»;*
- *A.7.2.1 «Информация должна быть классифицирована исходя из конфиденциальности, ценности и критичности для организации».*

В требованиях СОИБ [228] по классификации объектов защиты (ОЗ) приводятся иные термины и определения, где ОЗ трактуется существенно иначе, чем [222]:

- *АС – автоматизированная система;*
- *ИА – информационный актив;*
- *ПО – программное обеспечение.*

Согласно [222] под термином «*Объект защиты (ОЗ)*»: понимают информационные активы, технические и программные средства их обработки, передачи, хранения (п. 3.3.3). Этот перечень ОЗ является закрытым, объективно явно меньшим, чем дефиниция активов, представленная выше в стандартах ISO и ГОСТ Р. Соответственно, одним из критичных рисков может являться объективно явная неполнота идентифицированных и принятых к защите ОЗ в

СОИБ. В частности, в [228] никак не учтены активы по следующим категориям: персонал, место расположения (объекты) и структура организации. Необходимо обратить внимание, что предложенный подход СОИБ (в нотации ПАО «Газпром») вносит существенные сложности далее в процесс поддержания и обеспечения ИБ и, в частности, в области управления инцидентами ИБ и рисками ИБ. Например, стандарт ГОСТ Р ИСО/МЭК 18044 [28] оперирует примерами инцидентов ИБ, связанных с персоналом, а международный стандарт ISO серии 27040 по обеспечению безопасности хранящихся данных также принимает во внимание важнейшую роль персонала (внутреннего, внешнего) в обеспечении требуемого уровня ИБ на объектах инфраструктуры. В стандарте [228] в разделе 5 определены правила идентификации ОЗ. Для каждого из идентифицированных ОЗ должны быть определены его собственник, владелец и пользователи (п. 5.6). Каждый из них должен быть отнесён только к одному из следующих типов (п. 5.8): ИА, ПО или ТС. В [228] все ОЗ на основании определенного уровня критичности относят к одной из групп (п. 7.1).

Таким образом, можно сделать предварительный вывод по 1-му различию – для разработки и успешной эксплуатации СМИБ по требованиям [32] только выполнения требований СОИБ объективно недостаточно, т.к. учитывается крайне ограниченное множество критичных активов (ОЗ в нотации ПАО «Газпром») для объектов ТЭК.

Различие 2 – Оценка рисков ИБ

Для анализа 2-го различия рассмотрим требования [32] в части управления рисками ИБ и требования СОИБ [226] по анализу и оценке рисков. Основные определения, необходимые для анализа 2-го различия, приведены в [32] (п.п. 3.7 – 3.15). Основные требования по управления рисками ИБ удобно рассмотреть по фазам цикла PDCA, аналогично разделу выше. В фазе «План» (п. 4.2.1 [32]) необходимо, в частности:

— *установить критерии оценки рисков (4.2.1 b) 4)*

— *определить методологию оценки риска (4.2.1 c) 1)*

— *определить приемлемые уровни риска (4.2.1 c) 2)*

— *идентифицировать риски (4.2.1 d)*

— *проанализировать и оценить риски (4.2.1 e)*

— *определить и оценить различные варианты обработки рисков (4.2.1 f)*

— *получить утверждение руководством предполагаемых остаточных рисков (4.2.1 h)*

В фазе «Делай» (п. 4.2.2 [32]) необходимо:

— *разработать план обработки рисков (4.2.2 a)*

— *реализовать план обработки рисков (4.2.2. b)*

В фазе «Проверяй» (п. 4.2.3 [32]) необходимо:

— *пересматривать оценки рисков через установленные периоды времени,*

— *анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения (4.2.3 d)*

В Приложении А (обязательное приложение [32]) даны примеры реализации конкретных мер (средств) обеспечения ИБ (“*controls*”) в части касающейся менеджмента рисков, например:

— *A. 6.2.1. Определение рисков, связанных со сторонними организациями;*

— *A. 9.2.1. Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от воздействия окружающей среды и возможности несанкционированного доступа;*

— *A. 11.7.1. Необходимо иметь в наличии формализованную политику для защиты от рисков при использовании переносных устройств;*

— *A. 14.1.2. Непрерывность бизнеса и оценка риска;*

В свою очередь, в требованиях СОИБ [226] по анализу и оценке рисков выполняются следующие основные процедуры (п. 4.4):

— *идентификация риска;*

— *анализ риска;*

— *оценивание риска.*

Оценка рисков осуществляется только для АС, в состав которых входит хотя бы один ОЗ с максимальным уровнем критичности. Таким образом, объективно

существует критичный риск для целей создания СМИБ, при котором деятельность по оценке рисков в терминах только СОИБ может вообще не проводиться. Соответственно, деятельность, предусмотренная СОИБ [226] не будет осуществляться на «законных» основаниях, что может привести к ошибкам в процессах выявления, идентификации и классификации УБИ для защищаемых объектов, а также к недостоверному анализу ЛПР рисков ИБ и уязвимостей в процессах ИС в установленной области применения (*scope*).

Особенно важно, что может наблюдаться «вложенность» и «каскадирование» критичных рисков – невыполнение оценки рисков (Различие 2) может быть прямым следствием исключения персонала из активов в СОИБ (Различие 1). Соответственно, применение для целей оценки возможного ущерба ИБ качественной шкалы представляется не вполне оправданным и методически уязвимым с позиции обеспечения достижения ***измеримых*** целей – создание и обеспечение постоянного повышения результативности СМИБ.

Объективно, существует затруднение для определения уровня возможного ущерба для активов (в терминах стандартов ИСО), но не учтенных как ОЗ в системе СОИБ, например: персонал (собственный и посторонний), серверные (кроссовые) помещения, помещения для проведения конфиденциальных переговоров и пр. В СОИБ указано, что должны приниматься риски, превышающие допустимый уровень, если для данных рисков отсутствует подходящий способ обработки (п. 7.5 [226]). Это положение также создает существенное затруднение для обеспечения ИБ, т.к. не выполняется в системе СОИБ ПАО «Газпром» в силу применяемой парадигмы формирования ОЗ.

2.4.3 Расширение набора критериев при оценке уровня ИБ

Формирование расширенного набора критериев для аудита ИСМ

Известно, что любой комплексный аудит проводится в соответствии с утвержденными критериями [20], [21]. Например, внешний авиационный аудит в АК может проводиться на соответствие требованиям ISAGO [325] – [327], аудит по требованиям АБ может проводиться на соответствие требованиям Aviation Security Procedure (Процедура авиационной безопасности) или Air

Carrier Security Program (Программа безопасности авиаперевозчика) для международных авиакомпаний. Аудит СМИБ (СМИБ) может проводиться на соответствие требованиям международных стандартов ISO [317], [321].

Отметим появление новых угроз для АК:

- В июне 2016 г. в международном аэропорту г. Дубай в зоне полетов появился дрон, который привел к отмене взлетов и вылетов на 69 мин. Убыток аэропорта составил более 1 млн. долларов (по данным «Директор по безопасности», октябрь 2016 г., стр. 73);
- В августе 2017 г. на крупнейший военный корабль Великобритании «Queen Elizabeth» водоизмещением свыше 70 тыс. тонн по данным BBC[132] был посажен дрон без каких-либо мер противодействия. В обзоре BBC отмечается, как легко дрон мог доставить пластид прямо на летную палубу авианосца стоимостью 3 млрд. евро;
- Из-за сбоя в системе регистрации пассажиров компании All Nippon Airways 2016 г. в 50 аэропортах аннулировала 87 внутренних рейсов, на которых должны были лететь около 10 тыс. пассажиров;
- По данным бельгийской газеты L'Avenir 22.03.2016 глава полицейского профсоюза SLFP Police жаловался, что руководство аэропорта не отреагировало на жалобы о недостатке ресурсов. «Мы призывали увеличить штат полицейских, установленный шенгенскими соглашениями, в количестве 435 человек. Эта цифра была утверждена 15 лет назад!»[133].

Формирование расширенного набора критериев для аудита АК

Помимо общеизвестных международных стандартов – например, ISO или ISAGO, необходимо предусмотреть расширение базы критериев для проведения комплексного аудита ИСМ. Таким образом, центральным вопросом становится обеспечение фазы «контроля» (*check*) в цикле PDCA, который базируется на процессах управления документами и записями в терминах стандартов [20], [21]. Это требование также отражено в базовой модели ИСМ (см. Главу 1, рисунок

---

132 http://www.bbc.com/news/uk-scotland-highlands-islands-40910087

133 http://www.rbc.ru/society/23/03/2016/56f2b1309a79475fef3d0852

1.7). Для планирования аудита необходимо определить приоритет критериев аудита – т.е. формирования такого оптимального набора критериев аудита ИСМ (на базе стандартов ISO, ГОСТ и пр.), который позволит наилучшим образом решить поставленную задачу – формирование оценки уровня обеспечения безопасности АК. Совокупность требований, изложенных в представленных выше стандартах ISO, рассмотрена в работах [66], [78], [99], [154], [373].

Дополнительные требования по безопасности должны быть приняты во внимание с целью отражения специфики функционирования АК относительно базовой модели аудита ИСМ (см. Главу 1). К таким требованиям могут быть отнесены и, соответственно, оценены как метрики функциональных подсистем:

— *степень документирования требований АБ;*

— *степень соответствия персонала требованиям компетентности АБ;*

— *количество инцидентов в АК (в т.ч. динамика изменения).*

В качестве примера формирования расширенного перечня критериев для аудита АК рассмотрим безопасность топливного комплекса. По данным «Коммерсанта»[134] в августе 2017 г. «Газпромнефть-Аэро Шереметьево» оповестила авиакомпании о временных перебоях с авиакеросином. В результате «Аэрофлот» был вынужден задействовать резервную схему обеспечения авиатопливом на ТЗК Шереметьево.

Дополнительные нормативные документы ISAGO

Дополнительно рассмотрены нормативные документы [325] – [327]. Документ «ISAGO Standards Manual Effective January 2014 3rd Edition» [325] содержит 7 секций требований. Наибольшее значение имеют следующие:

— *Секция 2. Documentation and Records (Документации и записи).*

— *Секция 3. Safety and Quality Management (Менеджмент защиты и качества).*

— *Секция 6. Security Management (Менеджмент безопасности).*

134 https://www.kommersant.ru/doc/3383818

Важное требование по управлению функциями аутсорсинга ([325]) отражает функциональные спецификации ISAGO по получению подтверждений от «провайдеров» по документированию и мониторингу требований по безопасности и наземному обслуживанию. Это требование соответствующим образом учтено в базовой модели ИСМ (см. Главу 1, рисунок 1.7, блок аудита 2-й стороной). Отметим, что в Секции 1 «ORGANIZATION AND MANAGEMENT» присутствуют разделы, например, Management Review (*Анализ со стороны руководства*), Risk Management (Управление риском), соответствующие требованиям стандартов ISO ([33], [315], [319]). В документе «IATA Reference Manual for Audit Programs (IRM) Effective November 2012 3rd Edition» [326] представлены все основные сущности и артефакты процесса аудита, документированных оператором или провайдером. В документе «ISAGO & IGOM & GDDB Integrated solution for improved Ground Safety, Joseph Suidan Head of Ground Operations, ULD Care, May 2013» [327] представлены концептуальные пояснения к процессу обеспечения безопасности при наземном обслуживании в методических «разрезах»:

— *Что должно быть сделано* (подтверждается предоставлением документированных политик, стандартов и руководств по безопасности – для менеджеров);
— *Как должно быть сделано* (подтверждается предоставлением документированных процедур, инструкций и рабочих карт – для перронного персонала)

В документе также изложены спецификации к «сообществу аудиторов ISAGO» (ISAGO Audit Pool Membership), которое проводит аудит (*station audits*) на ежегодной основе и обеспечивает свободный доступ к отчетам уже выполненных аудитов. Всего ISAGO Audit Pool включает 38 авиакомпаний (на 2016 г.), среди которых «Аэрофлот». Отметим, что в 2014 г. Департамент внутреннего аудита компании «Аэрофлот» реализовал проект автоматизации аудита на базе SAP Audit Management, при котором все элементы внутреннего аудита автоматизированы на основе единой системы и обеспечивается

соблюдение международных стандартов внутреннего аудита и концептуальных основ управления рисками.

В системе аудита ISAGO для наземных служб (Ground Service Providers) принят 2-х летний цикл аудита (в отличие от 3-х летнего цикла, принятого в системе ISO [21]). Особенностью является цикл постоянного улучшения, реализованный на базе отраслевых требований. Пример цикла постоянного улучшения в IATA показан на рисунке 2.20.

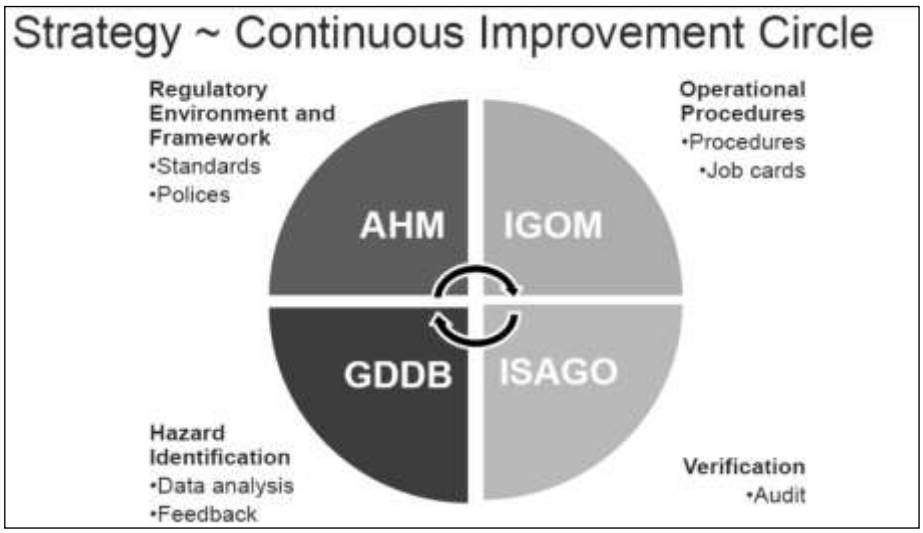


Рисунок 2.20 – Цикл постоянного улучшения IATA

Этот цикл соответствует в целом циклу PDCA, принятому в качестве методологии для всех стандартов ISO. В частности, фазе «*Check*» (в цикле PDCA) соответствует фаза «Verification» (в цикле IATA) и определен стандарт ISAGO. В обоих рассматриваемых циклах на этой фазе выполняется аудит, центральная задача которого – выявление фактов, свидетельствующих о степени выполнения установленных критериев аудита (например, стандартов ISO или стандарта ISAGO), т.е. оценка применительно к исследуемым процессам АК.

Рассмотрим специфические требования к аудиту, установленные IATA в Руководстве по авиационной безопасности Doc 8973/8. В разделе 4.4.1 определено, что, по возможности, государствам следует обмениваться информацией несекретного характера в рамках ограничений, установленных национальным законодательством в отношении защиты конфиденциальной или секретной информации по авиационной безопасности, при надлежащих

условиях и с использованием надлежащих средств в целях достижения общих стандартов, согласованных процедур и передовой практики. В разделе 7.2.3 указано, что меры по контролю качества должны быть объективными, достоверными и беспристрастными, что гарантирует сотрудничество со стороны контролируемых структур, признание результатов проверок и эффективное выполнение корректирующих действий. В разделе 7.4.7 указано, что орган по контролю качества должен выпускать годовое заявление, содержащее информацию о выявленных недостатках, о текущем статусе корректирующих действий, о внесенных изменениях и о состоянии ресурсов.

2.4.4 Дополнительные нормативные документы ГОСТ Р

Как показывает практика выполненных проектов ([103], [96]) только лишь внутренних процедур по управлению документацией и записями недостаточно. Этот «дефицит» предполагается покрыть за счет применения дополнительных стандартов. Представляется целесообразным расширить базовый набор критериев (требования стандартов ISO) двумя национальными стандартами ГОСТ Р 51901 [46] и ГОСТ Р 53704 [50]. Важно отметить, что эти ГОСТ оперируют понятием риска, что точно соответствует концепции современных риск-ориентированных стандартов ISO и, что более важно, позволяют получить модель для формирования численной оценки соответствия множеству требований, применимых для АК.

Положения стандарта [46] могут применяться при формировании модели ИСМ и, соответственно, модель ИСМ для проведения аудита АК дополняется аспектами, учитывающими численные оценки в процессе аудита ИБ:

— что может выйти из строя (идентификация опасности);

— с какой вероятностью это может произойти (анализ частоты);

— каковы последствия этого события (анализ последствий).

Эти положения точно соответствуют основным требованиям процедуры «*Business Impact Analyses»,* указанным в стандарте [315], и процедуры «*Information security risk assessment»,* указанной в стандарте [317]. Далее, в [46] (п. 4.4.1) отмечается, что «*Анализ частот используется для оценки вероятности*

каждого нежелательного события, идентифицированного на стадии идентификации опасности». Следующий важный элемент в [46] – прямое указание в п. 6.3 в Таблице 2 «*Перечень дополнительных методов, используемых при анализе риска*» на применение МПС, который реализуется как способ оценки и ранжирования совокупности рисков путем попарного сравнения. Отметим, что требования [46] весьма логичны и органично дополняют подходы к оценке принятия решений по методу анализа иерархий (метод Т. Саати), который применяется, в том числе и для оценок СМИБ и ИСМ ([105]). Вообще, оценка уровня обеспечения ИБ является весьма сложным вопросом, особенно при определении периодичности и методов ее проведения. В частности, в ряде публикаций (РФ, «Акрибия»[135]) и международных (Groundbreaking Security Measurement Index benchmark[136]) приводятся факты в пользу того, что результаты оценки уровня обеспечения ИБ задают вектор дальнейшего развития СМИБ и ИСМ. Однако вопрос о том, с какой периодичностью стоит проводить оценку уровня обеспечения ИБ, является неоднозначным. В ГОСТ Р [50] предложены важные определения, которые расширяют методическую область предложенной модели ИСМ для оценки АК, по сравнению, например, с [327]. Рассмотрим 3 определения:

- *безопасность защищаемого объекта* (п. 3.1 [50]);
- *латентность защищаемого объекта* (п. 3.9 [50]);
- *латентность фактора угрозы нанесения ущерба (вреда) защищаемому объекту* (п. 3.10 [50]).

Соответственно, предлагается объективная метрика, специфицирующая не только вопрос комплексной безопасности СлПО, но и оценку «логической цепочки» в процессе управления аудитом ИБ в АК – выявлению системных закономерностей в ИСМ и, как частный случай аудиторских наблюдений – выявление несоответствий, в том числе, в силу определенных причин «латентного» характера [50], как будет показано далее при анализе

---

135 http://www.acribia.ru/articles/7_reasons_for_annual_security_analysis

136 https://thycotic.com/wp-content/uploads/2013/03/2017-Cyber-Security-Strategy-Metrics-Report.pdf

документации ИСМ (см. Главы 3 и 4). Весьма важно, что [50] устанавливает (п. 5.3.1) в фазе «Проектирование» необходимость выполнения экспертного обследования объекта, что является, по сути, одной из известных техник проведения аудита ([19] – [21]). В качестве примера скрытых (латентных) угроз рассмотрим «потаенный» трафик Serial-over-LAN (SOL). Исследователи Microsoft выявили семейство вредоносного ПО, которое использует в качестве средства передачи данных технологию Intel SOL[137]. Компания Intel в результате аудита обнаружила 10 серьезных уязвимостей в системах ME, Trusted Execution Engine (TXE) и Server Platform Services (SPS)[138].

2.4.5 Специальные критерии для проведения аудита

После рассмотрения базовых и дополнительных критериев для оценки уровня ИБ в СлПО, обратим внимание на специальные критерии, появление которых может быть обосновано применением «целевых» ИС, в частности – SAP ERP HCM (Human capital management). Рассмотрим несколько примеров:

1. Анализ опасностей (Danger Analysis):
   - Уязвимость: нет SSL соединения с шифрованием.
   - Угроза: информация может быть считана и модифицирована.
2. Анализ последствий (Impact Analysis): процессы производства могут быть просмотрены или модифицированы конкурентами.
3. Анализ риска (Risk Analysis).
4. Применяемый контроль (*Controls*) – SSL-шифрование для всех туннелей.
5. Способ измерения (*Control Measure*) – ревизии и таблицы авторизации.
6. Стоимость внедрения (*Implementation Cost*).
7. Скорость внедрения (*Implementation Speed*).
8. Степень соответствия (*Degree of compliance*).
9. Приоритетность (*Priority of security recommendation*).

---

137 http://safe.cnews.ru/news/top/2017-06-13_troyany_nauchilis_obhodit_antivirusy_i_faervolly

138 https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr

2.4.6 Оптимизированная модель ИСМ для проведения аудита СлПО

На основании рассмотренных выше требований к критериям (базовым, расширенным и специальным), предложим оптимизированную модель ИСМ для проведения аудита СлПО, например в АК (см. рисунок 2.21).

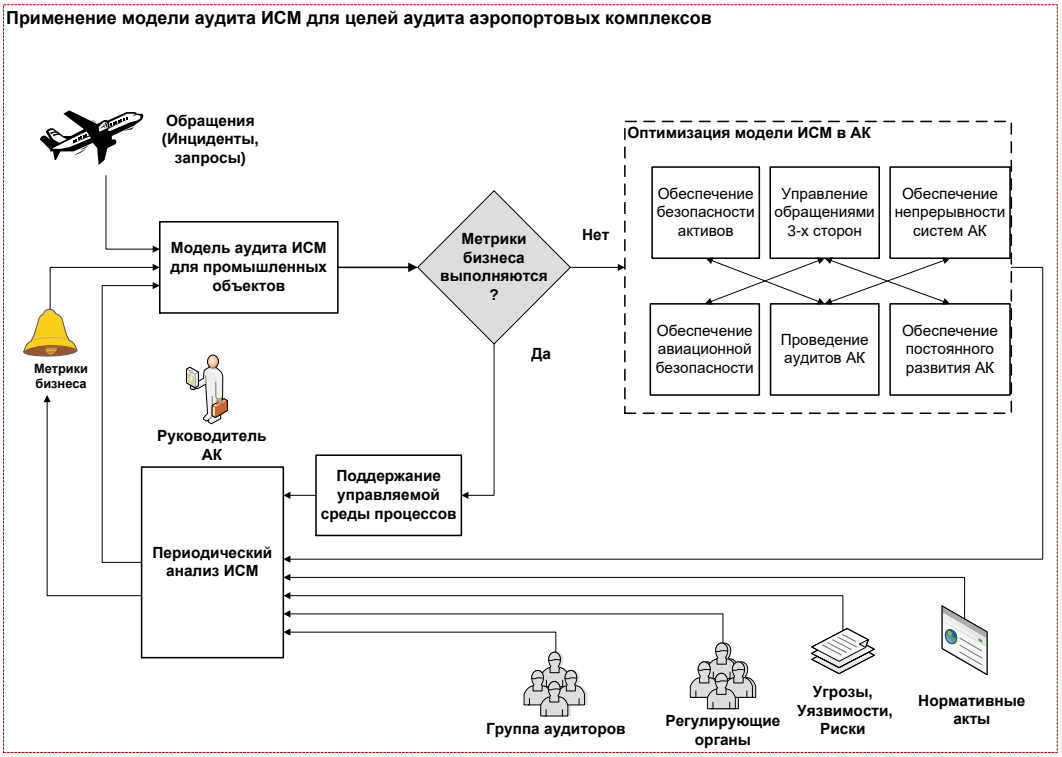


Рисунок 2.21 – Модель ИСМ для целей аудита АК

Новая модель основана на базовой модели аудита ИСМ (см. Главу 1, рисунок 1.9) и дополнена специальным блоком оптимизации – для целей получения оценки уровня обеспечения ИБ СлПО в режиме, близком к РРВ. С учетом указанных выше особенностей проведения комплексного аудита на примере АК, основное внимание должно быть уделено блоку оптимизации модели ИСМ в АК. Блок оптимизации учитывает («на входе») степень результативности бизнес-процессов АК, и отрабатывает необходимые изменения в модели ИСМ («на выходе»). Таким образом, возможно внесение управляющих воздействий (блок оптимизации) в цикле PDCA по каналам обратной связи: от базовой модели ИСМ промышленного объекта – через оценку результативности (степени достижения метрик) – через необходимую оптимизацию и периодический анализ ИСМ со стороны руководства.

Поставленная задача решается через оценку результативности (оценку уровня обеспечения безопасности) как для СМИБ, так и ИСМ в целом.

Дополнительно отметим важность проведения учений по отражению атак СлПО. В частности, учения «Кибер-Антитеррор-2016», проведенные на базе Лукомльской ГРЭС в Витебской области Белоруссии, показали важность получения оценки устойчивости СлПО при различных сценариях борьбы с кибертерроризмом. Известно, что в июне 2008 г. произошла авария на Лукомльской ГРЭС, последствия которой привели к отключению электроэнергии в Белорусии[139]. В частности, один из сценариев киберучений должен был проверить степень выполнения всех запланированных и реализованных мер энергетиков Лукомльской ГРЭС.

Еще одним примером киберучений служит новый стандарт Европейского центрального банка для проверки устойчивости финансового сектора к кибератакам[140]. В качестве такой проверки выступает симуляция последствий кибератак на критические системы в банковской отрасли Европейского союза. Кроме того, в отрасли представлена новая парадигма: Attack Mitigation Solution. Это решение объединяет WAF, SSL and DDoS защиту в режиме, близком к PPB и предусматривает автоматизацию проверок, оперативный анализ рисков и сервисные контракты с поставщиками[141]. Следующий пример касается учений по повышению безопасности единой сети электросвязи, проведенных Минкомсвязи в 2017 г. В рамках учений специалисты компании Positive Technologies осуществили различные атаки на сети «Мегафона» в Ростовской области[142]. Эксперты эксплуатировали уязвимости в протоколах SS7 и Diameter, моделируя ситуацию, когда злоумышленник пытается перехватить голосовой трафик, подменить текст SMS-сообщения и отследить местоположение по геолокационным сервисам. В очередной раз был подтвержден факт наличия в SS7 и Diameter[143] серьезных уязвимостей. В обзоре PT[144] (в 2018 г.) отмечается,

---

139 www.inside-zi.ru, № 5, 2016 г. С. 57 - 63

140 https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html

141 https://securityboulevard.com/2018/05/new-threat-landscape-gives-birth-to-new-way-of-handling-cyber-security/

142 https://www.securitylab.ru/news/490537.php

143 https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/SS7-Vulnerability-2018-rus.pdf

144 https://www.securitylab.ru/news/491884.php

что практически в каждой сети можно прослушать разговор абонента, прочитать входящие SMS-сообщения, а сети содержат опасные уязвимости, позволяющие нарушить доступность сервисов для абонентов. Любые учения призваны уделять больше внимания обеспечению готовности и общей устойчивости (*sustainability).* Готовность требует предварительного планирования комплекса действий в экстренной ситуации, тестирования и контроля, включая разработку планов информационного взаимодействия (в частности, см. ИСО серии 22301 [315]).

Рассмотрим пример («Руководство» [182]) демонстрации последствий атаки на электростанцию[145]. В 2007 г. ученые Национальной лаборатории Айдахо провели для Министерства национальной безопасности США наглядную демонстрацию получения доступа к СУ электростанции и управления ею извне для вызова физического сбоя путем введения ложных данных. Демонстрация, названная «Тест генератора Аврора», показала не только то, что хакеры способны преодолеть системы защиты и получить контроль над генератором, но и то, что генератор может быть физически разрушен. Известно, что 23.12.2015 несколько областей Западной Украины остались без электроэнергии в результате отключения 57 электроподстанций. Было подтверждено, что причиной стала хакерская атака ICS. По результатам расследования 4 января 2016 г. данная причина отключения была подтверждена украинской командой экстренного реагирования на кибератаки (CERT-UA), а этот инцидент был признан "*первым отключением электроэнергии в результате кибератаки*". Известно, что атака была выполнена хорошо спланированным способом в несколько этапов.

2.5 Парадокс ИБ для СлПО

2.5.1 Формулирование «Парадокса ИБ» для СлПО

С учетом фактов, отражающих возрастание угроз ИБ и использования уязвимостей современных ИС, серьезных сбоев критичных ИС и их компонент (как было отмечено выше), а также требований, содержащихся в применяемых стандартах и доступных методах, объективно существует положение, которое

[145] http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US (11/21/2012)

формулировано как «Парадокс ИБ» [106]. Предлагается следующая формулировка: «*На современном этапе развития ИС наиболее значимые (критичные) угрозы в течение жизненного цикла ИС в СлПО являются прямым следствием доминирования зарубежных компонент в программном и аппаратном обеспечении ИС, и, в то же время, механизм эффективного противодействия данным угрозам содержится в современных риск-ориентированных стандартах ISO*».

Известны многочисленные факты проявления данного парадокса – на примере МПлС Visa и MasterCard (отключение банков в РФ в 2014 г.), у которых вся критичная техническая инфраструктура размещена вне зоны разумного контроля в РФ. Объективно, на тот момент были возможны ограничения доступности и ощутимые финансовые издержки КО БС в РФ на любой фазе ЖЦ банковских ИС. Более того, даже сейчас уже при реализации НСПК (ФЗ-161, [241]) есть жизненная необходимость введения отечественной сертификации, т.к. в случае международных санкций EMVCo (международный стандарт Europay, Mastercard и Visa для стандартизации операций по банковским картам) может приостановить на неопределенный срок выдачу сертификатов безопасности на отечественные микросхемы[146]. Что касается чипов для SIM-карт, то данным АО «Микрон», этот рынок полностью отдан иностранным производителям. Отмечается, что задача интеграции российской криптографии в SIM-карты будет труднореализуемой, так как нужно будет договариваться с зарубежными разработчиками чипов о поддержке российских алгоритмов[147]. В тоже время экспертам известны минимально два случая отключения банков от системы SWIFT: в 2012 г. – в отношении иранских банков, в 2017 г. — в отношении банков Северной Кореи[148]. Определенно, действовали санкции по линии ООН, а в случае с Ираном SWIFT исполняла решение Евросоюза. Но запрет на использование SWIFT можно частично обойти: во-первых, были отключены не все иранские банки, а во-вторых, банки смогли арендовать

146 http://www.cnews.ru/news/top/2017-12-05_inostrannye_chipy_dlya_kart_mir_budut_podvergat
147 http://www.cnews.ru/news/top/2017-11-29_dlya_setej_5g_budut_sozdany_simkarty_s_rossijskoj
148 https://www.rbc.ru/politics/17/04/2018/5ad480ef9a7947fb625fa03e?from=center_3

телефонные линии в Дубае, Турции и Китае для передачи банковских сообщений[149]. Кроме того, банк в Бахрейне вывести от контроля регуляторов транзакции на 2,7 млрд. долл. США, используя некую «неформальную альтернативу системе SWIFT, которую сложно проследить»[150].

В качестве нормативной и методической поддержки для смягчения последствий западного доминирования в ИС рекомендуется тот же перечень стандартов, которые применяются во всем мире: это ряд стандартов ISO, например, серии 20000, 27001 и 22301 ([311], [317], [315]). Снова отметим, что эти же стандарты приняты в РФ в качестве ГОСТ Р ([30] – [32]), соответственно, могут и должны (наряду с внутренними мерами защиты, системами сертификации СрЗИ по требованиям ФСТЭК и/или СКЗИ по требованиям ФСБ), применяться для обеспечения требуемого уровня ИБ и парирования негативного воздействия на критичные ИС в СлПО. Аналогичный обзор с примерами национальных стандартов, гармонизированных с ISO 27032, публиковали эксперты «Эшелон» А.С. Марков и В.Л. Цирлов[151]. Однако, имеется объективный фактор, значительно усиливающий «Парадокс ИБ» – многие организации, не спешат с «*принятием на вооружение*» и не практикуют широкое применение новых стандартов ISO, хотя бы и в виде «локализованных» национальных ГОСТ Р, предпочитая опираться на руководящие документы ФСТЭК, утвержденных еще в 1992 г.

2.5.2 Пример решения «Парадокса ИБ»

В качестве примера практического решения «Парадокса ИБ» рассмотрим основные международные стандарты в области ИБ – ISO/IEC 27001:2013 (в РФ принят ГОСТ Р ИСО/МЭК 27001-2006) и ISO/IEC 20000:1-2011 (в РФ принят ГОСТ Р ИСО/МЭК 20000:1-2011) и продемонстрируем, какие меры и средства ИБ необходимо применять для обеспечения должного уровня ИБ в действующих ИС в СлПО (см. таблицу 2.19).

---

149 https://www.newsru.com/finance/25dec2017/gref.html
150 https://www.rbc.ru/rbcfreenews/54c212699a7947820788688d
151 http://s3r.ru/wp-content/uploads/2014/03/iso27032.pdf

Таблица 2.19 – Применение стандартов ISO для обеспечения ИБ ИС в СлПО (фрагмент)

Компонент ИБ	**Стандарты**		**Пример**
	ISO/IEC 27001	**ISO/IEC 20000:1**	
Определение контекста	4.1	-	Перечень зарубежных поставщиков компонент критичных ИС в СлПО. Дополнительно – перечень аналогов (производства «доверенных» стран)
Планирование поддержки и развития ИС	-	4.5.2	План создания, внедрения и поддержки ИС в СлПО (с учетом законодательства, ограничений по привлечению третьих лиц, аутсорсинга в ИБ)
Потребности заинтересованных сторон	4.2	4.1.1 d)	Перечень требований поставщиков компонент критичных ИС в СлПО в части ИБ. Дополнительно – перечень аналогов (производства «доверенных» стран)
Оценка рисков ИБ	6.1.2	6.6.2 d)	Реестр рисков (идентификация, анализ, оценка, сравнение с критериями) в части компонент ИС
Обработка рисков ИБ	6.1.3	6.6.3	Решение о приемлемом варианте обработки рисков (меры обеспечения ИБ, формирование плана, согласование с владельцем риска) в части компонент ИС
Компетенция	7.2. a)	4.4.2 a)	Определение необходимой компетенции персонала в части, касающейся ИБ и ИС в СлПО
Внутренний аудит ИБ	9.2 f)	4.5.4.2 b)	Процесс информирования высшего руководства в части, касающейся ИБ и ИС в СлПО. Дополнительно – привлечение внешних аудиторов в рамках аудита 2-й стороной.
Управление несоответствиями	10.1 b)	4.5.4.2	Предпринятые действия для устранения причин выявленных несоответствий ИБ. Дополнительно – привлечение внешних аудиторов и/или экспертов (ФСБ и/или ФСТЭК)

2.5.3 Принципы реализации «Парадокса ИБ» для ИС в СлПО

На основании приведенных выше фактов, анализа нормативно-технических документов, оценки УБИ и предложенной формулировки «Парадокса ИБ», представляется возможным сформировать принципы реализации для обеспечения ИБ для ИС в СлПО (см. [106]):

1. *Базовый минимальный принцип* – Необходимо реализовать систему управления, основанную на международных стандартах (или аналогичных ГОСТ Р) в СМИБ (ИСМ) и обеспечить комплекс мер и средств ИБ, адекватно выявленным и оцененным рискам ИБ. Результаты оцениваются (качественно или количественно) в рамках планового аудита СМИБ (ИСМ).
2. *Базовый достаточный принцип* – Необходимо реализовать в ИСМ комплекс международных стандартов (или аналогичных ГОСТ Р), достаточных для оказания услуг на согласованном уровне ИБ с учетом определенных рисков ИБ и, дополнительно, с учетом требований ИБ заинтересованных сторон. Результаты оцениваются (качественно или количественно) в рамках планового аудита ИСМ.
3. *Расширенный принцип «Государственного регулирования»* – Необходимо реализовать в ИСМ комплекс требований, установленных регуляторами (ФСБ, ФСТЭК России, МО, МЧС и пр.), с учетом специфики процессов ИБ при функционировании ИС в СлПО. Результаты оцениваются (качественно или количественно) в рамках планового аудита ИСМ, в т.ч. в рамках плановых проверок лицензиатов.

При реализации «Парадокса ИБ» важно принять во внимание специфику процесса лицензирования в области ИБ в РФ. Ряд экспертов (в частности, руководитель аналитического центра Zecurion В.Ульянов[152]) отмечают, что на рынке средств ИБ для госсектора очень много регуляторов, и только получив ряд сертификатов и лицензий, компания сможет поставлять свою продукцию. Отмечается, цитата: «*собственная система сертификации есть у Минобороны,*

---

152 http://www.rbc.ru/technology_and_media/31/07/2017/597b46f99a7947c6ad71eda3?from=newsfeed

ФСБ, ФСТЭК, кроме того, разрешительные документы выдают Минкомсвязь, Роскомнадзор и Центробанк». Соответственно, «Парадокс ИБ» может столкнуться с принципиальным и неразрешимым ограничением – невозможностью независимой оценки предлагаемых решений ИБ, так как, цитата: «*заказчики на этом рынке, в первую очередь смотрят не на функциональность программного продукта, а на то, есть ли на него необходимые документы, и даже получение всех нужных сертификатов не гарантирует, что компания сможет продать свой продукт*».

Для преодоления данного ограничения «Парадокса ИБ» на приоритетное место определен базовый минимальный принцип, а именно – необходимость реализации СУ, основанной на международных стандартах ISO / IEC (или аналогичных ГОСТ Р) для СМИБ (ИСМ) и обеспечение комплекса мер (средств) ИБ, адекватно выявленным и оцененным рискам ИБ.

4. *Расширенный принцип «Отраслевого регулирования»* – Необходимо реализовать в ИСМ дополнительно комплекс требований, установленных в отрасли (СТО БР ИББС, СОИБ «Газпром» ГОСТ РВ 0015-002-2012, ISAGO и пр.), с учетом специфики процессов ИБ при функционировании ИС в СлПО, требований к их доступности и надежности и пр. Результаты оцениваются (качественно или количественно) в рамках планового аудита ИСМ, в т.ч. в рамках плановых проверок лицензиатов.
5. *Расширенный принцип «Лучших практик»* – Рекомендуется реализовать в ИСМ комплекс «лучших практик», принятых в отрасли (ITIL, Cobit, SOX, Basel, COSO и пр.), с учетом специфики функционирования ИС в СлПО, требований к их доступности и надежности и пр. Результаты оцениваются (качественно или количественно) в рамках планового аудита ИСМ, в т.ч. в рамках плановых проверок независимых аудиторов.

Обратим внимание, что применение лучших международных стандартов в области ИБ (ISO/IEC серии 27001, 20000, 22301, 15408 и пр.), принятых в РФ в качестве национальных ГОСТ Р, оказало влияние на систему требований в государственном оборонном заказе. В ГОСТ РВ 0015-002-2012 в разделе 4.3

содержатся требования к ИБ и дана прямая ссылка на «целевой» стандарт ГОСТ Р ИСО/МЭК 27001-2006. Соответственно, наблюдается логичное и обоснованное включение требований по ИБ там, где это наиболее критично – в области государственного оборонного заказа. Представляется рациональным принятие таких же требований для иных критичных отраслей экономики РФ – отрасли связи, энергетики, транспорта, добычи (транспортировки) углеводородного сырья и пр. Необходимо выполнять периодическую оценку уровня обеспечения ИБ в СлПО и предлагается распространить практику «инструментального» аудита ИБ (по аналогии с PCI DSS) на критичные ИС в СлПО на базе национальных правил оценки текущего уровня обеспечения ИБ ИБ на периодической основе.

В этой связи отметим инициативу бизнеса по созданию «Хартии информационной безопасности критических объектов промышленности»[153]. В частности, вице-президент горно-металлургической компании «Норильский никель» В. Гасумянов пояснил: «*По нашим оценкам, в десятилетней перспективе уровень автоматизации в нашей компании превысит 80%. .... Уже сейчас совместно со службой риск-менеджмента "Норникеля" и с привлечением ведущих международных консультантов проведена работа по перспективной оценке рисков информационной безопасности компании, которые оцениваются в сотни миллионов долларов США*». В качестве примера актуальности представленного «Парадокса ИБ» (опубликованного еще в 2014 г. в [106]) рассмотрим доклад представителя ФСБ И.Лаврикова, в котором отмечена необходимость решения существующих проблем: многие международные стандарты разрабатывались в 80-90-е годы прошлого века и не удовлетворяют современным требованиям по безопасности, и более того – несоответствие зарубежных стандартов требованиям отечественных ИС и регуляторов[154]. Также отмечена необходимость унификации и стандартизации процессов, в том числе, процессов обеспечения безопасности[155].

153 https://www.kommersant.ru/doc/3496533
154 https://infoforum.ru/conference/digital_economy
155 https://www.securitylab.ru/news/488825.php

2.6 Выводы к Главе 2

1. На современном этапе развития ИТ для обеспечения требуемого уровня безопасности производимой продукции и оказываемых услуг, объективно, недостаточно только известных «классических» стандартов. Необходимое в условиях кризиса снижение издержек осуществляется за счет сокращения незапланированных потерь, которое, в свою очередь, достигается за счет внедрения эффективной системы непрерывного и всеобъемлемого управления рисками.
2. Применение современных риск-ориентированных стандартов для обеспечения комплексной безопасности СлПО особенно важно в сложившейся экономической обстановке. Это актуально как для коммерческих организаций, стремящихся сохранить и развить свой бизнес в агрессивной среде конкуренции, так и для государственных предприятий, ставящих перед собой задачи обеспечения национального промышленного паритета, реализации программ импортозамещения[156] и обеспечения «цифрового суверенитета».
3. Неоднозначность существующих различных систем оценки уязвимостей не позволяет ориентироваться на какой-либо единственный достоверный и надежный публичный источник данных, пригодный для планирования современной СМИБ (или ИСМ) для СлПО.
4. Состояние современной законодательной базы в области ИБ не позволяет в настоящее время в полной мере предложить единый методический подход и единую систему численных метрик ИБ, которые признавались всем отраслевым сообществом РФ и которые оперативно предоставляли высшему руководству СлПО объективные и непротиворечивые оценки уровня соответствия ИБ.

---

156 http://www.ng.ru/economics/2018-02-06/1_7166_import.html

3 Глава. Метод «мгновенных аудитов» ИБ

3.1 Текущая ситуация с методами обнаружения несоответствий ИБ

Для определения направлений движения к перспективным методам выполнения аудита (оценки) уровня обеспечения ИБ, целесообразно составить точное представление о текущей ситуации в данном вопросе. Крупнейшие ИТ-компании, консалтинговые группы и ведущие мировые поставщики систем ИБ предоставляют в своих отчетах информацию о текущей оценке уровня обеспечения ИБ ([395], [389], [293], [373], [390]). Представлена актуальная (2015 – 2017 гг.) для изучаемого вопроса информация [285]:

1. С мая 2015 г. компания Cisco сократила среднее время до обнаружения известных угроз (TTD) до 17 часов. Эта цифра намного превосходит текущие средние оценочные показатели TTD в отрасли, которые составляют от 100 до 200 дней.
2. Показано, что в перечне услуг представлен аудит ИБ с динамикой по предприятиям разных размеров до 56 %, также наблюдается тенденция увеличения в зависимости от размеров компании (см. рисунок 3.1).

ВСЕГО	Данные	Бразилия	Германия	Италия	Великобритания	Австралия	Китай	Индия	Япония	Мексика	Россия	Франция
Консалтинг 52 %	52 %	51 %	19 %	51 %	44 %	54 %	52 %	54 %	64 %	58 %	41 %	55 %
Аудит 47 %	50 %	55 %	38 %	48 %	50 %	36 %	33 %	51 %	41 %	63 %	40 %	59 %
Мониторинг 44 %	48 %	49 %	32 %	39 %	41 %	52 %	31 %	51 %	51 %	49 %	37 %	50 %
Реагирование на инциденты 42 %	46 %	39 %	32 %	38 %	43 %	53 %	34 %	49 %	53 %	45 %	27 %	54 %
Источник аналитики угроз 39 %	42 %	40 %	37 %	46 %	36 %	16 %	36 %	48 %	47 %	44 %	42 %	39 %
Восстановление 36 %	34 %	32 %	38 %	34 %	31 %	47 %	37 %	41 %	40 %	21 %	41 %	41 %
Нет/все внутри организации 12 %	18 %	9 %	18 %	13 %	19 %	4 %	19 %	12 %	10 %	3 %	16 %	4 %

Источник: сравнительное исследование возможностей систем информационной безопасности Cisco, 2015 г.

Рисунок 3.1 – Состав услуг в области ИБ

3. На рисунке 3.2 представлено соотношение качества инфраструктуры ИБ в различных отраслях и степеней развития «эффективность систем ИБ». Отметим, что «критичные» к качеству инфраструктуры ИБ отрасли не всегда применяют самые последние версии (обновления) ПО.

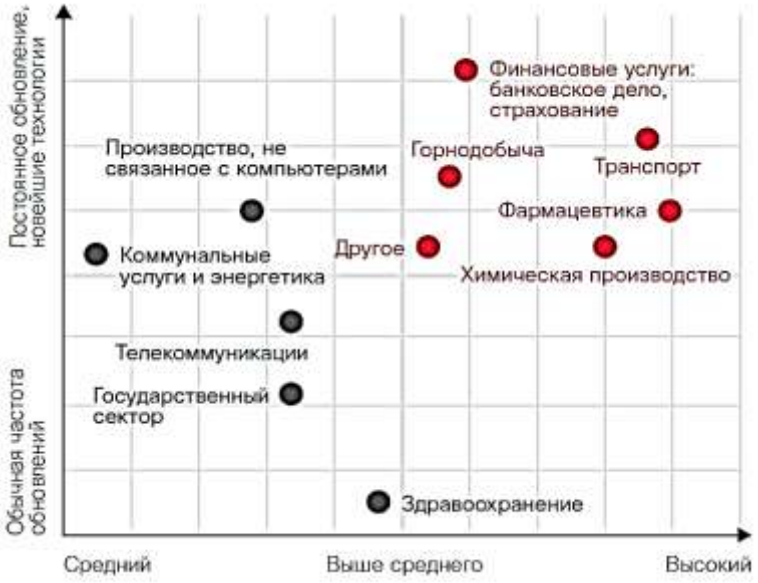


Рисунок 3.2 – Качество инфраструктуры ИБ в различных отраслях

4. На рисунке 3.3 представлено соотношение качества инфраструктуры ИБ в различных странах и степеней развития «эффективность систем ИБ».

Рисунок 3.3 – Качество инфраструктуры ИБ в различных странах

5. Анализ 115 тыс. устройств Cisco в сети интернет у заказчиков показал, что ПО в 106 тыс. устройств содержит известные уязвимости, в среднем 26 уязвимостей на одно устройство.
6. Исследование версионности ПО организаций в области финансовых услуг и здравоохранения показало, что используются версии ПО, выпущенные более 6 лет назад, т.е. уже наступил последний день поддержки (LDoS) и для них недоступны обновления безопасности.

7. Отмечается, что применение стандартизированных политик ИБ (на базе стандартов ISO 27001) постоянно увеличивается: на январь 2016 г. их применяли уже 63% организаций.
8. После известного разглашения конфиденциальной информации Э.Сноуденом «геополитическая среда управления» изменилась. Прецедентный иск М.Шремса к Facebook вызвал мощный резонанс, который побудил Судебную палату Европейского союза в 2015 г. отменить положение о «безопасной гавани» (Safe Harbor) США [377], [390].
9. Отмечается новый вектор угроз – атаки злоумышленников на данные о пациентах, т.е. продвижение атаки «горизонтально», чтобы получить контроль над системами сбора и архивирования изображений (PACS)[157].

3.2 Разработка методов и формирование метрик выполнения аудита ИБ

Проблема выполнения измерений (как процесс оценивания) для больших и/или сложных систем рассматривалась в классических трудах Н. Винера, И. Кини, Х. Райфа, И. Пригожина [13], [64], [147], [140]. Рассматривая объект – СМИБ (ИСМ) подразумевается ***открытая*** система, которая постоянно осуществляет обмен (в частности – информационный) с внешней средой. Иначе говоря, СМИБ (ИСМ) и создается для эффективного противодействия внешним негативным воздействиям среды на защищаемый СлПО. Данные воздействия могут быть описаны в пространстве параметров (метрик), по которому ЛПР объективно судит о состоянии системы в каждый требуемый (дискретный) момент времени. В настоящее время опубликованы материалы, посвященные проблеме измерения и формирования достоверных оценок результативности СМИБ ([57], [209], [69], [148], [96]). В ряде публикаций отражены подходы к управлению измерениями в ИСМ, организации системы аудита ИБ и анализа со стороны руководства. Там же показано, как эти же подходы могут быть применены в ИСМ ([96], [99]).

Предлагается для решения данной проблемы применять нормативную базу: стандарты ISO серии 27000 ([315] – [320]), а также NIST SP 800 ([369] – [372]).

---

157 infosecurity-magazine.com/news/wannacry-hits-medical-devices-in-us

Отметим, что не все специалисты однозначно точно понимают существенное различие в терминологии: «результативность» (*effectiveness*) отличается от «эффективности» (*efficiency*) [315]. Соответственно, различаются методические подходы и метрики, применяемые экспертами ИБ при измерении. Это затрудняет формирование единых объективных рекомендаций ЛПР для планирования и реализации программы необходимых измерений. В то же время успех стандартов серии 27001 привлекает внимание экспертов (см. обзор ISO [309]) и способствует унификации для ЛПР применяемых методик измерений и формированию набора метрик ИБ на базе ISO ([317], [318]).

3.2.1 Метод формирования численных метрик ИБ

Необходимо определить соответствующие заинтересованные стороны (*stakeholdes,* [315]), которым следует принимать участие в определении области измерений СМИБ (ИСМ). Результаты измерений результативности мер (средств) обеспечения ИБ (*controls,* [315]) следует определять и доводить до сведения заинтересованных сторон, которые могут быть внутренними или внешними по отношению к организации (п. 7.2 стандарта [315]). Соответственно, требуется механизм контроля передачи информации на разные интерфейсы (см. Главу 1, рисунок 1.13). Система метрик ИБ поможет поддержать принятие решений ЛПР на соответствующих уровнях иерархии ИСМ. Например, определение результативности основных видов деятельности, зависимых от степени обеспечения заданного ЛПР уровня ИБ ([110], [112]).

В «Руководстве» ([182]) отмечается, что СУ должна быть построена таким образом, чтобы быть как можно более полезной максимальному числу заинтересованных сторон, в том числе – позволять каждому заинтересованному лицу учитывать риски в его собственной зоне ответственности. Отметим исторический факт, что скорость принятия решения давно является ключевым фактором в успехе информационного противоборства – в частности, в военном деле. Известно, что в августе 1914 г. немецкий крейсер «Магдебург» был заведен на камни и были захвачены ценные шифровальные книги – в частности, «Сигнальная книга императорского флота» учетный №151. Этот успех русского

флота стал возможен благодаря длительному времени расшифрования телеграммы – 18 мин. и последующей ошибки маневрирования.

3.2.2 Выявленные противоречия

Изучение указанных выше научных работ и современной нормативной базы позволило выявить следующие противоречия:

1. Объективный факт, что значительное количество разработанных стандартов (международных, национальных, отраслевых) обуславливает широчайшую вариативность комбинаций их применения для целей обеспечения ИБ. В частности, ряд национальных стандартов ГОСТ Р «не успевают» обновляться синхронно с пересмотром международных стандартов ISO (например, ISO/IEC 27001:2013 и ГОСТ Р ИСО/МЭК 27001-2006). Более серьезные отставания демонстрируют отраслевые системы стандартизации (Журнал регистрации стандартов и рекомендаций ПАО «Газпром», стр. 337 на 01.11.2017), где отставание уже на 2 и более поколения:
   — Стандарт СТО Газпром 4.2-3-003-2009[158] СОИБ «Анализ и оценка рисков» содержит ссылку на отмененные британские стандарты BS серии 7799[159] версии 2002 г.
   — «Положение по аттестации объектов информатизации по требованиям безопасности информации», утв. председателем Государственной технической комиссии при Президенте РФ 25 ноября 1994 г.

Обратим внимание, что Британский институт стандартов опубликовал BS 7799-3:2017[160] новой версии: BS 7799-3:2017 Information security management systems. Guidelines for information security risk management[161].

2. Второе противоречие определяется тем фактом, что выбор наилучшего множества применимых метрик ИБ для оценки ИСМ по критерию наилучшего достижения поставленной цели – обеспечение заданного уровня ИБ, затруднен отсутствием механизма единственного

158 http://cn.gostinfo.ru/catalog/Details/?id=3858996
159 http://www.standards.ru/document/3858996.aspx
160 https://www.securitylab.ru/blog/personal/rusrim/343016.php
161 https://shop.bsigroup.com/ProductDetail?pid=000000000030354572

гарантированного «разумного подхода» ЛПР (в терминах Парето [141], [55]). Соответственно, возникают следующие риски:

— неверного определения (неизмеримость) целей создания СМИБ, как иерархической СУ для СлПО.

— технические решения не в полной мере обеспечивают требуемый уровень обеспечения ИБ для заданного перечня бизнес-процессов.

В дополнение к обоснованию противоречия и широчайшей вариативности комбинаций применения стандартов для целей обеспечения ИБ отметим, что по данным индекса IHS Standards Expert[162] в мире насчитывается более 2,1 миллиона международных, внутригосударственных и корпоративных технических норм и стандартов. Эти стандарты изданы более чем 370 организациями (*standards developing organizations, SDO*), такими как ISO, API, ASTM, NACE и др. От ЛПР ожидают фиксированного (ограниченного) множества критериев ИБ, размерность которого позволяет решать задачу выбора парето-оптимального множества решений с перспективой результативного применения в приемлемое время и при известных ограничениях ресурсов (финансовых, технических, персонала и пр.).

3.2.3 Базовые требования к методу формирования метрик ИБ

В аспекте данной постановки задачи важно, что в стандарте [318] определены требования к программе измерений (п. 5.2), в частности – по предоставлению результатов измерений заинтересованным сторонам для определения потребности в совершенствовании ИСМ. В стандарте [318] определены факторы, способствующие успеху программы измерений для совершенствования ИСМ, среди которых отметим две: количественную оценку мер ИБ и оценку полезности результатов измерений. Эти требования, по сути, представляют собой явный «мини-цикл» PDCA, который реализуется в ИСМ на соответствующих иерархических уровнях СМ и «снабжает» ЛПР данными для принятия эффективных управляющих решений. Метод выбора конкретных метрик ИБ должен ориентироваться на количественное измерение процесса

---

162 https://www.ihs.com/index.html

обеспечения ИБ применительно к защищаемым активам [318].В то же время в ряде публикаций ([273], [172], [377], [394], [288]) и в нормативных документах ([38], [362]) не приводятся необходимые метрики ИБ (даже самые простые), на базе которых возможно создание системы измерения результативности ИСМ (СМИБ). В частности, в ГОСТ [38] для СрЗИ приводятся только некоторые показатели живучести: рабочий диапазон температур, рабочий диапазон относительной влажности (см. таблицы №1 и №3 в [38]). В таблице 1 стандарта [38] приведена номенклатура показателей качества, которая может быть дополнена из приложения «С» [319] в части уязвимостей, например: «Оценка уязвимостей» (п. 1.2.7 [38]). Более того, даже в современных отчетах (например, «The 2017 State Of Cybersecurity Metrics Annual Report”[163]) даются оценки крайне неблагополучного процесса формирования метрик ИБ – как осознания собственно такой необходимости, выбора применимых метрик, оценки процессов ИБ и, самое важное – вынесение результатов на уровень руководства для принятия оперативных и адекватных решений.

3.2.4 Новые категории метрик ИБ

С учетом сказанного ранее, могут быть предложены различные категории метрик ИБ, унифицированных к типу защищаемых активов организаций, например: простые метрики, сложные метрики и комплексные метрики.

— Простые метрики (например, количество выявленных инцидентов и событий ИБ, количество предотвращенных утечек ПДн, количество проведенных по плану аудита ИБ и пр.);
— Сложные метрики (например, отношение стоимости мер защиты к стоимости защищаемых активов и пр.);
— Комплексные метрики (например, число произошедших инцидентов ИБ, приведших к ущербу (вынужденному простою) в ИС, определенных как критичные для бизнеса).

163 https://thycotic.com/wp-content/uploads/2013/03/2017-Cyber-Security-Strategy-Metrics-Report.pdf

Отметим влияние «объективисткого подхода» (в терминах Перегудова Ф.И. см. [151], стр. 121), в соответствии с которым в конкретной реализации СМИБ (или ИСМ) невозможно обойтись без измерения ряда величин, порядка формирования методик таких измерений и соответствующих правил оценивания адекватности полученных результатов – применительно к целям обеспечения безопасности СлПО. В качестве критериев разделения метрик ИБ на указанные категории предлагается использовать следующие правила:

— Простые метрики могут быть получены напрямую специалистами службы ИБ через технические средства или по результатам анализа мероприятия ИБ (например, анализ «логов» SIEM, IPS, DLP, FW и пр.);
— Сложные метрики вычисляются на основании простых метрик и требуют привлечения дополнительно специалистов иных служб (например, оценка стоимости защищаемых активов требует данных от финансово-экономических подразделений);
— Комплексные метрики вычисляются на основании сложных метрик и требуют привлечения высшего менеджмента, ответственного за безопасное выполнение определенных бизнес-процессов. Кроме того, учитывая прямое отношение комплексных метрик к защищаемым активам и оценку, в том числе, и ущерба, для расчета данной категории метрик ИБ должен допускаться ограниченный ряд менеджеров.

При реализации на конкретном проекте оценки результативности СМИБ (ИСМ), правила определения и градация метрик ИБ могут выбираться ЛПР на основании своих (реже отраслевых) предпочтений.

3.2.5 Требования к выбору метода измерения

Для каждой отдельной основной меры измерения должен быть определен метод измерения, который используется для количественного определения объекта измерения путем придания атрибутам значения, соответствующего основной мере измерения [318]. Рекомендуется применять объективный метод измерения, который использует количественные оценки, и может быть реализован «*машинным*» способом (например: IPS, SIEM, DLP, GRC). Важно,

что в терминах ФЗ-102 «Об обеспечении единства измерений» указан класс таких средств: «*технические системы и устройства с измерительными функциями – технические системы и устройства, которые наряду с их основными функциями выполняют измерительные функции*». Это позволяет говорить о применении – именно для практической цели получения автоматических «*машинных данных*» для формирования общей количественной оценки уровня ИБ в ИСМ для СлПО. Метод измерения должен оставаться единообразным с течением «оперативного» времени (при замыкании «мини-цикла» PDCA), с тем, чтобы значения, приданные основной (производной) мерам измерения и полученные в разное время, были бы сопоставимыми [318].

3.2.6 Применение теории элитных групп для отбора метрик ИБ

Для отбора наилучшей, в смысле решения поставленной задачи, совокупности метрик ИБ предлагается применять базовые положения «элитных групп» (предложены А.Н. Ефимовым) [55]. В базовом варианте имеется совокупность элементов счетного множества **Y** (в новом варианте предложено специфицировать множество метрик ИБ). Свойство каждого элемента выражается определенной критериальной величиной $\mathbf{y_i}$, находящейся в диапазоне $\mathbf{0 \le y \le 1}$, и известно, что чем больше значение достигает $\mathbf{y_i}$, тем лучше. В частности, это требование точно соответствует задаче оценки конкретного атрибута – чем лучше его «абсолютная» оценка безопасности, тем лучше, и тем выше общая оценка измерения результативности СМИБ (ИСМ). Известна цель: $\mathbf{0 \le \alpha \le 1}$ и известно требование – достижение цели с условием, чтобы определенный показатель качества был не ниже заданной величины $\mathbf{\alpha \le 1}$. Задача формируется как отбор из исходного множества **Y** заданного количества элементов для достижения поставленной цели с заданным ЛПР показателем качества. В множестве **Y** могут присутствовать и элементы $\mathbf{y_i}$, для которых выполняется $\mathbf{y_i \ge \alpha}$ (называемые «*элитные*» элементы) и $\mathbf{y_i \le \alpha}$ (называемые «*сорные*» элементы).

Отметим, что в «Руководстве» ([182]) описан практический подход, реализуемый NATO и отдельными организациями, при проведении регулярных

учений по кибербезопасности[164]. В зависимости от цели учений, для важнейших объектов критичной инфраструктуры оцениваются различные режимы систем управления ЧС[165]. Такие учения дают возможность оценить постоянно изменяющийся «*ландшафт риска*» с тем, чтобы адаптироваться к постоянным изменениям стандартов, концепций и отдельных мер безопасности.

В **новом** предложенном методе экспертам рекомендуется элементы $\mathbf{y_i}$ выбирать случайно, что является, во-первых, требованием стандарта [317] по формированию «выборки аудита» (*audit sample*) и, во-вторых, должно исключить на практике случаи «подгонки» множества элементов **Y** под заранее заданный результат **α.** Таким образом, предложенное новое распределение качества **Y** в определенной «элитной» группе может характеризоваться новой плотностью распределения [55]:

$$F_{Elite\ New}(y) = \left\{ \gamma \frac{\beta}{F(\alpha)} f(y): y < \alpha; (1-\gamma) \frac{1-\beta}{1-F(\alpha)} f(y): y \geq \alpha \right\} \quad (3.1)$$

где:

$F_{EliteNew}(y)$ *– функция распределения качества y в исходной группе;*

α *– показатель качества;*

β *– вероятность отбора в элитную группу «сорных» элементов;*

γ *– вероятность отбора в элитную группу ранее не использованных элементов;*

$f(y)$ *– соответствующая плотность распределения.*

Важно, что если в силу ряда причин, элементы отобранной «элитной» группы могут выбывать, но требуется сохранить «представительность» данной группы для целей измерения (например, для целей измерения в процессе аудита ИБ определенного фиксированного количества процессов СМИБ и/или ИСМ), то необходимо решать задачу повторного выбора элементов из оставшейся базовой совокупности **Y**. **Новый** алгоритм применения «элитных групп» для целей измерений результативности СМИБ показан на рисунке 3.4.

---

164 http://www.enisa.europa.eu/activities/Resilienceand-CIIP/cyber-crisis-cooperation/cyber-europe (02/13/2013)

165 http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Sonstiges/Infos_ueber_Luekex.html (02/13/2013)

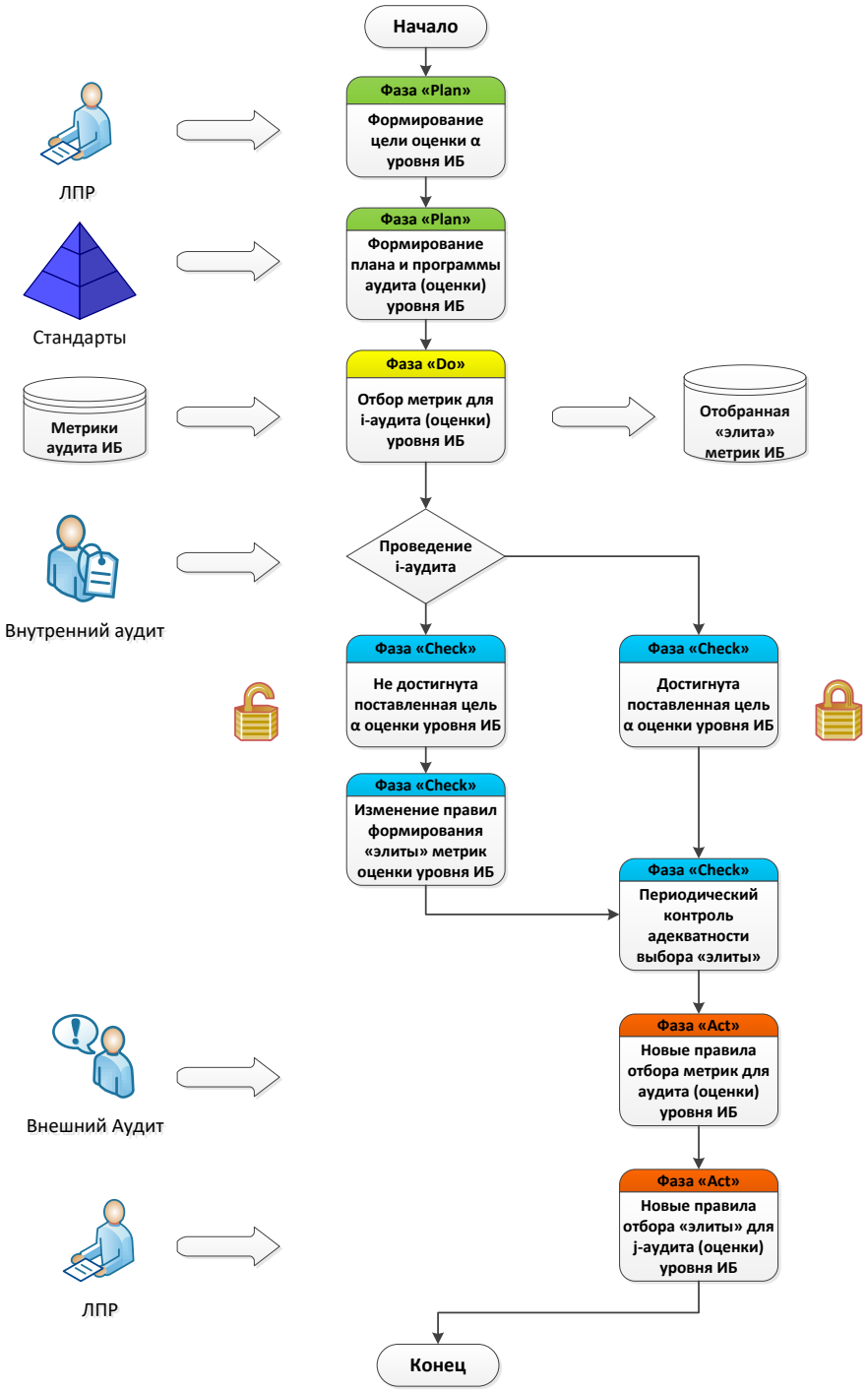


Рисунок 3.4 – Алгоритм применения «элитных групп» для СМИБ

Для развития базовой теории «элитных групп» для применения в целях управления аудитом ИБ в представленном алгоритме введены новые функции в строгом соответствии с циклом PDCA. Рекомендуется принять во внимание (применительно к аудиту ИСМ) ряд принципиально **новых** обстоятельств:

— необходимо ориентироваться, прежде всего, на долю «элитных» элементов, удовлетворяющих $\mathbf{y_i \geq \alpha}$, но ранее не отобранных для аудита в течение одного полного замкнутого цикла программы аудита;

— необходимо отслеживать характер изменения «качества» каждого отобранного «элитного» элемента, а при наличии достаточных ресурсов – всей совокупности «элитных» элементов, в т.ч. «резерва» множества **Y**;
— необходимо формировать правила выбора, ротации и отсева «элитных» элементов (на практике это означает пересмотр метрики ИБ по итогам, например, внутреннего аудита СМИБ и/или ИСМ).

Определим объективные сложности разработки методов формирования метрик ИБ для измерения результативности СМИБ, которые заключаются в том, что требуется минимально:

— сформировать методику измерения, дающую воспроизводимые и достоверные результаты оценки;
— предложить метод сравнения с мерой (различных разновидностей – дифференциальный, замещения, дополнения, совпадения и пр.);
— сформировать систему метрик ИБ для оценки результативности СМИБ;
— доказать ЛПР, что выделенный бюджет на СМИБ позволяет достигать поставленных задач обеспечения ИБ;
— определить перечень применяемых средств измерений, алгоритмов обработки результатов измерений и оценки показателей точности.

Для процесса формирования, анализа и сравнения метрик ИБ «базовым» является применение «целевого» стандарта ISO 27001 [317]. Ниже будет представлена методика измерения результативности СМИБ и пример формирования численных (количественных) показателей (метрик ИБ) для выполнения независимой оценки (аудита ИБ).

3.2.7 Многокритериальная задача для оценки результативности ИСМ

Для оценки результативности СМИБ необходимо применять численные критерии, при этом возможно применять сложные многокритериальные показатели. В ряде изданий показано, как можно свести решения сложных многокритериальных задач к решению однокритериальных [64], [147]:

$$q_0(x) = q_0\left(q_1(x), q_2(x), \ldots q_r(x)\right)$$

В данном случае суперкритерий ***q₀ (x)*** позволяет упорядочить альтернативы, выделив наилучшую (для данного критерия). Отметим, что подробное обоснование и примеры приведения многокритериальной задачи к однокритериальной (в частности, для формирования оптимального подходящего суперкритерия) рассмотрены в ряде публикаций: ([151], стр. 208 и стр. 322). Кроме того, данные примеры приведены в работе ([64], стр. 9) с тем предупреждением, что ЛПР не может просто взять и поставить ряд значений различных «несоизмеримых» показателей (критериев) в некоторую сборку, которую «кто-то предложил в отрыве от реальной ситуации». Вид функции ***q₀ (x)*** определяется по способу представления собственного вклада каждого критерия в суперкритерий. Этот вклад может быть оценен в виде различных функций (например, аддитивных или мультипликативных):

$$q_0 = \sum_{i=1}^{r} \frac{a_i q_i}{S_i} \qquad (3.2)$$

$$1 - q_0 = \prod_{i=1}^{r} \left(1 - \frac{\beta_i q_i}{S_i} \right) \qquad (3.3)$$

где:

— α_i *и* β_i *отражают вклад каждого частного критерия в суперкритерий;*

— S_i *в формулах обеспечивают безразмерность отношения* q_i / S_i, *т.к. частные критерии могут иметь различную размерность (см. выше примеры простых метрик ИБ – время, количество, частота)*

Соответственно, решение задачи сводится к максимизации единственного супер-критерия:

$$\boldsymbol{Q = arg\ x\ [max\ (q_0\ (q_1(x), q_2(x), \ldots q_r\ (x))\ ]}$$

Супер-критерий играет важную роль при оценке поведения системы при изменении различных альтернатив. Например, выбор новой альтернативы при элементарной замене коэффициентов в функции (3.2) вида **Z = αX + βY (**случай аддитивной функции для СМИБ) может вызвать значительное изменение наклона прямых (см. расчет по практическим кейсам в Главе 5 соответственно).

Решение поставленной задачи имеет и другой вариант – поиск альтернативы, наиболее удаленной от нуля, стремящейся к 1, которая, очевидно, соответствует наилучшим ожиданиям ЛПР при известных бюджетных затратах на СМИБ. В частности, можно использовать следующий вариант максимизации минимального критерия [147]:

$$X^{\text{»}} = \arg max_{x \in X} \left\{ min_i \left[\frac{a_i \, q_i(x)}{S_i} \right] \right\}$$

Дополнительно рекомендуется применение критерия «пессимизма-оптимизма» (критерий Гурвица), который оперирует взвешенной комбинацией наилучшего и наихудшего исхода для исследуемой альтернативы $\mathbf{x_i}$.

$$\mathbf{R\,(x_i) = \alpha\ min\ q_{ij} + (1 - \alpha)\ max\ q_{\,ij}, \quad 0 \le \alpha \le 1}$$

где α – показатель пессимизма-оптимизма, при α = 1 имеем максимальный критерий и оптимальная альтернатива есть:

$$\mathbf{X'' = arg\ max\ R\,(x_i)}$$

3.3 Реализация годовой программы аудита

В фундаментальной работе Г. Николиса и И. Пригожина [140] отмечено, что при большем отклонении от равновесия и при достижении определенного критического порога возможно расслоение стабильной ранее структуры. Там же приводится тезис Аристотеля, что свойства пространства определяются событиями, выполняемыми в данной определенной системе координат ([140], стр. 18). Таким образом, для оценки начала «сваливания» стабильной ранее системы (СУ конкретного СлПО) необходимо реализовать всеобъемлемую систему аудита, как механизм независимой, непрерывной и системной внешней оценки «смещений», возникающих в заданной «системе координат» СУ. Известно, что для неконсервативных систем неравновесные состояния характеризуются неисчезающими потоками обмена между системой (некоторой «системной оболочкой», в конкретном случае – СУ определенного типа) и внешней средой ([140], стр. 70). Режим неравновесного состояния системы обеспечивает возможность изменений, т.е. небольшие изменения не обязательно приводят к структурным изменениям (в пределе – к «сваливанию», к

разрушениям). Важно, что они могут по итогам успешной и результативной реализации программы аудита стать источником эволюционного развития исследуемой системы (СлПО). Рассмотрим пример нормальной программы аудита ИСМ, т.к. это принято в соответствии с известными стандартами ([20], [21]). В таблице 3.1 показан пример годовой программы аудита некоторого СлПО, причем показаны как плановые (**пл**), так и неплановые (**н/пл**) аудиты.

Таблица 3.1 – Пример годовой программы аудита

№ аудита	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Тип аудита	пл	пл	н/пл	пл	пл	пл	пл	пл	н/нл	пл	пл	пл	пл	пл
Кол-во н/с	**9**	**8**	**9**	**7**	**10**	**8**	**9**	**8**	**9**	**10**	**7**	**9**	**10**	**12**
Кол-во проверяемых подразделений	4	4	2	4	5	4	5	5	2	6	4	5	4	4

Поскольку состояние реальных СУ никогда не остается стабильным во времени (постоянным по отношению к дате проектирования и/или создания), т.к. они контактируют с внешней средой, важно оценить роль внешней среды. Именно внешняя среда является источником всех изменений параметров состояний, что делает, по некоторым оценкам, невозможным полный тотальный контроль с высокой точностью ([140], стр. 81). Точность управления зависит от полноты, достоверности и скорости предоставления данных по всем изменениям параметров состояния системы. Таким образом, роль программы внутреннего аудита СМИБ (ИСМ) может быть сведена к «доставке» ЛПР объективных, достоверных и независимых оценок о состоянии конкретной СУ с заданной частотой. График выявленных несоответствий представлен на рисунке 3.5. Покажем важность роли годовой программы аудита СМИБ (ИСМ) на одном важном весьма показательном примере – компрометации данных аудиторской компании Deloitte. В статье «Deloitte Breach Affected All Company Email, Admin Accounts»[166] описан взлом БД одной из крупнейших аудиторских компаний мира.

[166] https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/

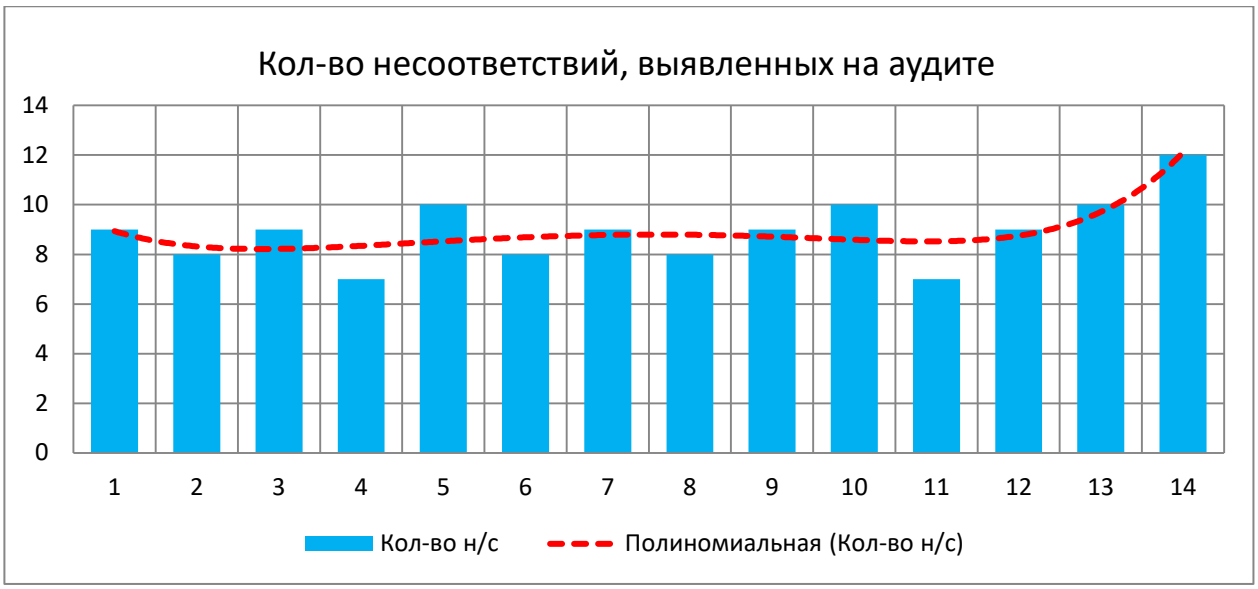


Рисунок 3.5 – График выявленных несоответствий по аудитам

По данным исследователей, на незащищенных серверах Amazon Web Services хранилось более 137 ГБ конфиденциальных данных, в том числе 40 тыс. паролей, данные учетных записей, включая IP-адреса[167], утечка была обнаружена Крисом Викери (Chris Vickery)[168]. Отметим, что для доверителей конфиденциальной информации проведение периодического аудита ИБ, даже для компании уровня Deloitte, представляется нелишней. Еще один характерный пример касается важности защиты самих данных аудита (даже если они выполняются не регулярно). В частности, лондонский аэропорт Хитроу в 2017 г. начал внутреннее расследование после того, как на улице был найден USB-накопитель с конфиденциальной информацией[169]. Этот накопитель содержал график патрулирования объектов, карты с расположением камер наблюдения, информацию о системе проверки состояния взлетно-посадочных полос и ограждений. Всего на накопителе было 2,5 Гб данных[170].

Рассмотрим практическую задачу статистического анализа результатов годовой программы аудита СМИБ (ИСМ) с применением дискретных вариационных рядов и построения кривой нормального распределения. Известно, что непрерывная случайная величина **x** имеет нормальное

167 www.securitylab.ru/news/489044.php
168 https://www.upguard.com/breaches/cloud-leak-accenture
169 http://www.rbc.ru/society/29/10/2017/59f5ceee9a7947190808f524?from=newsfeed
170 http://www.mirror.co.uk/news/uk-news/terror-threat-heathrow-airport-security-11428132

распределение (или распределение по нормальному закону) в том случае, если плотность распределения вероятности ***f (x)*** имеет вид ([11]):

$$f\ (x) = \frac{1}{\sigma_x \sqrt{2\pi}} e^{\frac{-(x- M_x)^{\ 2}}{2\ \sigma_x^{\ 2}}} \qquad (3.4)$$

где:

M_x *– математическое ожидание случайной величины x,*

σ_x *– среднее квадратическое отклонение*

Известно, что функция распределения *F (u)* имеет вид ([11]):

$$F\ (u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{\frac{-\ t^{\ 2}}{2}}\ dt \qquad (3.5)$$

где:

$$u = \frac{\mathrm{x} -\ M_x}{\sigma_x}$$

Известно, что вероятность попадания случайной величины **x** в интервал **(a; b)** определяется следующим образом ([11]):

$$P\ (a\ \leq x\ \leq b) = \mathrm{Z}\left(\frac{\mathrm{b} -\ M_x}{\sigma_x}\right) - \mathrm{Z}\left(\frac{\mathrm{a} -\ M_x}{\sigma_x}\right) \qquad (3.6)$$

где:

$$Z\ (u) = \frac{1}{\sqrt{2\pi}} \int_{0}^{u} e^{\frac{-\ t^2}{2}}\ dt$$

Таким образом, для **3σ** получаем вероятность попадания случайной величины **x** в интервал **(a; b)**, равную 0,997. Это означает на практике, что случайная величина **x**, распределенная по нормальному закону (3.4), находится в интервале **+/– 3σ.** Для приведенного примера (см. таблицу 3.1) определим основные показатели (для анализа статистики несоответствий):

— Среднее число несоответствий (на аудит) $N_{ср}$ = 8,328

— Дисперсия D = 1,763

— Среднее квадратичное отклонение σ = 1,328

В том случае, если исходное частотное распределение вариационного ряда (см. рисунок 3.5) отличается довольно большим разбросом значений, возможно

перейти к интервальному вариационному ряду, объединяя частоты для определенного количества несоответствий (или подразделений), попадающих в соответствующие интервалы. Число интервальных групп **K** (для несоответствий) определим по формуле Стерджесса ([67]):

$$\mathbf{K = 1 + \log 2\ N = 1 + 3{,}322 \lg N}$$

где

N = 125 – объем выборки по приведенному примеру аудита.

Для примера $K = 1 + 3{,}322 \times \lg(125) = 1 + 3{,}322 \times 2{,}09 = 7{,}965 \approx 8$.

Ширина интервала для примера равна $(12 – 7) / 8 = 0{,}625 \approx 0{,}63$.

Результат расчета частотного интервального вариационного ряда программы аудита ИСМ представлен в таблице 3.2.

Таблица 3.2 – Частотный интервальный вариационный ряд аудита

№ интервального вариационного ряда:	1	2	3	4	5	6	7	8
Диапазон значений ряда:	7	7,63	8,25	8,88	9,50	10,13	10,75	11,38
	7,63	8,25	8,88	9,50	10,13	10,75	11,38	12,00
Кол-во несоответствий	7	16	24	27	18	10	11	12

График распределения по вариационным рядам представлен на рисунке 3.6.

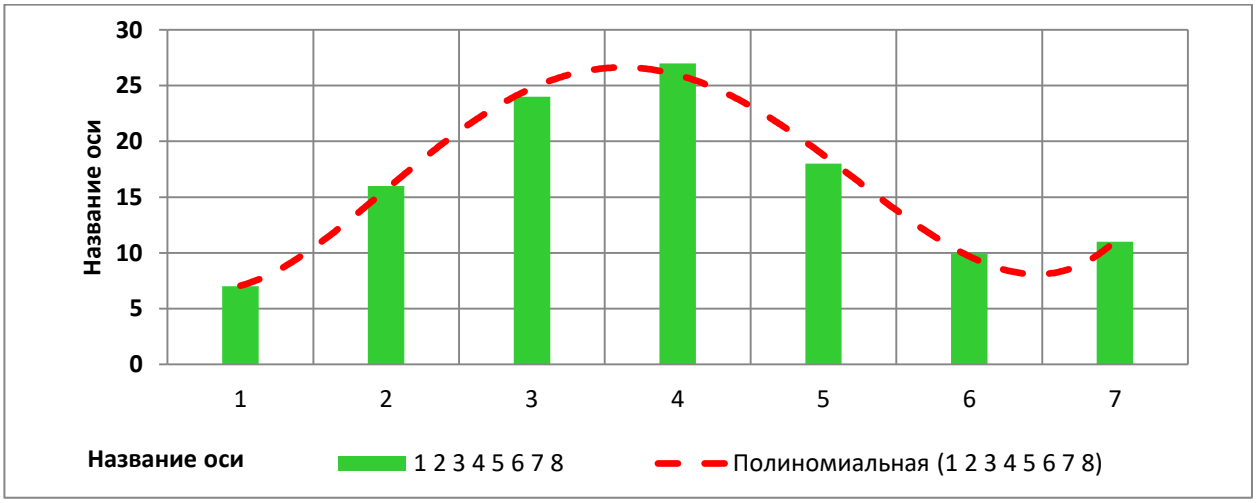


Рисунок 3.6 – График выявленных несоответствий по аудитам

Вид гистограммы на рисунке 3.6 позволяет сделать предположение о том, что распределение несоответствий аудита подчиняется нормальному закону, и кривая нормального распределения (Гаусса), в целом, соответствует эмпирическому интервальному распределению. Для более детального изучения

вопросов статистической значимости можно применять критерии Пирсона ([11], [67]). В то же время, в работе Г. Николиса и И. Пригожина отмечается, что проблема изучения состояний, далеких от равновесия, приводит к появлению новых «*веток решения*» в результате процесса бифуркации ([140]). Там же отмечается, что во многих случаях полная спецификация всех параметров исследуемой системы не имеет смысла, и в ряде случаев практически целесообразно применение вероятностного подхода ([140], стр. 103). Отдельно отметим, что в ряде работ отмечается неприменимость Марковских цепей для оценки состояния всех параметров сложных систем, т.к. запоминается только крайнее положение (переход состояния). Это ограничение позволяет анализировать только самые простые случаи и только с применением сложных и ресурсоемких методов численного моделирования ([140], стр. 181). Для анализа СлПО посредством аудита необходимо анализировать несколько предшествующих состояний по группе параметров, что позволяет обеспечить ЛПР принятие разумных управляющих решений ([89], [92]).

3.4 Методы оценки степени соответствия ИБ

3.4.1 Базовые требования

В работе М. Месаровича, Д. Мако и И. Такахара [127] отмечается, что «*число ученых, занятых оптимальным подбором параметров в системах с обратной связью значительно больше, чем число ученых, интересующихся качественным аспектом управления*». В определенном смысле, аудит как процесс получения численной оценки степени соответствия некоторой конкретной СУ заданным требованиям, можно рассматривать как инструмент «*добивающегося удовлетворения администратора*» в терминах Марча и Саймона ([127], стр. 37). Для оценки степени соответствия системы обеспечения ИБ в определенной СМ (СМИБ или ИСМ) установленным требованиям ИБ (в терминах ISO 19011 – «*критерии аудита*» [20]), используются частные и групповые показатели ИБ. Для формирования числовой оценки СМИБ и ИСМ, в строгом соответствии с требованиями «базового» стандарта аудита [20], представляется целесообразным применять и иные стандарты (в частности [21],

[318]). Подробно **новые** математические оценки степени соответствия ИСМ (СМИБ) представлены в Главе 5. Процесс оценки степени соответствия СМИБ (ИСМ) возможно реализовать в рамках систематического процесса аудита, т.е. выполнять постоянное измерение и анализ в рамках аудита ИБ. В таком случае, в процессе реализации годовой программы аудита ИБ возможно оценить как общее «глобальное» отклонение, так и «локальные» отклонения (в терминах Р. Кини и Х. Райфа [64]) по установленным критичным процессам СМИБ (ИСМ). Для реализации программы аудита ИБ вполне достаточно указанных выше стандартов ISO (ГОСТ Р ИСО), однако, для практического применения для целей оценки степени соответствия СМИБ (ИСМ) необходимо дополнительно рассмотреть ряд существующих моделей и оценить их преимущества.

3.4.2 Модель аудита в комплексе СТО БР ИББС

В практике проведения аудита в области ИБ для КО БС Российской Федерации применяется комплекс стандартов СТО БР ИББС [217] – [220]. Так же указано (п. 8.14.1 [219]), что аудит ИБ организации БС РФ должен проводиться в соответствии с требованиями стандартов Банка России СТО БР ИББС-1.1 и СТО БР ИББС-1. В стандарте [219] (раздел 6) установлено, что для оценки степени соответствия обеспечения ИБ организации требованиям СТО БР ИББС-1.0 используются групповые и частные показатели ИБ. Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки текущего уровня ИБ организации, менеджмента и уровня осознания ИБ [219]. Отметим новацию ЦБ РФ – стандарт ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», который вступил в действие 01.01.2018[171]. Этот стандарт содержит требования к организации процессов ИБ, включая противодействие ВПВ, утечкам информации, нарушению целостности и угрозам при удаленном доступе с использованием мобильных устройств. Отметим, что в стандарте определены требования к защите информации на всех этапах ЖЦ АС и предусмотрена оценка

[171] https://www.eg-online.ru/news/352250/

остаточного операционного риска. Отметим и новые термины, планируемые ЦБ РФ к введению, прежде всего «*сквозного идентификатора*». В этом случае речь идет о создании технологической связки между платформами разных ведомств РФ, в базах которых хранятся цифровые идентификаторы граждан[172]. В ЦБ РФ также разработаны «Рекомендации по защите объектов информационной инфраструктуры кредитно-финансовой сферы в период проведения в РФ чемпионата мира по футболу»[173].

Аудит БС в РФ является жизненно необходимым. Например, известно, что в феврале 2016 г. со счета Металлинвестбанка исчезло более 600 млн. руб.[174]. Атака реализована через АРМ клиента Банка России, с которого ведётся управление счетом. По словам экспертов, за инцидентом в Металлинвестбанке и ещё, как минимум, 13 взломами, стоит группировка Buhtrap, члены которой задержаны в июне 2016 г. Другой случай произошел на Московской бирже в феврале 2015 г., во время торгов курс рубля снизился на 15%, и один из трейдеров (казанский «Энергобанк») продавал валюту по явно «нерыночным» ценам. За 15 мин. «странной» торговли потери составили 243,6 млн. руб. По некоторым данным, это была месть сотрудника за увольнение[175]. В сентябре 2016 г. в Петербурге всего за пять часов из банкоматов было украдено 12,6 млн руб. В них обнаружили отверстия диаметром 4 см., а через него неизвестные подключились к блоку управления банкомата, Эксперты полагают, что работа мошенников была бы невозможной без подельника внутри.

Отметим, что в феврале 2017 г. в журнале "Внутренний контроль в кредитной организации" № 1 (33) 2017 опубликовано интервью с зам.начальника ГУБиЗИ Банка России А.Сычевым, в котором анонсированы ближайшие планы Банка России по повышению киберустойчивости финансового рынка[176]. В частности, объявлено, что в планах Банка России исключить самооценку ИБ в кредитных организациях как метод подтверждения соответствия требованиям.

---

172 https://www.kommersant.ru/doc/3541951?from=four_finance

173 http://www.cbr.ru/fincert/rekomendacii-po-zaschite-ob-ektov-informacionnoy-infrastruktury-kreditno-finansovoy-sfery-v-period-provedeniya-v-rossiyskoy-federacii-chempionata-mira-po-futbolu-2018/

174 https://habrahabr.ru/company/itinvest/blog/332080/

175 http://www.banki.ru/news/daytheme/?id=10391123

176 http://www.securitylab.ru/blog/personal/estekhin/342536.php

Иными словами, роль независимого аудитора постепенно признается отраслевым регулятором.

В то же время известно, что КО РФ в течение 2017 г. не сообщили в FinCERT о каждой пятой успешной атаке хакеров. Банкиры не доверяют структуре, созданной внутри ЦБ для обеспечения ИБ, очевидно, опасаясь привлечь надзорное внимание регулятора. По словам В.Матвеевой (Group-IB), атакам Cobalt были подвержены банки разного масштаба, суммы хищений варьировались от нескольких миллионов до полумиллиарда[177]. Результаты аудита, как численная оценка уровня осознания ИБ в КО, определяются с помощью метрик групповых показателей, например, M_{28} – M_{34}, значения которых из одного реального проекта представлены в таблице 3.3.

Таблица 3.3 – Значения групповых показателей M_{28} – M_{34}

Обозначение группового показателя	Наименование группового показателя	Значение группового показателя	Структурный элемент СТО БР ИББС-1.0
M_{28}	Оценка деятельности руководства организации БС РФ по поддержке функционирования службы ИБ	0,93	п. 8.2
M_{29}	Оценка деятельности руководства организации БС РФ по принятию решений о реализации СОИБ	1	п. 8.7
M_{30}	Оценка деятельности руководства организации БС РФ по поддержке планирования СОИБ	0,9	п.п. 8.3, 8.4, 8.5, 8.6, 8.8
M_{31}	Оценка деятельности руководства организации БС РФ по реализации СОИБ	0,86	п.п. 8.9, 8.10, 8.11
M_{32}	Оценка деятельности руководства организации БС РФ по поддержке проверки СОИБ	0,62	п.п. 8.12, 8.13, 8.14, 8.15
M_{33}	Оценка деятельности руководства организации БС РФ по анализу СОИБ	0,72	п. 8.16
M_{34}	Оценка деятельности руководства по поддержке совершенствования СОИБ	0,63	п.п. 8.17, 8.18

В соответствии с требованиями СТО БР ИББС перед высшим руководством КО стоит задача достижения требуемого уровня соответствия ИБ $R \geq 4$ [220]).

[177] https://www.kommersant.ru/doc/3474979

Круговая диаграмма, отображающая текущие оценки групповых показателей M_1 – M_{34}, представлена на рисунке 3.7. Круговая диаграмма, отображающая текущие результаты оценки по соответствующим направлениям оценки EV_1, EV_2, EV_3, представлена на рисунке 3.8. Значение R определяется по наименьшей из трех оценок по направлениям оценки EV_k и равно (в примере) 0,701, что соответствует третьему уровню соответствия ИБ в КО требованиям СТО БР ИББС-1.0-2014.

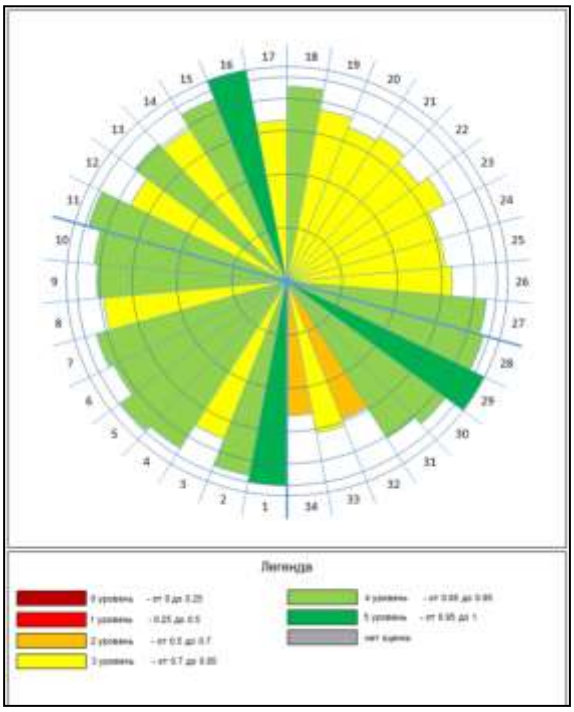


Рисунок 3.7 – Круговая диаграмма, отображающая текущие оценки групповых показателей M_1 – M_{34}

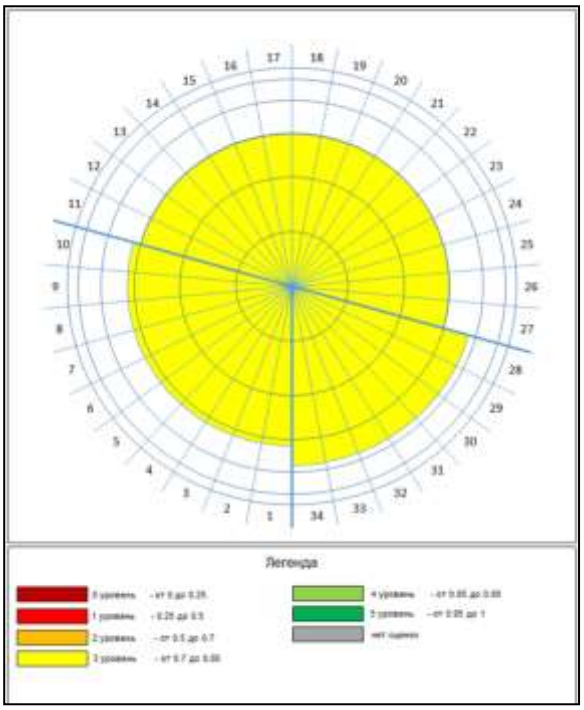


Рисунок 3.8 – Круговая диаграмма, отображающая текущие оценки EV_1, EV_2, EV_3

Представляется важным обратить внимание на определение оптимального перечня организационно-распорядительной документации по ИБ, которая позволяет обеспечить соответствие по частным показателям, требующим документирования согласно [220]. При определении перечня документов необходимо учитывать тот факт, что один нормативный документ СОИБ в КО может успешно «закрывать» несколько требований:

— «Политика менеджмента инцидентов ИБ» является подтверждением выполнения требований: $M_{1.4}$ – $M_{1.5}$, $M_{3.22}$ – $M_{3.23}$, $M_{3.28}$, $M_{3.32}$;

— «Политика ИБ» является подтверждением выполнения более 20 требований: $M_{15.1}$ – $M_{15.4}$, $M_{15.19}$ – $M_{15.22}$ и пр.

— «Политика инцидентов ИБ» является подтверждением выполнения требований: $M_{20.3}$ – $M_{20.4}$, $M_{20.7}$, $M_{20.11}$ – $M_{20.13}$.

В продолжение этого требования также необходимо формировать документационное обеспечение аудита ИБ (подробнее данный вопрос будет исследован далее в Главе 5 и Главе 6). Важное значение необходимо уделить объективному, достоверному и адекватному документальному обеспечению аудита ИБ, иначе говоря: сбору и подробному анализу «свидетельств (доказательств) аудита» (в терминах п. 3.12 стандарта [220]). Повышение уровня ИБ в КО до рекомендуемого четвертого уровня возможно за счет устранения полного (для частных показателей с оценкой «0») или частичного (для частных показателей с оценкой от «0» до «1») несоответствия требованиям, определенным в частных показателях. В рамках приведенного одного полного цикла программы аудита ИБ в конкретном проекте КО, был проанализирован весь перечень показателей (метрик) ИБ и ЛПР было принято решение, что для КО наиболее рациональным является улучшение определенного ряда показателей.

Пример рекомендуемых мер по повышению оценки степени соответствия обеспечения ИБ по направлению «Менеджмент ИБ» приведен в таблице 3.4. Соответственно, круговая диаграмма, отображающая целевые (которые могут быть получены по результатам принятия рекомендованных мер по повышению уровня обеспечения ИБ) оценки групповых показателей M_1 – M_{34}, представлена на рисунке 3.9. Круговая диаграмма, отображающая целевые (которые могут быть получены по результатам принятия рекомендованных мер по повышению уровня обеспечения ИБ) результаты оценки по соответствующим направлениям оценки EV_1, EV_2, EV_3, представлена на рисунке 3.10.

Таблица 3.4 – Рекомендуемые меры повышения оценки степени соответствия

Обозначение частного показателя	Текущая оценка частного показателя	Целевая оценка частного показателя	Рекомендуемые меры
M13.7	0	1	▪ рекомендуется внести изменения в документацию СОИБ в части анализа рисков в Банке (Положение по анализу рисков); ▪ рекомендуется установить период пересмотра рисков (и их градации), например, ежемесячно.
M22.2	0	1	▪ рекомендуется рассмотреть отчет по выполненной ранее самооценке и выполнить новую самооценку на соответствие актуальной версии СТО БР ИББС-1.0-2014; ▪ рекомендуется пересмотреть следующие документы: «Положение о внешнем аудите», «Политика ИБ»
M15.4	0,5	1	▪ Рекомендуется пересмотреть содержащиеся во внутренних документах требования по обеспечению ИБ с учетом выявленных в ходе классификации активов
M20.8	0,5	1	▪ рекомендуется внести изменения в документацию СОИБ в части тестирования плана обеспечения непрерывности бизнеса в Банке (Политика инцидентов ИБ, План действий в чрезвычайных ситуациях)

Важным представляется тот факт, что выполнение самооценки, равно как и внешней оценки, выполняется по единым правилам, на основании единого опубликованного стандарта, что позволяет высшему руководству КО располагать определенным «маневром» относительно диапазона изменения набора «*сорных*» (в нотации Ефимова) показателей (метрик) ИБ.

В практике выполнения проектов независимой оценки ИБ был сделан вывод, что результаты оценки (самооценки) СОИБ имеют непосредственное отношение к задаче совершенствования уровня ИБ в КО. Более того, в развитии данного предположения, определено, что эта задача имеет важное практическое

приложение при решении совместно задачи максимизации групповых показателей M_1 – M_{34}.

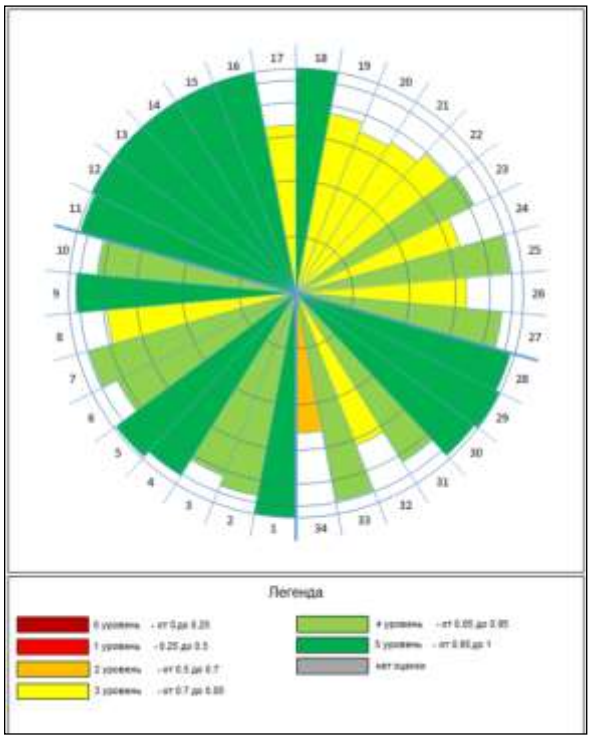


Рисунок 3.9– Круговая диаграмма, отображающая целевые оценки групповых показателей M_1 – M_{34}

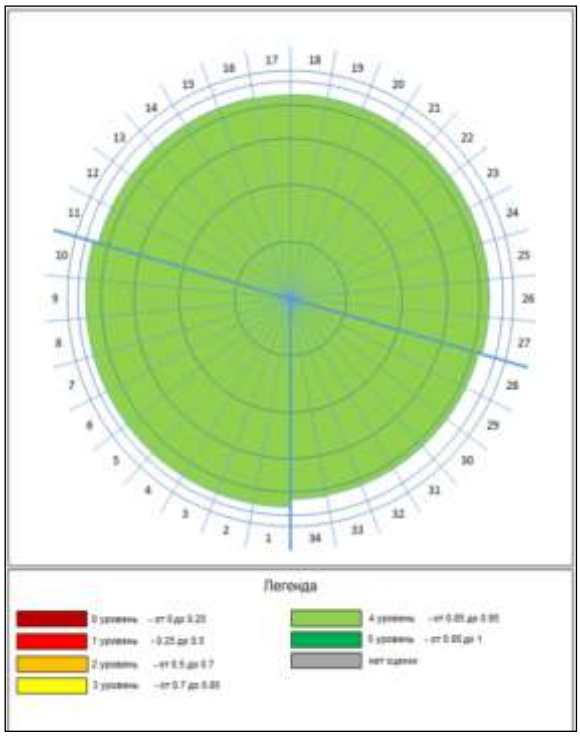


Рисунок 3.10 – Круговая диаграмма, отображающая целевые оценки EV_1, EV_2, EV_3

Одновременно обеспечивается минимизации затрат на реализацию различных мер (средств) обеспечения ИБ Kj и минимизация времени, затрачиваемого на выполнение операций **T*f*.** Эта задача может быть описана как система уравнений (3.7 – 3.9):

$$\begin{cases} \sum_{i=1}^{34} M_i \to \max & (3.7) \\ \sum_{j=1}^{n} K_j \xrightarrow{R\max} \min & (3.8) \\ \sum_{f=1}^{m} T_f \xrightarrow{R\max} \min & (3.9) \end{cases}$$

Решение проблемы формирования минимального набора критериев (метрик) ИБ, обеспечивающих оптимальное решение системы уравнений (3.7 – 3.9), может быть предложено на основании максиминных критериев (иначе называемых критериями Сэвиджа) вида:

$$\mathbf{X^{*} = arg\ max_i\ min_j\ \{\ q_{ij}\ \}}$$

подробно рассматриваемых в работе Ф. Перегудова и Ф. Тарасенко [151].

В развитие данного подхода следует принять во внимание следующие критерии, практическое применение которых может существенно улучшить процесс выполнения аудита ИБ (изложено в работах [137], [98], [99]):

1. Время, выделяемое на реализацию программы аудита ИБ.
2. Состав мер (средств) обеспечения ИБ, планируемых к внедрению.
3. Требования к перечню, порядку и частоте выполнения аудита.

Часть указанных выше критериев будут подробно рассмотрены далее. В более сложных случаях, при наличии достаточных вычислительных ресурсов, может быть рекомендовано формирование n-мерных «профилей эффективных действий» и построение аддитивных функций полезности (ценности) вида:

$$u(x_1, x_2, ...x_n) = \sum_j^m \lambda_j u_j(x_j)$$

где:

— набор критериев $x_1,\ldots x_n$ образует «профиль эффективных действий», а весовой коэффициент λ удовлетворяет требованиям:

$$\sum_j^m \lambda_j = 1$$

$$0 < \lambda < 1$$

предложенных и подробно рассмотренных в работе Р. Кини и Х. Райфа [64].

В работе М. Месаровича, Д. Мако и И. Такахара [127] отмечается, что функции полезности применяются не только для анализа произведенной продукции (оказанных услуг), но и для оценки обеспеченности «*внутренним продуктом*». Очевидно, что современные методы (в том числе, и современные риск-ориентированные стандарты) позволяют оценивать численно соотношение «внутреннего продукта» и произведенной продукции. В частном случае данный подход позволяет оценить затраты на обеспечение ИБ для гарантированного выпуска продукции (оказания услуг надлежащего качества), с учётом известных внутренних и внешних негативных факторов.

3.5 Анализ существующих методов к оценке бюджета ИБ

3.5.1 Общие положения оценки бюджета ИБ

Отметим одну из практических задач измерения результативности СМИБ (ИСМ) – обоснование выделяемого бюджета на обеспечение ИБ. По объективным оценкам (ISO, Reuters, Osterman Research, PwC – [394], [377], [395], [293], [309]), бюджет ИБ составляет до 10 % от бюджета на ИТ. В РФ эксперты в целом подтверждают оценки бюджета, выделяемого на ИБ. Например, для концерна «Ростеха» известна оценка 800 млн. руб. в год, что составляет от 7 до 10 % бюджета на ИТ, РЖД в среднем тратит около 20 млрд. в год на ИТ и около 10% бюджета (2 млрд. руб.) выделяется на ИБ и примерно столько тратит ЦБ – по оценкам эксперта Zecurtion В.Ульянова[178]. На конференции «Рускрипто-2016»[179] в докладе А.П. Баранова «Проблемы ИБ, вытекающие из тенденций технического развития. Доступность» отмечено, что объективно существует проблема признания цены ущерба.

В «Руководстве» ОБСЕ отмечается, что отсутствие мер по защите важнейших объектов инфраструктуры может иметь серьезные последствия, в частности, нарушения в их работе могут привести к ущербу государственной безопасности или другим серьезным последствиям ([182]). Отсюда следует необходимость формирования подходов к управлению бюджетом ИБ, поскольку возможны «международные последствия» аварий, как это было в 2003 г. в Нью-Йорке (США), а последствия затронули более 55 млн. человек в США и Канаде. Следует принять во внимание, что аспекты управления бюджетом ИБ, как экономической функцией, отражены не только в государственных законодательных актах, отраслевых нормативах, но и в современных концепциях, например – ISO 27032 ([182], стр. 38).

В отчете [377] приводятся оценки бюджета на обеспечение ИБ в диапазоне от 3,6% до 3,8% от бюджета ИТ в течение периода измерений 2010 – 2014 гг. Максимальное значение бюджета ИБ составляет 6,9% в промышленной отрасли

---

178 http://www.rbc.ru/politics/17/08/2017/599180249a7947963e65f566?from=main

179 http://www.ruscrypto.ru/accotiation/archive/rc2016/

(*Industrial product*). В то же время отметим, что оценки не коррелируют с оценкой динамики роста количества инцидентов. Например, среднее количество детектированных инцидентов ИБ в отрасли энергетики возросло с 1.179 (2013 г.) до 7.391 (2014 г.), т.е. на 526 % [377]. ЛПР логично полагают уместным не тратить значительные средства на реализацию технических систем обеспечения ИБ, когда можно реализовать только организационные меры. По данным [394], в организациях реализованы следующие процедуры ИБ (см. таблицу 3.5):

Таблица 3.5 – Перечень процедур СМИБ

№ п.п.	Применяемая процедура	Доля, %
1.	Корпоративная политика управления инцидентами	63%
2.	Назначение менеджера по инцидентам ИБ и формирование команды реагирования на инциденты ИБ	54%
3.	Ведение протокола для идентифицированных активов, в отношении которых были выявлены нарушения ИБ	46%
4.	Ведение протокола информирования о нарушениях ИБ деловых партнеров, клиентов и иных заинтересованных сторон	45%
5.	Идентификация заинтересованных сторон, которые могут помочь в процессе расследования инцидентов ИБ	38%

Таким образом, в наилучшем варианте представители службы ИБ располагают достоверными оценками существующего (планируемого) комплекса мер (средств) обеспечения ИБ, исходя из выполненной оценки рисков (как это требуется [317] и [319]). В наихудшей ситуации вниманию ЛПР представляются оценки прошлого года с прогнозом (примерным трендом) развития противоборствующих техник.

Обратим внимание, что на конференции «Рускрипто-2016»[180] был представлен отчет Е. Старостиной «Инвестиции, тренды и технологии: основные данные глобального исследования в области ИБ для России», согласно которому бюджет на цели обеспечения ИБ в России останется на том же уровне – 53%. В отчете Gartner[181] отмечается, что рост затрат на обеспечение ИБ в мире составляет примерно 7% в год. В отчете [394] представлены следующие оценки (см. таблицу 3.6):

---

180 http://www.ruscrypto.ru/accotiation/archive/rc2016/

181 http://www.gartner.com/newsroom/id/3784965

Таблица 3.6 – Оценки бюджета

№ п.п.	Оценки бюджета ИБ со стороны ЛПР	Динамика, %
1.	Бюджет на 2015 будет значительно больше, чем бюджет 2014	13 %
2.	Бюджет на 2015 будет немного больше, чем бюджет 2014	38 %
3.	Бюджет на 2015 будет таким же, как бюджет 2014	48 %
4.	Бюджет на 2015 будет немного меньше, чем бюджет 2014	1 %
5.	Бюджет на 2015 будет значительно меньше, чем бюджет 2014	0 %
	Всего	**100 %**

3.5.2 Метод выполнения измерений результативности ИБ

С учетом изложенного выше, метод выполнения измерений ИБ должен основываться на атрибутах выбранных объектов измерений (п. 5.4.2. стандарта [318]). Дополнительным параметром для оценки результативности является ограничение бюджета СМИБ. Примерами объектов измерений могут служить:

— результативность мер и средств контроля и управления в СМИБ;

— степень удовлетворенности уровнем ИБ заинтересованных сторон.

Отметим, что термин «*мера и средство контроля и управления*» точно соответствует ГОСТ Р ИСО/МЭК 27000-2012 (п. 2.10), как перевод английского термина «*control*» ([315]). Метод измерений может использовать объекты измерений и атрибуты из разнообразных источников, например: сообщения об инцидентах ИБ. Для примера выберем ряд мер и средств контроля и управления ИБ в соответствии с требованиями стандарта ISO 27001 [317]. Выбор именно этого множества обоснован, во-первых, замкнутым «мини-циклом» PDCA для контроля активов, во-вторых, применением практически в любой СМИБ с малой вероятностью исключения из «Заявления о применимости» (*Statement of Applicability* [317]) и, в-третьих, достаточностью для объективного рассмотрения системы метрик ИБ и измерения результативности СМИБ. Результаты представлены в таблице 3.7:

Таблица 3.7 – Меры и средства контроля и управления ИБ

№ п.п.	Мера и средство контроля и управления ИБ	Пункт стандарта	Объект
1.	Договорные соглашения с работниками и должны определять их ответственность ИБ	А.7.1.2	Персонал
2.	Должны быть определены владельцы всех активов, включенных в реестр активов	А.8.1.2	Активы
3.	Должно быть принято решение о классификации события ИБ как инцидент ИБ	А.16.1.4	Инциденты ИБ
4.	Организация должна проводить внутренний аудит через запланированные промежутки	9.2	Внутренний Аудит
5.	При появлении несоответствия организация должна определить причину и реализовать любые необходимые корректирующие действия	10.1	Корректирующие действия

На основании сформированных в соответствии с дополненной теорией «*элитных групп*» [55] средств контроля и управления ИБ, предложим метрики для измерения результативности СМИБ (здесь и далее – на установленный интервал проведения аудита), результаты представлены в таблице 3.8.

Таблица 3.8 – Метрики ИБ

№ п.п.	Метрика ИБ	Индекс	Пункт стандарта
1.	Кол-во инцидентов ИБ	$И_1$	А.16.1.4
2.	Кол-во повторных инцидентов ИБ	$И_2$	А.16.1.4
3.	Кол-во выполненных аудитов СМИБ	$А_1$	9.2
4.	Кол-во запланированных корр. действий	К	10.1
5.	План выполнения внутренних аудитов	$П_1$	9.2
6.	План выполнения корр. действий	$П_2$	10.1

Далее на примере обязательной процедуры «Корпоративная политика управления инцидентами» (наибольшая доля, см. таблицу 3.5) с учетом допущений о неизменности бюджета СМИБ (наибольшая оценка, см. таблицу 3.6), с учетом предложенных мер и средств контроля и управления ИБ (см. таблицу 3.7) и сформированных метрик ИБ (см. таблицу 3.8) предложим **новый** метод выполнения измерений результативности СМИБ. Описание шагов представленного метода отражено в таблице 3.9.

Таблица 3.9 – Метод измерения результативности СМИБ

№ п.п.	Шаг метода измерения	Результат действия
1.	Определение назначения и области применения метода	Формирование области применения
2.	Определение измеряемой процедуры в СМИБ	Выбор процедуры (заполнение таблицы 3.6) Бюджетные ограничения (заполнение таблицы 3.7)
3.	Определение объектов измерений	Выбор объектов измерения (заполнение таблицы 3.8)
4.	Определение атрибутов объектов измерений	Формирование $И_{ij}$, где i – номер объекта, j – номер атрибута; например $И_{11}$ – атрибут кол-ва инцидентов ИБ $И_{21}$ – атрибут кол-ва повторных инцидентов ИБ
5.	Определение метода измерения и структуры измерительной системы	Подсчитать кол-во (инцидентов) $И_{21}$ по отношению к $И_{11}$; Подсчитать кол-во (аудитов) $А_{11}$ по отношению к плану $П_1$;
6.	Определение основной меры измерений	Норма аудитов $А_{11}$ / $П_1$, завершенная на установленную дату
7.	Определение функции измерения	Количество $А_{11}$ и $К_{11}$ на установленную дату
8.	Определение производной меры измерения	Статус выполнения $А_{11}$ и $К_{11}$ на установленную дату
9.	Формирование аналитической модели	Делить $И_{21}$ на ход выполнения $А_{11}$ и $К_{11}$ на установленную дату;
10.	Определение метрик (показателей) ИБ	Тренд по своевременности аудитов $А_{11}$ и достаточности корректирующих действий $К_{11}$ для повторных инцидентов $И_{21}$
11.	Определение критериев принятия решения	Более 0,9 – тренд нормальный; равно и менее 0,9 – необходимо срочное изменение в плане аудита $П_1$ и корректирующих действий $П_2$
12.	Определение результатов измерений	Тренд понижения говорит о недостаточном контроле, а тренд неубывающий говорит о достаточном контроле процедуры контроля инцидентов ИБ.

Решение поставленной задачи – оценка результативности СМИБ (ИСМ), может быть продемонстрировано как оптимизация количества применяемых метрик ИБ, увеличение скорости выполнения оценки и «выдачи» оптимальных управляющих воздействий ЛПР, оптимизация бюджета для обеспечения

заданной результативности СМИБ (ИСМ). Заметим, что предложенное решение поставленной задачи позволяет дополнительно исправлять ошибки методом локализации обратным процессом, как показано в работе Н. Винера ([13], стр. 222). Локализация ошибки начинается с точки, где она замечена, но крайне важно обеспечить, чтобы проверка и отработка выявленной ошибки шла с такой же скоростью, как и сам процесс; иначе «эффективная скорость» процесса измерения (в составе СМИБ или ИСМ) снижается из-за более медленного процесса аудита ИБ.

3.5.3 Оценка результативности системы управления ИБ

Стандарт ISO требует от организации определять, «*каким образом проводить измерение результативности выбранных мер и средств контроля и управления ИБ и их групп*» [317]. Также рекомендуется, чтобы не выделялись чрезмерные ресурсы в ущерб основной деятельности, и текущая деятельность, связанная с постоянными измерениями, была бы интегрирована в плановую деятельность организации с привлечением минимальных дополнительных ресурсов (п. 8.2 стандарта [318]). Очевидно, что экономия ресурсов на обеспечение измерений ИСМ (СМИБ) должна приводить к выполнению целей измерений, связанных с ИБ, и получению оценки результативности реализованной СМИБ (п. 5.1. b) стандарта [317]). Меры и средства контроля и управления ИБ, выбранные на основании дополненной теории «элитных групп» в рамках программы измерений, на практике следует непосредственно связывать с функционированием «конкретной реализации» ИСМ, а также процессами основной деятельности организации. В формуле (3.10) предложено формировать общую оценку результативности СМИБ (отдельно или в составе ИСМ) как последовательное суммирование всех частных оценок результативности внедренных мер и средств контроля и управления ИБ, получаемых в результате выполнения аудита всех типов. **Новизна** представленной формулы оценки результативности СМИБ с учетом бюджетных затрат выражается в двойном суммировании: сначала выполняется оценка по всем мерам (средствам) контроля и управления ИБ в рамках одного типа аудита, затем – формирование итоговой

оценки по всем типам аудита. Соответственно, оценка результативности СМИБ (как безразмерная величина $0 \leq К_{СМИБ} \geq 1$) может быть измерена по формуле следующего вида:

$$К_{СМИБ} = \frac{\frac{И\ тек.}{И\ баз.} \cdot \sum_{i=1}^{m} \sum_{k=1}^{3} M_{\ ИБ\ ik} \cdot \alpha_{ik}}{\sum_{j=1}^{n} A\ j \cdot V_j} \qquad (3.10)$$

где:

$И_{тек}$ – *кол-во выявленных инцидентов ИБ за текущий период;*

$И_{баз}$ – *кол-во инцидентов ИБ за предыдущий период;*

$i\ (1, m)$ – *перечень мер (средств) контроля и управления ИБ;*

$k\ (1, 3)$ – *виды аудита (первой, второй и третьей стороной);*

$M_{\ ИБ\ ik}$ – *стоимость i-меры и средств контроля и управления ИБ;*

α_{ik} – *оценка результативности i-меры (средства) контроля и управления ИБ по итогам k-аудита;*

$j\ (1, n)$ – *перечень защищаемых активов;*

A_j – *стоимость защищаемого актива;*

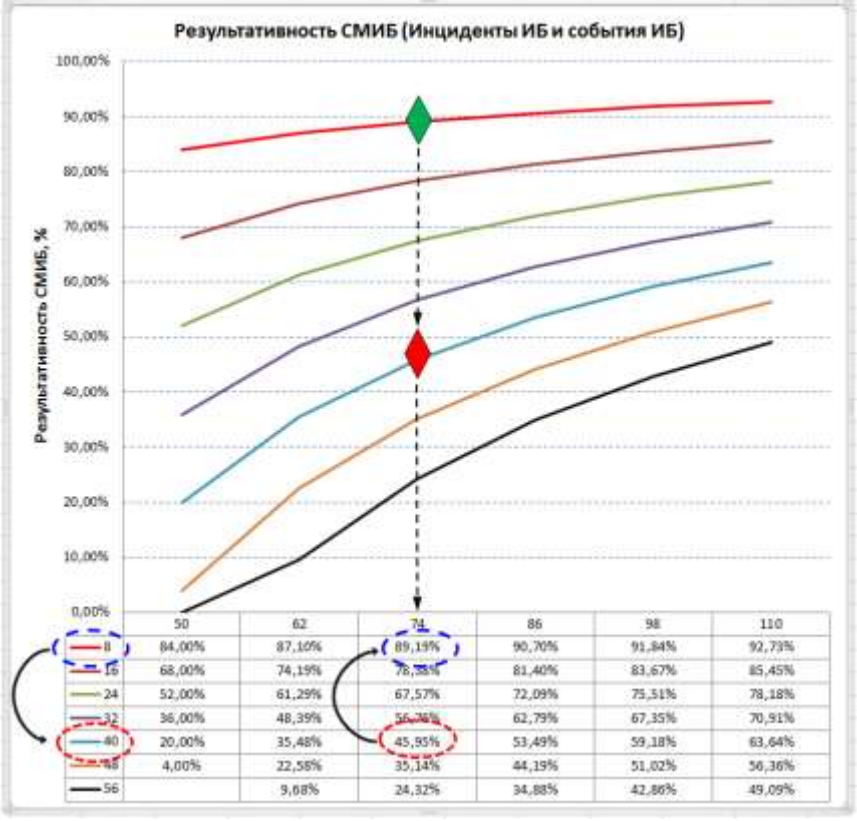
V_j – *оценка значимости для бизнеса защищаемого актива.*

3.5.4 Практический кейс

Метрика оценки результативности по формуле (3.10) α_{ik} также является безразмерной величиной, имеющей значение в диапазоне $0 \leq \alpha_{ik} \geq 1$. Формула (3.10) позволяет оценить результативность СМИБ в текущей конфигурации *scope* ИСМ и сопоставлять (в графическом виде) отношения по состоянию до внедрения СМИБ и в любой последующий год. Рассмотрим практический кейс для демонстрации работы **нового** предложенного метода на основании оценки последствий инцидентов ИБ по формуле (3.10). Следующие расчеты выполнены для 4-х значений соотношения $И_{тек}$ / $И_{баз}$ (от 0,5 до 0,99) и для 5 значений результативности технических систем и средств обеспечения ИБ (от 0,5 до 0,99). Результаты представлены на рисунке 3.11.

Показано, как при реализации программы измерений в соответствии с [20], [21], [317], [318] возможно оперативное снижение количества инцидентов ИБ (например, с 40 до 8), что обеспечивается внедрением более результативных мер

(средств) контроля ИБ, и что позволяет, в конечном итоге, значительно увеличить результативность СМИБ с исходных 46% до существенных 90%.



	50	62	74	86	98	110
8	84,00%	87,10%	89,19%	90,70%	91,84%	92,73%
16	68,00%	74,19%	78,38%	81,40%	83,67%	85,45%
24	52,00%	61,29%	67,57%	72,09%	75,51%	78,18%
32	36,00%	48,39%	56,76%	62,79%	67,35%	70,91%
40	20,00%	35,48%	45,95%	53,49%	59,18%	63,64%
48	4,00%	22,58%	35,14%	44,19%	51,02%	56,36%
56		9,68%	24,32%	34,88%	42,86%	49,09%

Рисунок 3.11 – Расчет результативности СМИБ по формуле (3.10)

Предложенный **новый** метод выполнения измерений результативности СМИБ (ИСМ) позволяет реализовать в режиме, близком к РРВ, поставленную задачу в пределах одного «замкнутого» цикла PDCA, длительность которого определяется решением ЛПР, доступными ресурсами и перечнем применяемых мер (средств) контроля и управления ИБ.

3.6 Методы оценки уровня обеспечения ИБ СлПО на примере ТЭК

3.6.1 Постановка задачи

В настоящее время к проблеме обеспечения безопасности объектов ТЭК приковано внимание различных специалистов, в том числе, в области обеспечения ИБ [149], [148], [174], [209]. На законодательном уровне разработаны Федеральные законы [246], принят ряд постановлений Правительства [157] – [161], утвержден приказ ФСТЭК № 31 [167], [62]. Установлены важные определения [246]:

— *акт незаконного вмешательства* (Ст. 2.1 [246]);

— *критически важные объекты ТЭК* (Ст. 2.5 [246]);

Также важно принять во внимание, что в [246] введено понятие «*Паспорт безопасности объекта ТЭК*». Для выполнения требований национальных нормативных документов и стандартов ISO предлагается применять введенный ранее новый термин СлПО. Практическая задача касается формирования системы численных показателей для оценки уровня обеспечения ИБ СлПО в ТЭК, на базе реализация СМИБ – как отдельно, так и в составе ИСМ для обеспечения безопасности объектов ТЭК.

3.6.2 Приоритет защиты активов СлПО в ТЭК

В «Руководстве» отмечается приоритет защиты объектов ТЭК[182] (по отраслям «электричество», «природный газ» и «нефть») для обеспечения ИБ всей критичной инфраструктуры современного общества [182]. Более того, законодательно установлены лимиты для обеспечения функционирования критичной инфраструктуры в случае глобальных сбоев. Каждое государство — член ЕС должно обладать запасами нефти, достаточными для удовлетворения внутреннего спроса в течение не менее 90 дней[183]. Текущего стратегического нефтяного запаса США, который составляет около 694 млн. баррелей нефти, хватит на 36 дней[184]. Таким образом, для компенсации различий в уровне мер ИБ, принимаемых в важнейших отраслях, крайне важны межотраслевые соглашения по предотвращению кризисных ситуаций.

Применительно к отрасли энергетики отметим, что в последние годы энергетическая цепь поставок стала более автоматизированной и, как следствие, более зависимой от компьютерных СУ. Это обеспечивает более эффективное и надежное функционирование современной энергетической инфраструктуры, но в то же время повышает риски, поскольку современные сети управляются удаленно[185]. Несмотря на то, что использование открытых стандартов ПО позволяет снизить затраты на эксплуатацию сетей, оно также делает

---

182 https://www.dhs.gov/national-infrastructure-protection-plan

183 http://www.iea.org/publications/feeepublications/publication/EPPD_Bochure_English_2012_02.pdf

184 http://www.spr.doe.gov/dir/dir.html

185 http://www.ensec.org/index.php?option=com_content&view=article&id=205:critical-energy-infrastructureprotection-the-case-of-the-trans-asean-energy-network&catid=98:issuecontent0809&Itemid=349

энергетическую сеть более уязвимой для кибератак, поскольку злоумышленники получают доступ к известному исходному коду, значит, могут использовать его в собственных целях.

3.6.3 Формирование перечня защищаемых активов СлПО ТЭК

В любой СМ (ИСМ) первым и одним из важнейших вопросов является вопрос правильного выявления перечня активов (*asset*, в нотации [317]), которые требуют защиты от актов незаконного вмешательства. Для ТЭК проблему выявления и защиты КВО (в терминологии [246]) возможно сопоставить с общей проблемой выявления и защиты ценных для бизнеса активов СлПО в СМИБ (ИСМ). Предлагаемый подход к выявлению и оценке активов для СМИБ представлен следующим образом (см. рисунок 3.12).

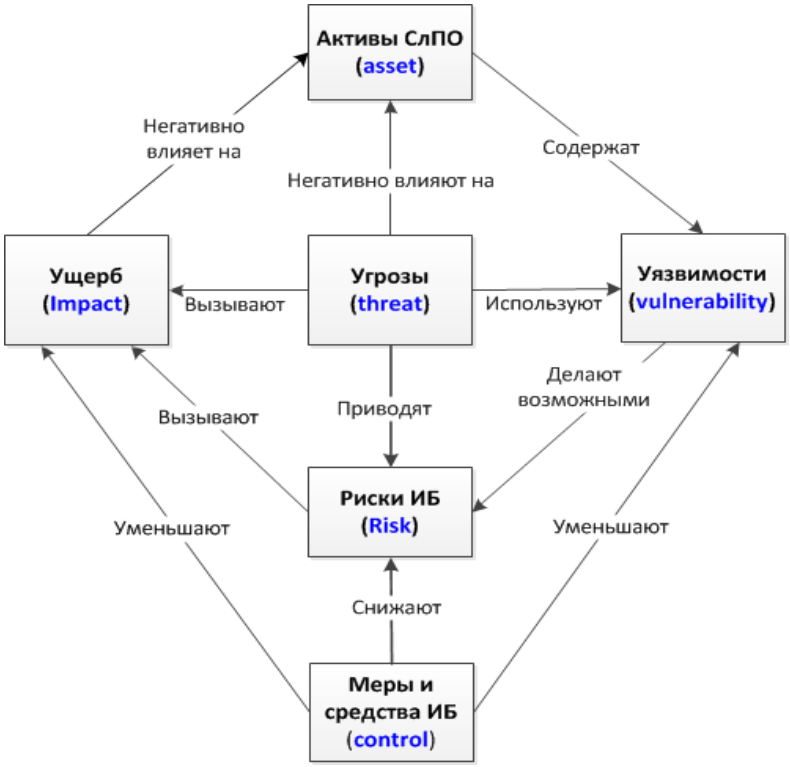


Рисунок 3.12 – Взаимодействие понятий СМИБ

Предполагается, что перечень активов, подлежащих защите, находится в определенном балансе по отношению к стоимости мер (средств) ИБ, обеспечивая принцип экономической эффективности ИСМ (СМИБ), как показано выше. Для формирования перечня угроз рекомендуется использовать совместно Приложение «В» стандарта ISO [317] и Приказ ФСТЭК России [167]. Критерии, используемые в качестве основы для присвоения ценности каждому активу в

организации ТЭК, должны быть четко определены. В качестве возможных критериев, используемых для определения ценности актива, могут быть выбраны: исходная (балансовая) стоимость, стоимость замены (воссоздания) актива в случае реализации неблагоприятного сценария (события риска ИБ) или дополнительную ценность (например, ценность репутации) [96].

3.6.4 Формирование перечня угроз активов СлПО ТЭК

В постановлении Правительства № 861 (ст. 2) [161] отмечено, что «*субъект топливно-энергетического комплекса обязан представлять информацию об угрозе совершения и о совершении акта незаконного вмешательства на объекте топливно-энергетического комплекса…*». Подразумевается, что такой перечень угроз сформирован на основании Приложения 1 к Постановлению Правительства [161], утвержден в установленном порядке на каждом СлПО ТЭК. Сопоставим указанный выше перечень с перечнем типовых угроз, согласно Приложения «С» стандарта [319], специально адаптированного для СлПО ТЭК. В таблице 3.10 представлены 3 категории данных: перечень угроз согласно постановлению Правительства [161], выборка из перечня типовых угроз стандарта [319] и оценка последствий для указанных угроз в соответствии с [319] и [321].

Таблица 3.10 – Перечень угроз СлПО ТЭК (фрагмент)

№ п.п.	Угроза (постановление Правительства № 861)	Угроза (Приложение «С» стандарта 27005)	Последствия
1.	Угроза захвата	н/д	Вторжение
2.	Угроза взрыва	н/д	Взрыв (терроризм)
3.	Угроза поражения опасными веществами	—Загрязнение	Вмешательство в систему
4.	Угроза хищения	—Кража оборудования —Уничтожение оборудования или носителей	Хищение
5.	Угроза технического воздействия	—Авария системы кондиционирования воздуха —Нарушение энергоснабжения —Отказ оборудования —Кража носителей или документов	Системная атака (отказ в обслуживании)

Дополнительно важно отметить, что в постановлении [161] уделено внимание очень важной технической задаче, реализация которой, как правило, отражена только в стандартах ISO (соответственно, п. 7.5.3 [317] и п. 4.6.5 [321]) – задаче управления записями в СлПО ТЭК. В частности, отражены требования для обеспечения защиты важных записей при предоставлении информации об угрозе, в зависимости от способа (средств): телефонной связи, радиосвязи, электронной или факсимильной связи (п.п. 9 и 10). Отметим, что в Постановлении [161] установлен месячный срок хранения носителей информации об угрозе, подтверждающих факт ее передачи (п. 13).

3.6.5 Формирование перечня уязвимостей активов СлПО ТЭК

В соответствии с приказом ФСТЭК России [167] УБИ определяются на каждом из уровней АСУ по результатам анализа возможных уязвимостей АСУ (п. 13.3). В дополнение к приказу ФСТЭК России [167] представляется полезным проанализировать определенный ранее перечень типовых угроз и на этой базе рассмотреть дополнительно перечень уязвимостей согласно Приложению «D» стандарта [319] (см. таблицу 3.11).

Отметим важное практическое требование, содержащееся в ФЗ [246]: в ст. 10 установлены требования к персоналу, обеспечивающему безопасность объектов ТЭК, и конкретно – запрет приема определенных категорий лиц на работу, непосредственно связанную с обеспечением безопасности объектов ТЭК. Например, известен факт отказа регистрации ОС «ОСь» (разработка компании НЦИ в составе «Ростеха») в реестре отечественного ПО[186]. Эксперт BaseALT А.Смирнов отметил, что «ОСь» спрограммирована на базе двух ОС с открытым кодом — CentrOS и Fedora, которые полностью принадлежат компании RedHat (США). Согласно анализу BaseALT, большая часть исходных составных частей (пакетов) — заимствованы и без изменений добавлены из CentrOS. Собственных пакетов, утверждает А. Смирнов, всего 19 из 1257, т.е. примерно 1,5%. Ранее аналогичные опасения в части создания «ГосСОПКА»

[186] http://www.rbc.ru/technology_and_media/28/07/2017/597ac7cc9a79477575518208?from=newsfeed

высказывали эксперты «Независимого военного обозрения» (в частности – И.Пискунов)[187].

Таблица 3.11 – Уязвимости и методы оценки уязвимостей (фрагмент)

№ п.п.	Тип	Уязвимость	Угроза
1.	Аппаратные средства	Чувствительность к колебаниям напряжения	Потеря электропитания
2.		Незащищенное, небрежное хранение	Хищение носителей данных или документов
3.	Программные средства	Отсутствующее или недостаточное тестирование программных средств	Злоупотребление правами
4.		Отсутствие «следов» аудита	Злоупотребление правами
5.	Сеть	Плохой менеджмент паролей	Фальсификация прав
6.		Отсутствие эффективного контроля изменений	Сбой программных средств
7.	Персонал	Отсутствие персонала	Нарушение работоспособности персонала
8.		Неадекватные процедуры набора персонала	Разрушение оборудования или носителей данных
9.	Объект	Безнадзорная работа внешнего персонала или персонала организации, занимающегося уборкой	Хищение носителей данных или документов
10.		Отсутствие процедур идентификации и оценки риска	Злоупотребление правами

Указанные требования по тестированию компонент ИС находят свое практическое применение в Постановлении Правительства (п.п. 9, 16, 17 [158]) и, в том числе, в Указе Президента Российской Федерации от 22.12.2017 № 620[188]. Определена задача СОПКИ по контролю степени защищенности информационных ресурсов РФ[189]. Отметим важную особенность оценки уязвимостей – этот процесс не должен принимать как достоверные входные

187 http://www.ng.ru/ideas/2016-12-23/5_6893_kiber.html
188 http://publication.pravo.gov.ru/Document/View/0001201712220008?index=1&rangeSize=1
189 https://www.securitylab.ru/news/490498.php

данные ни известные протоколы, ни их «фирменные» реализации без объективной экспертизы. Все критические элементы объекта ТЭК должны быть оценены в независимой системе оценивания (экспертизы), например, имеющей и аккредитацию ФСТЭК по ИСО/МЭК 15408 «Общие критерии» и международную, например, имеющую аккредитацию по FIPS 140.

Рассмотрим пример, который поясняет представленный выше тезис: в протоколе Kerberos[190], используемом в Windows, Linux и macOS, найдена уязвимость, возраст которой составляет 21 год. Протокол Kerberos разрабатывался в Массачусетском технологическом институте, первая его версия появилась в 1983 г.

Дополнительно отметим, что в ст. 9 [161] определено, что паспорт, признанный по результатам актуализации подлежащим замене и утратившим силу, хранится в порядке, установленном субъектом ТЭК, в течение 25 лет. Это требование соответствует требованиям стандартов, соответственно (п. 9.3 [317] и п. 4.7 [321]) по анализу со стороны руководства (*Management Review*). В то же время в постановлениях Правительства [157] – [161] не отражены в явном виде требования к обеспечению полного цикла управления рисками для организаций ТЭК. Также не предусмотрена оценка остаточного риска (*Residual Risk*), которая позволяет оценить уровень обеспечения ИБ активов СлПО ТЭК в полном цикле PDCA после применения выбранных мер (средств) обеспечения ИБ и определенного перечня рисков. Это обстоятельство может быть компенсировано применением стандартов ISO (ГОСТ Р) серии 27001 и внедрением «целевого стандарта» ISO серии 31000, который также принят в Российской Федерации как ГОСТ Р ИСО 31000 [33].

3.6.6 Формирование требований по проверкам (аудиту) СлПО ТЭК

Требования по выполнению проверок (аудита) активов СлПО ТЭК установлены в стандартах, соответственно, [317] (п. 9.2) и [321] (п. 4.6.3). Установлены общие для всех стандартов ISO (ГОСТ Р) требования к периодичности, объективности и беспристрастности [20], [21]. Практические

---

190 http://safe.cnews.ru/news/top/2017-07-14_v_windowslinux_i_macos_najdena_obshchaya_dyra_vozrastom

требования по проверкам (аудиту) АСУ ТП на объектах ТЭК установлены Приказом ФСТЭК [246] и наиболее важные проверки рассмотрены в качестве примера (см. таблицу 3.12). Дополнительно отметим, что в Приказе ФСТЭК [246] многократно отмечается важная роль стандартов серии 27001, в частности, даны прямые ссылки (п.п. 13.4 и 15.2) на ГОСТ Р ИСО 27001 [32], который является аутентичным переводом стандарта ISO 27001 [317]. Отметим, что роль аудита практически не определена в практике обеспечения безопасности компонентов АСУ ТП даже с учетом негативной статистики. Например, в отчете РТ за 2017г. отмечается, что в 2016 г. в РФ был обнаружен 591 компонент АСУ ТП, доступный из сети интернет, а в 2017 г. — уже 892, что позволяет говорить о растущей угрозе увеличения доступных из интернета компонентов АСУ ТП, расположенных в РФ[191].

Таблица 3.12 – Перечень проверок АСУ СлПО ТЭК (фрагмент)

№ п.п.	Требования проверки	Приказ ФСТЭК № 31	ISO 27001
1.	При проектировании системы защиты АСУ осуществляется проверка, в т.ч. при необходимости с использованием макетов или тестовой зоны	14.1.	A.12.1, A.12.4, A.12.6
2.	При внедрении организационных мер защиты информации осуществляется проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий персонала АСУ	15.3.	A.7.2, A.9.2, A.14.2
3.	Предварительные испытания системы защиты АСУ проводятся с учетом ГОСТ 34.603 и включают проверку работоспособности системы защиты АСУ	15.5.	A.14.2, A.14.3
4.	Меры по управлению обновлениями ПО должны обеспечивать безопасное получение, проверку и установку обновлений ПО на компонентах АСУ ТП	18.15	A.12.1, A.12.7, A.14.2
5.	Меры по информированию и обучению персонала должны обеспечивать информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты АСУ, а также теоретическое и практическое обучение (в том числе проведение тренировок) по эксплуатации системы защиты АСУ.	18.18	A.7.2, A.17.1

191 https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-2017-rus.pdf

Рост количества известных уязвимостей, а также доступных в интернете компонентов АСУ ТП дает злоумышленникам все больше возможностей для проведения атак, что отмечается в обзоре[192]. Кроме того, рекомендуется на этапе проектирования АСУ ТП предусматривать механизмы безопасности, предназначенные для защиты компонентов АСУ ТП (это отражено в ряде стандартов IEC серии 61501 и 61511), но не всегда выполняется[193].

3.7 Методы учета социальных факторов при выполнении аудита

3.7.1 Постановка задачи

Проблема учета социальных факторов при выполнении программы аудита известна и нашла отражение в ряде стандартов ISO [20], [21]. В то же время новые процессы, развивающиеся в обществе, требуют дополнительного внимания к проявлению «человеческого фактора», тем более, когда это касается функционирования СлПО и выполнения аудита ИБ [264], [273], [10], [232], [233]. В работе [1] представлена функция вида:

$$R_i = f\,(N_i, Z_i, a, b, P_i, C_i, \ldots)$$

с помощью которой предлагается оценивать масштаб распространения слуха с учетом ряда факторов. В работе [4] отмечается, что СрЗИ не гарантируют 100% защиты по причине того, что «самым слабым звеном в цепочке обеспечения ИБ» является сотрудник. Предлагается оценивать и осознанные и неосознанные действия пользователя, что в целом соответствует принятым общим подходам ФСТЭК. Это предложение подчеркивается тем фактом, что минимально хотя бы 1 раз сообщали свои идентификационные данные 84,5% респондентов. Так же отмечается важность и актуальность проблемы перехода от профиля психологических особенностей пользователя к профилю уязвимостей. Отметим, что данный подход встречается и в документах ФСТЭК [167], и в стандартах СТО БР ИББС [217] и ISO [317]. Однако, в ряде новых стандартов рекомендуется переходить к анализу актуальных УБИ, не заостряя внимание на бесчисленном множестве уязвимостей (см. ГОСТ Р ИСО/МЭК

192 https://info.publicintelligence.net/FBI-AntisecICS.pdf
193 https://ics-cert.us-cert.gov/advisories/ICSA-12-228-01A

15408 [23]). В работе [234] предложено определение «*социоинженерной атаки*». Это определение, в целом, согласуется с существующими нормативными документами, однако, не включает иные объекты защиты, в частности – компоненты СлПО (АСУ ТП и пр.). В работе [3] представлены 5 типов уязвимостей пользователя, которые, в общем случае, хорошо согласуются с приложениями стандартов ISO серии 27001 [317] и серии 27005 [319], в частности, слабые пароли, техническая халатность (безграмотность), что может быть использовано в различных универсальных (типовых) моделях оценки уровня обеспечения ИБ СлПО.

3.7.2 Предпосылки для контроля угроз социальной инженерии

Как было показано выше, проблема учета «человеческого фактора» и его проявления в СлПО является и актуальной, и достаточно сложной для технического решения с помощью современных СрЗИ и/или СКЗИ. Прежде всего, представляется сложным определить функциональный набор метрик ИБ, которые возможно применить для противодействия «социоинженерных атак». Однако, есть несколько примеров применения метрик ИБ именно для контроля угроз социальной инженерии. Например, в публикации ESET[194] в 2017 г. показано, что около 84% компаний недооценивают риски, связанные с человеческим фактором и более 69% респондентов в России никогда не проходили обучение основам кибербезопасности в своих компаниях. В то же время более 60% участников аналогичного опроса в США сообщили, что их работодатели организовали обучение по кибербезопасности. Также хорошим примером «отраслевой культуры безопасности» является оценка размера ущерба и оценка количества атак. В частности, зампред правления Сбербанка С. Кузнецов[195] пояснил, что для Сбербанка потенциальный ущерб от подобных кибератак составляет порядка 700 млн. руб., и каждую неделю фиксируется порядка 5 тыс. атак с использованием социальной инженерии. Если смотреть на

[194] https://www.esetnod32.ru/company/press/center/eset-84-kompaniy-nedootsenivayut-riski-svyazannye-s-chelovecheskim-faktorom-/
[195] http://www.securitylab.ru/news/486533.php

проблему шире, то можно определить ряд конфликтов, которые на практике выявляются как существенные противоречия, например:

— Направление «личное и корпоративное» (например, BYOD);
— Направление «доступность и удобство» (например, одноразовые пароли);
— Направление «скорость и защита» (например, антивирусы и DLP).

В то же время, как показывает практика аудита, могут быть предложены метрики ИБ, формализуемые в рамках технических средств (СрЗИ), например:

— Определение соотношения количества аккаунтов личных е-майл / число работников, что может характеризовать «мягкость» установленного режима ИБ при работе с почтовыми сервисами;
— Определение частоты сообщений личных е-майл / число работников, что может характеризовать возможность в рабочее время пользоваться публичными почтовыми сервисами;
— Определение объема вложений в сообщениях личных е-майл / число работников, что может характеризовать потенциальные угрозы передачи ПДн, конфиденциальной информации и пр.

В работе Р. Кини и Х. Райфа приведен пример сепарабельных функций полезности ([64], стр. 6), которые можно применять и в других приложениях, связанных с учетом различных факторов социоинженерных атак. На специализированных конференциях (ISPIT, Infosecurity, ИБ КВО АСУТП и пр.) отмечалась опасность атак, которые отличаются сложностью детектирования: либо полностью не обнаруживаемые (при использовании типовых шаблонов настроек СрЗИ), либо с так называемым «*малым ущербом*», плохо обнаруживаемые (в случае «пограничных состояний» триггеров безопасности). Весьма ярким примером является новая техника внедрения кода, получившей название «Process Doppelgänging», о которой было рассказано на конференции Black Hat Europe 2017 в Лондоне[196]. Новая атака работает на всех версиях

196 https://www.securitylab.ru/news/490142.php

Windows и позволяет обойти большинство современных антивирусов («Касперский», ESET, McAfee, Norton, AVG, Sophos, Trend Micro, Panda)[197].

3.7.3 Меры обеспечения ИБ для защиты от социальных атак

На основании положений, приведенных выше, рассмотрим перечень мер и средств обеспечения ИБ для противодействия и создания системы защиты от социоинженерных атак (см. таблицу 3.13). В качестве методической базы рассмотрим Приложение А стандарта ISO 27001 [317].

Таблица 3.13 – Список мер ИБ для защиты от «социальных атак» (фрагмент)

Код	Наименование	Описание меры (средства) обеспечения ИБ
A.7.1.2	Условия трудоустройства	Договорными соглашениями с работниками и подрядчиками должны определять их ответственность в поле информационной безопасности.
A.7.2.3	Дисциплинарный процесс	Должен существовать формализованный дисциплинарный процесс, на основании которого предпринимаются меры в отношении сотрудников, совершивших нарушение.
A.8.1.3	Допустимое использование активов	Правила допустимого использования активов, связанных с информацией и средствами для обработки информации, должны быть определены, документированы и внедрены.
A.8.2.1	Классификация информации	Информация должна быть классифицирована с точки зрения правовых требований, ценности, критичности и чувствительности к нарушению конфиденциальности или изменению.
A.9.4.3	Система управления паролями	Система управления паролями должна быть интерактивной и обеспечивать качество паролей.
A.11.2.9	Политика чистого рабочего стола и экрана	Должна быть внедрена Политика чистого рабочего стола для бумажных активов и съемных носителей информации, а также Политика чистого экрана для средств обработки информации.
A.18.1.4	Конфиденциальность и защита персональной информации	Конфиденциальность и защита персональной информации должна быть обеспечена в соответствии с требованиями законодательства, где это применимо.

197 https://www.blackhat.com/eu-17/briefings.html#lost-in-transaction-process-doppelgänging

3.7.4 Формирование «профиля негодяя»

Для определения типов нарушителей ИБ, использующих методы социальной инженерии, представляется полезным сформировать «*профиль негодяя*». Этот профиль позволит с определенной точностью оценить возможности потенциального нарушителя нанести ущерб с помощью методов социальной инженерии, выявить уязвимости в существующей СМИБ и предложить меры, повышающие уровень обеспечения ИБ. Достаточно интересная ситуация может наблюдаться при недостаточном внимании к вопросам социальной инженерии, например, при использовании различных моделей аутсорсинга и, прежде всего, при аутсорсинге ИТ-сервисов или функций ИБ. В отличие от ситуации, в которой возможен прямой контроль, например: «*человек – человек*», более высокие риски ИБ будут наблюдаться в ситуации «*человек – организация*»[198]. Существенно возрастает степень неопределенности (см. «классическое» определение риска из ISO серии 31000 или 27005). Но в ситуации «*организация – организация*» возникает уже **n**-мерная неопределенность, т.к. сама роль «аутсорсера» для любого заказчика вовсе не прозрачна. Возникает масса вопросов, которые физически не могут быть определены в договорах (SLA) и, соответственно, контролироваться, например: кто персонально (**k** из **n**) будет иметь доступ к моей «чувствительной» информации? Кому (**m** из **k**) они могут рассказать (передать) информацию, к которой получили доступ? Кто (**k** из **n** ∪ **m** из **k**) из них через месяц планирует уволиться, и к кому (**p** из **k**) они планируют перейти (к конкурентам – **q** из **p**)? Все эти вопросы, к сожалению, не могут быть формально отражены в SLA, и даже персональные обязательства (NDA), как показала практика ряда крупнейших утечек от подрядчиков Пентагона, мало помогают обеспечению ИБ. На SOC-Форуме 2017 «Практика противодействия кибератакам и построения центров мониторинга ИБ» эксперты обсуждали, последствия использования социальной инженерии мошенниками[199]. Весьма интересно рассмотреть 7

198 http://www.securitylab.ru/blog/personal/ddudko/205730.php
199 https://www.securitylab.ru/news/489846.php

базовых принципов People-Centric Security (PCS), которые предложены Gartner[200] и которые, в определенном аспекте, могут быть полезны для поставленной цели.

Формирование «профиля негодяя» в документах ОБСЕ

В «Руководстве» ([182]) отмечается, что при рассмотрении вопроса качественного состава группы экспертов ИБ, следует опираться на международный опыт, который показывает, что уровень должностного положения в рамках организации, весьма важен. Эту ситуацию следует трактовать и в обратную сторону – для оценки потенциала «негодяя»; а для этого, помимо общих факторов, имеющих значение для участников противоборства, следует выделить опыт и знания. Например, возможна и компрометация репутации российской компании (RVision) со стороны иностранных «партнеров» (IBM), стремящихся выиграть ценный контракт[201]. В частности, в «Руководстве» ([182]) отмечается, что в некоторых странах участники процесса обмена информацией в области ИБ преднамеренно не допустили к участию в нем экспертов из определенных областей. Например, члены правоохранительного сообщества некоторых стран не участвуют в обмене информацией, поскольку разглашение определенных сведений потребовало бы от них совершения действий, которые могли бы отрицательно сказаться на готовности участников делиться какой-либо информацией в принципе.

Учет человеческого фактора в документах ИКАО

В документе ИКАО «Руководство по безопасности для защиты гражданской авиации от актов незаконного вмешательства» (Doc 8973) определены важные требования по учету человеческого фактора:

– *«Знание человеческого фактора»* (п. 8.2.1.8).
– *«Неэффективная рабочая практика»* (п. 8.2.2.2).

Отметим, что в документе ИКАО Doc 8973 определены также и мероприятия, связанные с человеческим фактором:

– «*Связанные с человеческим фактором мероприятия*» (п. 8.2.5.1);

---

200 https://cybersecurity.isaca.org/static-assets/documents/State-of-Cybersecurity-part-2-infographic_res_eng_0517.pdf
201 https://rvision.pro/blog-posts/ofitsialnaya-pozitsiya-kompanii-r-vision-po-publikatsii-v-ramkah-elektronnogo-auktsiona-0273100000117000146/

– «*Мотивация персонала*» (8.3.10.2);

– «*Персонал, не относящийся к службе безопасности*» (п. 8.4.1);

– «*Изучение любых пробелов в личном деле»* (п. 11.2.6.9);

– «*Строгие правила отбора (квалификационные критерии)»* (п. 12.4.2.1).

В таблице 3.14 приведены важные аспекты человеческого фактора, которые следует учесть при создании «профиля негодяя»:

Таблица 3.14 –Аспекты человеческого фактора

Пользователи	Пользователи системы и их характеристики, например, сотрудники службы безопасности, руководители низшего звена, дежурные менеджеры, пассажиры и т.д.
Задачи	Текущие задачи пользователей и специалистов по техническому обслуживанию, которые они выполняют, и каким образом. Будущие задачи пользователей и специалистов по техническому обслуживанию, которые они должны будут выполнять, и каким образом.
Результаты	Последствия внедрения новой системы для пользователей и любых других участвующих сторон; может ли это увеличить рабочую нагрузку сотрудников службы безопасности
Риск	Угрозы и риски, создаваемые производственной средой, и как это повлияет на требования.
Ресурсы	Навыки и способности, необходимые персоналу для эксплуатации оборудования.
Требования	Любые, ориентированные на человеческий фактор требования, которые будут создавать препятствия при разработке, например: все ли сотрудники службы безопасности полностью понимают характер изменений, внесенных в процедуры обеспечения безопасности? Является ли достаточным уровень подготовки персонала, организуемой изготовителем оборудования для целей безопасности?

Формирование «профиля нарушителя» в документах ИКАО

В документе «Человеческий фактор в системе мер безопасности гражданской авиации» (Doc 9808, ИКАО) вводится определение «*культуры безопасности*» и, как следствие, определены требования для создания позитивной культуры безопасности. Характеристики различных видов культуры безопасности представлены в таблице 3.15.

Таблица 3.15 – Спецификация различных видов культур безопасности

Культура безопасности: Характеристики	**Низкая**	**Бюрократическая**	**Позитивная**
Информация об опасных факторах:	Замалчивается	Игнорируется	Активно отслеживается
Лиц, сообщающих об опасных факторах:	Не поддерживают или наказывают	Терпят	Обучают и поощряют
Ответственность за безопасность:	Избегается	Дробится на части	Является общей
Распространение информации об опасных факторах:	Не поощряется	Разрешается, но не поощряется	Вознаграждается
Сбои приводят к:	Укрытию фактов	Локальным решениям	Расследованиям и реформе системы
Новые идеи:	Отвергаются	Рассматриваются как новые проблемы (а не возможности)	Приветствуются

Отмечено, что культура безопасности является естественным побочным продуктом корпоративной культуры и определяет границы приемлемого поведения человека на рабочем месте путем установления поведенческих норм и пределов, что является основой для управленческих решений и решений, принимаемых сотрудниками по вопросам безопасности. Признаки позитивной культуры безопасности:

1. Руководители уделяют большое внимание вопросам БП как составной части стратегии контроля факторов риска (т. е. минимизации потерь);
2. В организации создается климат, способствующий позитивному отношению к критике, замечаниям и информации по вопросам безопасности, обеспечивается «некарательная» производственная среда;
3. Оперативно и эффективно принимаются меры для уменьшения последствий выявленных недостатков в области обеспечения БП;
4. На всех уровнях организации существует понимание важности передачи соответствующей информации по вопросам БП;

5. Существуют реалистичные и действенные правила в отношении опасных факторов, вопросов БП и потенциальных источников ущерба;
6. Персонал подготовлен и осознает последствия небезопасных действий;
7. Число случаев рискованного поведения незначительно, и в организации существует этика безопасности, которая не поощряет такое поведение.

Определение «профиля нарушителя» как функции ценности

Для реализации «профиля негодяя» воспользуемся принципом оценки эффективности альтернативных действий, предложенным Р.Кини и Х. Райфа [64]. Определим перечень критериев, по которым будут оцениваться возможности потенциального нарушителя ИБ как X*n*, примем, что критерии X*n* будут ориентированы положительно, т.е. будем заинтересованы в выявлении тех нарушителей, которые имеют наибольшие возможности для реализации социоинженерных атак. Определим, что «профиль негодяя» может быть оценен как аддитивная функция ценности вида:

$$C^{\sim}\ (x_1, x_2, x_3, \dots x_n,) = \sum_{k=1}^{n} \alpha_k * C_k^{\sim}(x_k,)$$

где:

$$\sum_{k=1}^{n} \alpha_k = 1 \text{ и } 0 < \alpha_k < 1$$

Определим, что набор X*n* при выбранном n = 4 образует «профиль негодяя» $C^{\sim}$ (см. рисунок 3.13).

Предлагаются следующие основные критерии:

X_1 – типы затрагиваемых активов;

X_2 – размер потенциального ущерба в случае успешной атаки;

X_3 – возможности потенциального нарушителя;

X_4 – результативность существующих мер защиты (СрЗИ, СКЗИ).

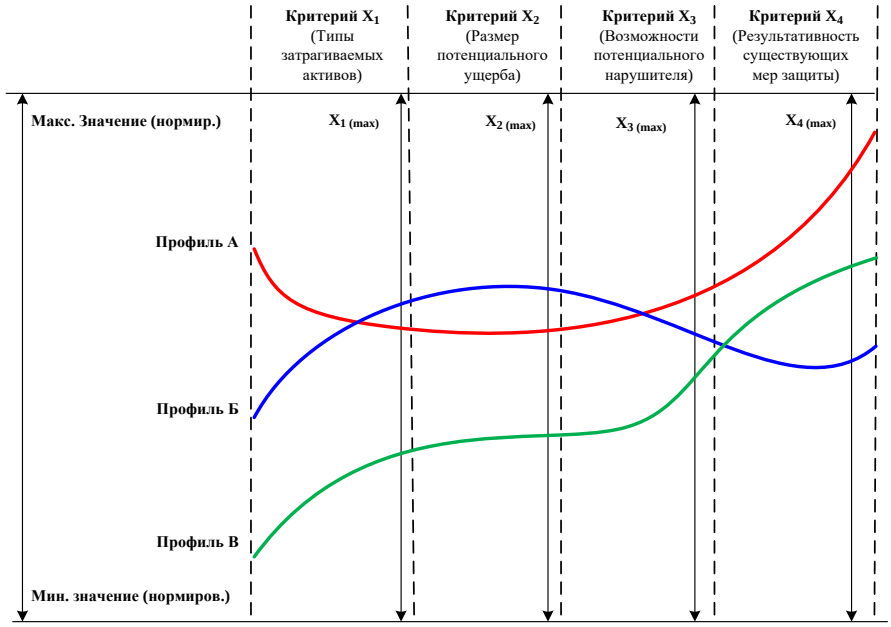


Рисунок 3.13 – Сопоставление различных «профилей негодяя»

При необходимости формирования расширенного «профиля негодяя» для целей описания возможностей социоинженерных атак применительно к конкретным СлПО могут быть выбраны иные критерии.

3.8 Разработка метода «мгновенных аудитов» ИБ

3.8.1 Постановка задачи

Проблема выполнения аудита (как процесс оценивания) для больших и/или сложных систем рассматривалась в классических трудах Н. Винера, Р.Кини, Х. Райфа, И. Пригожина ([13], [64], [147], [140]). В работе Н. Винера отмечено требование невмешательства человека в процесс, начиная с момента ввода исходных данных и до получения результата ([13], стр. 47). В работе Р.Кини и Х. Райфа важное внимание уделено потоку данных, поступающему уже непосредственно в самом процессе. Отмечается, что выработка и анализ возможных альтернатив действий становится явно зависимым от информации, которая станет известна уже в процессе ([64], стр. 24). В работе И. Пригожина и И. Стенгерс [150] отмечается подход К. Рубино (*Rubino C.)*, который обращает внимание на философский принцип выполнения любой деятельности (в т.ч. оценки) – при рассмотрении любого предмета не следует стремиться к большей точности, чем допускает природа предмета. Этот постулат является продолжением «*аристотелевской мудрости*» (например, в работе Аристотеля

«Этика»). Поскольку «*любые процессы, управляемые людьми, ненадёжны*», крупнейшие поставщики средств ИБ предлагают «единственный» вариант – только постоянное совершенствование технических СрЗИ, в частности, Check Point Threat Emulation и Qualys Continuous Monitoring ([273], [172], [288]). Подобная оценка представляется коммерчески выгодной, но весьма далекой от решения хорошо известной технической проблемы – противостояния СрЗИ как «брони» и угроз – как «снаряда».

Очевидно, что «гонка вооружения» между целевыми (таргетированными) атаками ("*advanced persistent threats*", APT) не приведет в ближайшем времени к повышению уровня защищенности объектов, и это отмечается многими экспертами ([273], [172], [288]). В этой ситуации предлагается применять не только технический подход (СрЗИ), но предложить комбинированный метод, основанный на концепции «мгновенных аудитов» ИБ. Методической базой концепции «мгновенных аудитов» является семейство стандартов ISO серии 27001 и 19011, дополненное множеством (расширяемым) метрик ИБ для формирования количественной оценки уровня защищенности объекта ([20], [317], [318]). В частности, рекомендуется применять дополнительно количественные метрики обеспечения ИБ из стандартов ISO серии 20000 (для управления ИТ-услугами, например – SLA) [311] и ISO серии 22301 (для управления непрерывностью бизнеса, например – RTO, RPO) [315]. В отрасли известны примеры оценки убытков при остановке работы корпоративных ИС на одни сутки (обзор «Коммерсант»[202]). Треть организаций (33%) считают, что потеряют 0,5–2 млн. руб., 19% организаций дают оценку минимум в 50 млн. руб. 23% уверены, что за сутки потеряют до 0,5 млн. руб.

Для успешного решения отраслевых задач ИБ необходимо принять во внимание дополнительно отраслевые стандарты, в частности, для аэродромных комплексов – IATA [326], [327]. Необходимо отметить, что сам процесс аудита (в том числе ИБ) хорошо известен и является обязательным требованием всех

---

202 https://www.kommersant.ru/doc/3494853?from=four_tech

упомянутых стандартов ISO (в РФ они приняты как ГОСТ Р ИСО[203]). При этом на усмотрение организации отдаются вопросы планирования (частоты) выполнения аудита и области охвата (*scope*) ([20], [21]). Именно на процесс аудита, управляемый по частоте, возлагается задача оперативного (в режиме, близком к PPB) выявления уязвимостей в ИС. Для формирования концепции «мгновенных аудитов» ИБ, как средства противодействия АТР, представляется полезным применить известное математическое понятие предела функции, точнее, предела слева, которое позволит формировать количественные оценки уровня обеспечения ИБ в процессе выполнения аудита ИБ [94].

3.8.2 Обоснование практической ценности «мгновенных аудитов»

Практическая ценность предлагаемой концепции «мгновенных аудитов» основана на известных фактах, что порядка 96% успешных взломов можно было бы избежать, если бы был внедрен ряд простых мер ИБ, а более 75% атак использовали уже известные уязвимости, которые могли бы быть «закрыты» регулярными патчами безопасности ([273], [172]). При этом отмечается, что 85% реально произошедших вторжений были обнаружены спустя месяцы (среднее время обнаружения – 5 месяцев) [273]. Дополнительно отметим отчет ЦБ РФ за 2014 г. с данными по оценке обеспечения ИБ на уровне пользователей [175]. В целом банковская система РФ продемонстрировала способность останавливать от 46% до 38% несанкционированных операций (НСО), а средняя сумма одной НСО составляет 335 тыс. руб. В большинстве случаев НСО, связанные с попытками списания денежных средств посредством систем дистанционного банковского обслуживания, произошли вследствие воздействия вредоносного кода на используемое устройство.

В качестве мер противодействия УБИ в настоящее время применяются различные подходы, направленные, в основном, на пресечение последствий потенциально возможных угроз, но не на выявление и устранение уязвимостей, например:

1. «Песочницы», имитирующие рабочие станции организации;

---

[203] https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty

2. Анализ аномальной сетевой активности;

3. Поведенческий анализ рабочих станций.

Соответственно, для атак, реакция на которые крайне критична по времени, указанные выше примеры дают известный эффект только при постоянном наращивании вычислительных ресурсов для сокращения времени «аналитических» проверок СрЗИ в режиме, близком к РРВ. При этом не инициируется объективный анализ всей совокупности потенциальных уязвимостей и не затрагивается уровень технологических, программных и иных уязвимостей ([315], [318]). Обратим внимание, что объективный анализ всей совокупности потенциальных уязвимостей должен учитывать, насколько это возможно, информацию о скорости закрытия уже известных уязвимостей. Например, Positive Technologis[204] нашла уязвимость в системе Siemens SICAM PAS для управления энергосистемами, которая имеет оценку 9,8 по 10-балльной шкале CVSS v.3, данное ПО используется и в РФ. Отмечается, что производитель подтвердил наличие брешей и выпустил рекомендации по их устранению, но это редкое исключение: лишь 14% уязвимостей АСУ ТП устранены в течение 3 месяцев, 34% устранялись более 3 месяцев, а оставшиеся 52% ошибок – либо вовсе не исправлены, либо производитель не сообщает о времени устранения. Рассмотрим еще один пример «Лаборатории Касперского», представленный на конференции ISMF-2017: специалистами Kaspersky ICS было выявлено 75 уязвимостей (всего 30 закрыто), а экспертами ICS CERT (США) выявлено 187 уязвимостей (всего 139 закрыто)[205]. Примерно такие же данные показывают другие разработчики: согласно официальному сообщению компании Oracle[206], более 100 уязвимостей можно было эксплуатировать удаленно, без аутентификации.

Рассмотрим дополнительно обоснование адекватности результатов оценки уровня обеспечения ИБ, получаемых в случае применения концепции «мгновенных аудитов». В работе Ф. Перегудова и Ф. Тарасенко отмечается, что

---

204 https://www.ptsecurity.com/ru-ru/about/news/131504/

205 http://www.itsecurityforum.ru/materials/

206 https://xakep.ru/2017/04/19/oracle-april-cpu/

адекватность подразумевает выполнение определенных требований «не вообще», а в той мере, которая достаточна для достижения цели. Можно дать оценку адекватности, если ввести количественную меру, или, цитируя точно: “*количественно выражаемую меру адекватности*” ([151], стр. 51). Также можно применить рекомендации Р. Кини и Х. Райфа по введению групповых решений, которые, цитируя точно: “*систематизируют решение конкретных проблем*” ([64], стр. 22). На практике эти рекомендации применяются для формирования количественных метрик, пригодных, в том числе, для групповых оценок деятельности в области ИБ, например, оценивается динамика количества выявленных уязвимостей в ИС по результатам аудита ИБ. В работе Н. Винера отмечается прогресс передачи «полезных знаний» в развитии промышленных революций, в частности, что может «*предложить для продажи*» квалифицированный специалист ([13], стр. 79). Очевидно, что прямой участник любого процесса аудита – аудитор, и он обязан «предложить» ЛПР свои наилучшие знания, усилия, компетенции и опыт для того, чтобы внести посильный вклад в совершенствование процесса управления ИБ.

Процесс аудита, как любой процесс оценивания, предполагает получение объективных оценок на основании свидетельств аудита, которые затем могут быть дополнительно проверены независимыми экспертами [20]. При этом сам процесс оценивания предполагает определенные временные рамки (как было показано выше [64]), при этом управление «частотностью аудита» позволяет более оперативно контролировать динамику процесса изменения оценки уровня обеспечения ИБ против любых изменений (соответственно – «динамической перестройки» критериев аудита) [20]. Например, низкая (или даже нулевая) частота независимого аудита может привести к компрометации крупной платежной системы – транспортных карт «Тройка»[207]. Хакеры получили доступ к ключам шифрования и потери составили примерно 2 млн. руб. В картах «Тройка» используется чип Mifare, в котором применяются старые алгоритмы

[207] http://www.rbc.ru/technology_and_media/25/08/2017/599f0c6e9a7947641df10f03?from=main

шифрования, скомпрометированные еще в 2008 г., и результаты исследований были опубликованы группой из голландского университета Radboud.

Важным преимуществом предложенной концепции является акцентирование именно на получении численных оценок, а не простого «соответствия» или «несоответствия». Именно периодическое систематическое получение измеримых численных оценок ИБ представляется практически полезным для ЛПР. Соответственно, адекватность результатов оценки уровня обеспечения ИБ допустимо трактовать, во-первых, как соответствие установленным критериям аудита, во-вторых, соответствие процессным требованиям аудита ИБ и, в-третьих – получение «текущих» значений степени обеспечения ИБ, необходимых для поддержки «разумных решений» ЛПР.

3.8.3 Требования ISO к проведению аудита ИБ

Требования выполнения аудита ИБ на постоянной циклической основе определены в стандарте ISO/IEC 17021 [21]. В частности, отмечается, что «*программа аудита должна включать в себя проведение двухэтапного первичного аудита, надзорных аудитов в течение первого и второго года и ресертификационного аудита – в течение третьего года до истечения срока действия сертификата*». Трехлетний цикл сертификации начинается с принятия решения о сертификации (п. 9.1.1 [21]). Также отмечается частота выполнения надзорных аудитов: «*надзорные аудиты должны проводиться, по крайней мере, один раз в год*» (п. 9.3.2.2). Аналогичные требования предъявляются к проведению аудита по требованию PCI DSS, в частности, все три вида аудита (QSA – внешний, ISA – внутренний и SAQ – самооценка) проводятся с периодичностью 1 раз в год. Последовательность выполнения аудита СМИБ с учетом требований ISO/IEC 17021:2006 состоит из: CA – сертификационного аудита (1-й и 2-й этапы соответственно), SA – надзорного аудита (1-го и 2-го года соответственно) и RA – ресертификационного аудита (см. рисунок 3.14).

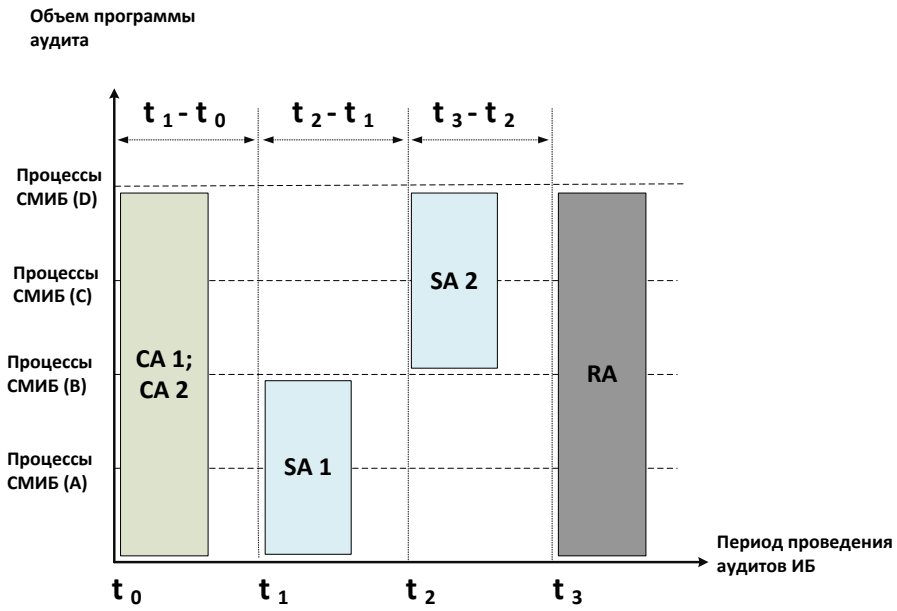


Рисунок 3.14 – Схема выполнения аудита СМИБ

Важно, что базовые интервалы $(t_1 - t_0)$, $(t_2 - t_1)$ и $(t_3 - t_2)$ в общем случае (без экстраординарных ситуаций) равны. Дополнительно необходимо отметить, что аналогичного подхода придерживаются и иные международные системы аудита, в частности – IATA. В стандарте ISO 19011 (п. 5.2, e, h) непосредственно указано, что цели аудита должны формироваться с учетом: правовых и иных других требований, которые организация принимает на себя; показателей деятельности организации (случаи возникновения нарушений, инцидентов или жалоб потребителей) и результатов предыдущих аудитов [21]. Также ISO 19011 при формировании объема программы аудита рекомендует принять во внимание иные факторы [21]. Соответственно, представляется экономически нецелесообразным постоянно осуществлять значительные затраты на применение только дорогостоящих СрЗИ (СКЗИ) – если, например, на уровне рабочих станций не выполняются требования доменных политик ИБ, на уровне пользователей – не выполняется информирование о правилах работы в сети интернет, на уровне руководителей – не выполняется аудит ИБ, анализ отчетов и принятия безотлагательных мер в области ИБ.

3.8.4 Концепция «мгновенных аудитов» ИБ

Концепция «мгновенных аудитов» предполагает реализацию принципа выполнения аудита ИБ с частотой, определяемой высшим менеджментом (ЛПР)

и зависящей от предыдущего состояния «слева» оценки уровня обеспечения ИБ объекта ([138], [16], [7]). В работе Н. Винера показано, что метод управления с помощью информирующей обратной связи возможно реализовать в форме механизма ([13], стр. 183). Для данной задачи наибольшее значение для целей аудита ИБ как раз играет метод опережающего управления, при котором ЛПР не ждет, когда «*машину поведет на скользкой дороге*», как указано в примере Н. Винера. В случае управления СлПО именно механизм «*мгновенных аудитов*» ИБ, реализуемый, в том числе, с помощью средств автоматизации, может позволить удержать объект в заранее заданных управляемых условиях.

В случае, если предыдущий Аудит_1 ИБ, проведенный, предположим, месяц назад (отметка t_0), выявил ряд несоответствий (в терминах [21]) и показал, что 40% компьютеров по-прежнему работают под Windows XP с SP2, на 60% рабочих станций пользователи обладают правами администратора, на 70% ноутбуков обновление антивируса не выполняются и/или отключены, то оценка (отметка t_1) текущего уровня обеспечения ИБ $R_{base} \mid t_1 <= R_{base} \mid t_0$, т.е. не выше предыдущей (см. рисунок 3.15).

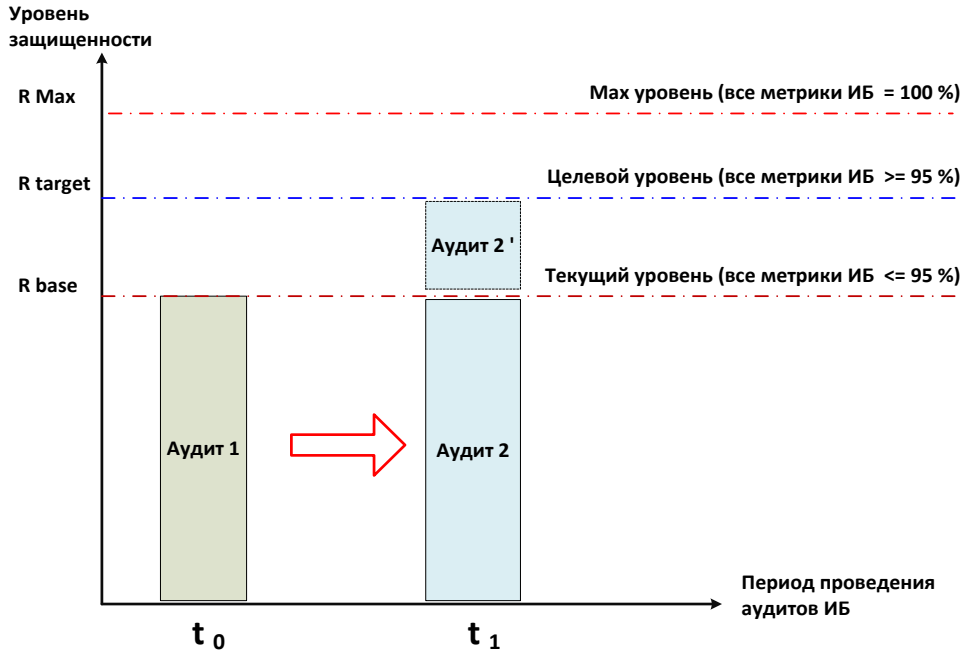


Рисунок 3.15 – Оценка достижения уровней оценки обеспечения ИБ

Также маловероятно и экономически нецелесообразно проводить Аудит_2′ в надежде достигнуть на отметке t_1 целевой уровень обеспечения ИБ R_{target}, например, 95%. Соответственно, текущая оценка уровня обеспечения ИБ

объекта (отметка t_1) $R_{target} | t_1$ соответствует оценке слева (отметка t_0) $R_{base} | t_0$ при отсутствии изменений в состоянии объекта, выявленных на предыдущем Аудите_1.

В качестве примера рассмотрим сообщение «Лаборатории Касперского»[208] о вирусе-шифровальщике WannaCry. Анализ показал, что атака происходила через известную сетевую уязвимость Microsoft Security Bulletin MS17-010. В то же время известно, что патч, закрывающий эту уязвимость для ОС Windows Vista и старше, стал доступен еще 3 месяца назад. Более того, 19.05.2017 Microsoft выпустила даже патч для Windows XP, не связанный с WannaCry – KB982316 для уязвимости в SMB. Как оказалось, обновление было готово еще в феврале 2017 г. и могло предотвратить волну атак WannaCry[209].

Обратим внимание, что при аудите АСУТП важное значение имеет своевременное получение отчетов об уязвимостях. В отчете компании Dragos показано, что в 2017 г. было опубликовано 163 рекомендации с описанием различных уязвимостей, позволяющих вызвать сбои в работе целевой системы[210]. По словам исследователей, одной из основных проблем являются трудности при исправлении уязвимостей в АСУ ТП, т.к. определенные особенности данных систем часто приводят к задержкам при установке исправлений – иногда на неопределенный срок (!). Помимо этого, пользователям надо иметь в виду, что 64% уязвимостей, были обнаружены в компонентах, которые изначально являлись небезопасными[211].

При изменении на интервале $\mathbf{(t_0 - t_1)}$ состава мер (средств) ИБ, закрытие выявленных на Аудит_1 несоответствий (например, проведения дополнительного обучения), выполнение последующего аудита (Аудит_2′) может иметь смысл для достижения R_{target}. Важно, что частота выполнения аудита ИБ определяется, в том числе, и допустимым уменьшением интервала $\mathbf{(t_0 - t_1)}$, например, с ежегодного (как это принято в СМИБ, PCI DSS, IATA) до

208 http://www.rbc.ru/society/12/05/2017/5915ebf29a794763a8bff785
209 http://www.securitylab.ru/news/486223.php
210 https://www.dragos.com/media/2017-Review-Industrial-Control-Vulnerabilities.pdf
211 https://www.securitylab.ru/news/491822.php

ежемесячного (еженедельного) и чаще – по требованию ЛПР. В доказательство этого высказывания предоставим пример стабильного роста на 10 % в год уязвимых приложений Adobe Flash (*outdated versions*), и по состоянию на 2017 г. их доля достигает уже 53%[212]. Очевидно, что это обстоятельство является критичным для многих узлов корпоративной сети. Отметим, что если время реагирования меньше, чем время, необходимое атакующему для нанесения ущерба, то система находится в безопасности. Эта концепция известна под названием «*временная безопасность*»[213]. Эта взаимосвязь актуальна для всех видов кибератак, особенно в случае нападения на важнейшие КВО ТЭК, где ущерб может быть катастрофическим [182]. Представляется важным, чтобы система безопасности регистрировала события ИБ[214], которые могут помочь в выявлении нарушений ИБ, например:

– неудачные и успешные входы в систему,
– попытки подключения к службам,
– аномальные показания датчиков.

Проблема определения оптимальной частоты аудита ИБ может рассматриваться ЛПР на основании полученных наборов оценок уровня обеспечения ИБ и проведенного анализа в рамках стандартной процедуры «Анализ со стороны руководства» (*Management review*) [317], [311], [321], [315]. Очевидно, что бессмысленно выполнять подряд аудиты ИБ друг за другом, не успевая исправить выявленные несоответствия, не выявив «корневую» (*root*) причину и не успевая полностью реализовать комплекс корректирующих мер. Этот тезис необходимо подкрепить экспертным заключением, например, в Positive Technologies выяснили, что в более, чем половине (55%) исследованных корпоративных ИС, нарушитель с минимальными знаниями и низкой квалификацией способен преодолеть внешний периметр[215]. При этом средний возраст уязвимостей систем достигает нескольких лет (!): были обнаружены ИС,

---

212 https://threatpost.com/53-percent-of-enterprise-flash-installs-are-outdated/126069/
213 http://securityaffairs.co/wordpress/8175/hacking/saudi-aramco-are-we-ready-for-anescalation-of-cyber-attacks.html
214 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), стр 14
215 https://www.phdays.ru/program/256682/

содержащие уязвимости на протяжении 9 лет, а самая старая из обнаруженных уязвимостей опубликована более 17 лет назад. Соответственно, возникает ряд вопросов к процессу анализа защищенности в таких системах: в чем причины такой продолжительности уязвимости ИС?

Обратим внимание на факт разрыва длительного сотрудничества «Транснефть» и Schneider Electric, которая поставляла корпорации АСУ ТП. По итогам глубокого анализа рисков в части ИБ АСУ ТП были найдены многочисленные критичные уязвимости, в том числе, во встроенных механизмах защиты АСУ ТП. Эти данные были переданы в Schneider Electric, но реакции от поставщика пришлось ждать более полугода, что привело к отказу применения оборудования[216].

Метрикой для «старта» следующего аудита ИБ может являться скорость «замыкания» мини-цикла PDCA, которая, объективно, формирует предел $\mathbf{lim\ (t_k - t_i)}$. Соответственно, для достижения R_{target} период аудита ИБ может уменьшаться как $\lim\ \mathbf{(t_k - t_i) \rightarrow 0}$ (см. рисунок 3.16).

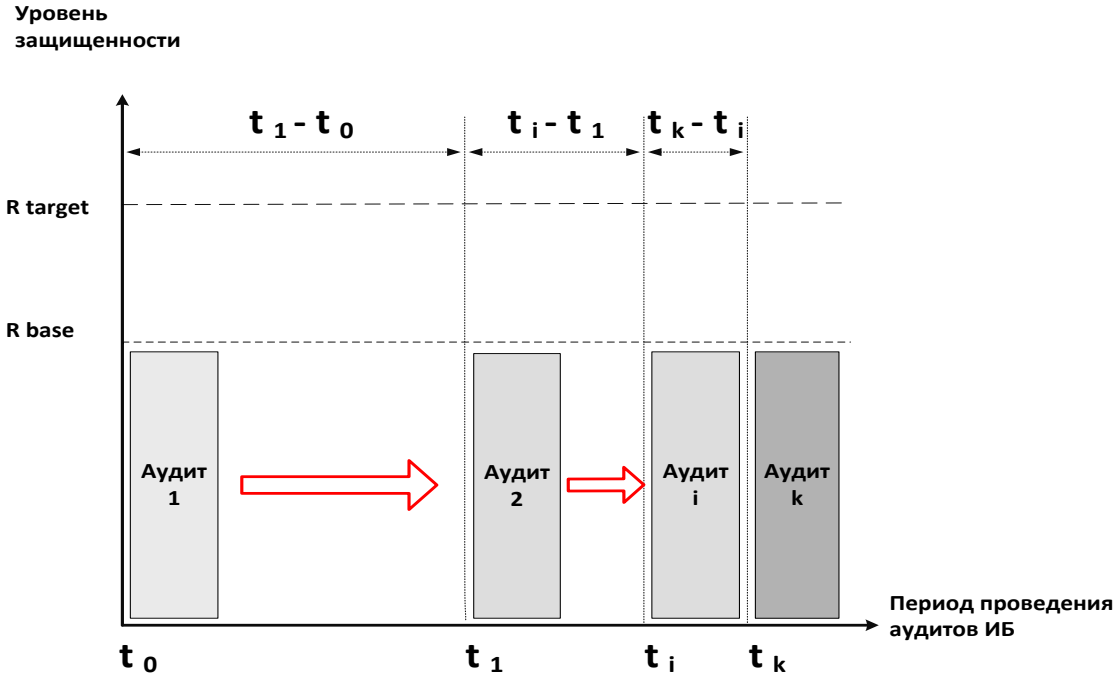


Рисунок 3.16 – Снижение периода оперативного противодействия угрозам

Кроме того, для эффективного противодействия APT необходимо уменьшить период выявления, анализа и «*закрытия*» несоответствий, так как

216 http://www.cnews.ru/news/top/2017-12-14_transneft_otkazalas_sotrudnichat_so_schneider

успешная реализация этого процесса представляется значительно быстрее, чем выбор, закупка, доставка, установка и настройка новых и новых СрЗИ. При этом, во-первых, выполняются все требования ISO, во-вторых, дополнительно выполняются требования ЛПР (не желающих ждать целый год для приведения оценки ИБ к требуемому бизнесом уровню обеспечения ИБ) и, в-третьих, решаются вопросы оперативного противодействия современным угрозам (в пределе «время реакции» СМИБ $\mathbf{(t_k - t_i)}$ стремится к нулю).

3.8.5 Система метрик процесса «мгновенных аудитов»

Любая концепция обеспечения ИБ требует обоснования у ЛПР (владельцев ценных для бизнеса активов) численных оценок достигнутого (реального) уровня обеспечения ИБ. Предлагаемая концепция «мгновенных аудитов» применяет систему количественных (численных) метрик ИБ:

1. Рекомендации SANS 20 Critical Security Controls.
2. Рекомендации PCI DSS (например, версии 3.0);
3. Стандарты ISO (например, ISO 27004);
4. Стандарты Центрального Банка РФ (например, СТО БР ИББС);
5. Документы ФСТЭК России (например, приказ ФСТЭК № 31).

Рассмотрим на примере систему мер (средств) обеспечения ИБ, сформированную на базе рекомендаций SANS 20 Critical Security Controls, документов ФСТЭК России [167] и стандарта ISO 27001 [317]. Примем во внимание, что состав метрик ИБ не является фиксированным (возможно расширение по требованию ЛПР и пр.), и рекомендуемые метрики содержат не только СрЗИ, но и комплекс организационных мер (см. таблицу 3.16).

Рассмотрим далее на примере оценку системы мер (средств) обеспечения ИБ, установленных действующим законодательством РФ, но невыполняемых полностью или частично операторами связи. По итогам волны «телефонного терроризма» в 2017 г. ФСБ провела оценку результативности СОРМ, внедренных на сетях крупнейших операторов. Руководитель ФСБ отмечал, что

определить местонахождение преступников «*сложно из-за того, что они использовали в своей работе IP-технологии*»[217].

Таблица 3.16 – Соответствие мер (средств) обеспечения ИБ (фрагмент)

№ п.п.	SANS 20 Critical Security Controls	Мера ИБ (ISO 27001)	Мера защиты (ФСТЭК)
1.	Учет авторизованных (неавторизованных) устройств	A.8.1.1 – A.8.1.4, A.11.2.8	ИАФ.2
2.	Учет авторизованного (неавторизованного) ПО	A.8.1.1 – A.8.1.4	ИАФ.7 ОПС.0 - ОПС.4
3.	Безопасная конфигурация рабочих станций, серверов, ноутбуков	A.12.1, A.18.2.3	ЗСВ.7, ЗИС.29 УКФ.0 – УКФ.5
4.	Постоянное обнаружение и оценка уязвимостей	A.12.6, A.17.1.2	АНЗ.1 ОБР.1
5.	Антивирусная защита почтовых приложений	A.12.5.1, A. 13.2.3	АВЗ.0 – АВЗ.3
6.	Прикладное ПО для обеспечения ИБ	A.9.4.4	ИАФ.7 ЗИС.25
7.	Обучение и тренинги в области ИБ	A.7.2.2	ДНС.2 ИПО.0 – ИПО.3
8.	Безопасная конфигурация сетевых устройств	A.13.1.1	УПД.3

На примере арбитражного дела № А40-40245/17-17-368 выяснилось, что в сетях связи ПАО «ВымпелКом» на территории Сахалинской области попросту не записывается интернет-трафик пользователей[218]. И эти факты не единичные: анализ арбитражной практики 2016–2017 гг. показал, что Роскомнадзор на основании обращения ФСБ возбудил 451 дело об административных нарушениях в связи с затягиванием сроков внедрения и модернизации СОРМ.

3.8.6 Обоснование базы концепции «мгновенных аудитов» ИБ

Для формирования оценки уровня обеспечения ИБ по результатам аудита ИБ необходимо применять достоверные математические понятия, дающие обоснование предложенной концепции, в частности, предела функции слева:

$$\lim_{x \to a-0} f(x) = A \Leftrightarrow \forall \varepsilon > 0 \; \exists \delta =$$

$$= \delta(\varepsilon) > 0 \; \forall x \in (a - \delta, a): |f(x) - A| < \varepsilon.$$

Производная функции ***f (x)*:**

[217] http://www.rbc.ru/technology_and_media/09/11/2017/5a03187e9a7947d88f988f53?from=newsfeed

[218] http://kad.arbitr.ru/PdfDocument/1eaa2106-9ccf-4fef-83ce-5d54fcb232ea/A40-40245-2017_20170420_Reshenija_i_postanovlenija.pdf

$$\lim_{\Delta x \to 0} = \frac{f(x+\Delta x)-f(x)}{\Delta x} = \lim \frac{d}{dx} f(x) = f'(x).$$

Соответствующий односторонний предел называют левой производной, обозначают $\mathbf{f'_{-}(x)}$ [57], [62].

3.8.7 Пример определения производных для «мгновенных аудитов» ИБ

Левая производная позволяет оценить требуемый интервал, на котором допустимо (по времени) могут быть выполнены необходимые изменения в СМИБ и обосновано проведение нового аудита ИБ. Для цели противодействиям УБИ рассмотрим действительную функцию переменных:

$$\boldsymbol{y = f\,(x_1, x_2, x_3, \dots, x_n),}$$

где, например, первые 4 переменные описывают атрибуты аудита ИБ:

- x_1 – частота проведения аудита, определяемая как отношение кол-ва аудитов в СМИБ к наблюдаемому периоду;
- x_2 – объем программы аудита, определяемый как отношение кол-ва охваченных процессов к общему кол-ву процессов в заявленной области сертификации СМИБ;
- x_3 – метрика достижения уровня обеспечения ИБ, определяемая как мера результативности СМИБ R_{base} / R_{Max};
- x_4 – метрика выполнения корректирующих действий, запланированных на интервал проведения аудитов ИБ.

Тогда частная производная первого порядка по первой переменной x_1 имеет вид:

$$\lim_{\Delta x_1 \to 0} = \frac{f(x_1+\Delta x_1, x_2, x_3, \dots, x_k) - f(x_1, x_2, x_3, \dots, x_k)}{\Delta x_1} = \frac{\partial}{\partial x_1} f(x).$$

Для одной изменяемой переменной x_1 (например, частоты проведения аудитов ИБ) оценим практическое значение частной производной (при фиксации иных переменных), получаем оценку скорости роста уровня обеспечения ИБ:

$$\frac{\partial}{\partial x_1} = f'(x_1, x_2, x_3, \dots, x_n) = \frac{\Delta R_k}{\Delta t k}.$$

Реализация концепции «мгновенных аудитов» для оценки уровня обеспечения ИБ ценных для бизнеса активов с любой требуемой частотой, может быть продемонстрирована как сокращение периода (увеличение частоты)

проведения аудита ИБ при использовании предела слева функции переменных (см. рисунок 3.17).

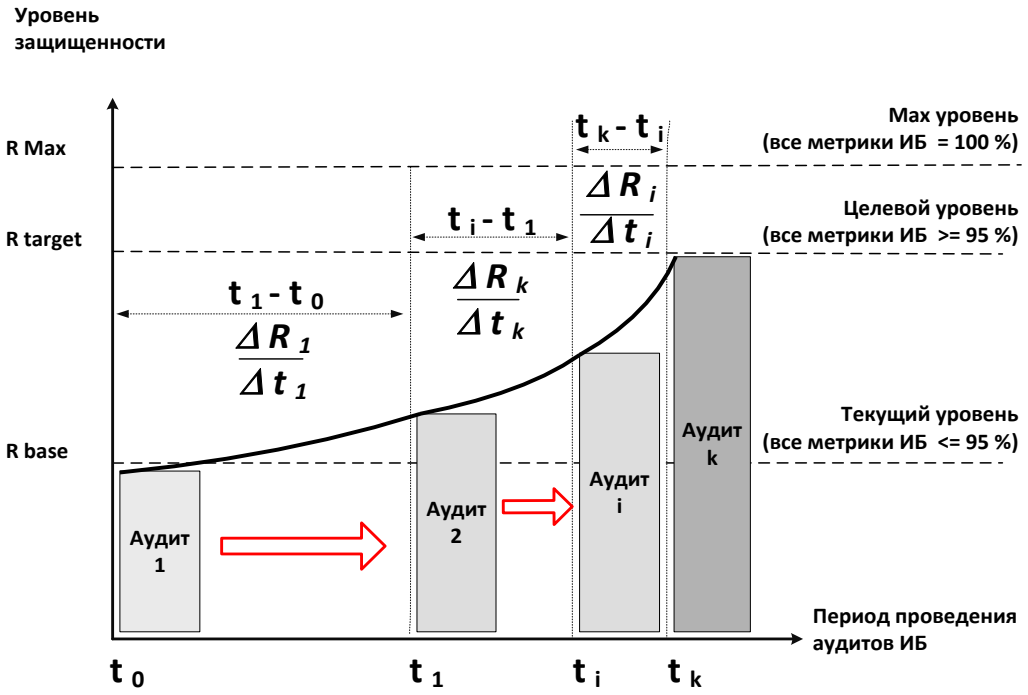


Рисунок 3.17 – Пример увеличения скорости роста уровня обеспечения ИБ

Заметим, что предложенная концепция позволяет также дополнительно исправлять возможные ошибки, присущие сложному процессу аудита, методом локализации обратным процессом, как показано в работе Н. Винера ([13], стр. 222). «Второй контур контроля», реализующий локализацию ошибки стартует с точки, где она замечена, но крайне важно обеспечить, чтобы проверка и отработка выявленной ошибки шла с такой же скоростью, как и сам процесс аудита ИБ, иначе «эффективная скорость» процесса обеспечения ИБ (в ИСМ) может снижаться из-за более медленного процесса аудита ИБ. Отметим так же, что полная «скорость реакции» СМИБ определяется частотой аудитов ИБ, что значительно превышает скорость полного цикла обновлений даже наилучших отраслевых решений СрЗИ (СКЗИ) ([273], [172], [288]). При этом объективно повышается способность системы (СМИБ или ИСМ) эффективно противодействовать УБИ в режиме, близком к РРВ. В примере для одной переменной x_1 продемонстрировано увеличение скорости роста оценки уровня обеспечения ИБ СМИБ $\frac{\Delta R_k}{\Delta t_k}$ при известных переменных процесса аудита ИБ.

3.9 Выводы к Главе 3

1. Для СлПО обеспечение комплексной безопасности является крайне важной и особо актуальной проблемой для современных объектов ТЭК и АК. Особенностями СлПО являются учет значительного множества требований безопасности: функциональной, технической, информационной, персонала, а также защита инженерной инфраструктуры. Для обеспечения безопасного функционирования СлПО необходимо применять комплексные СУ, в состав которых входят СМИБ (ИСМ), соответствующие национальным и международным стандартам (ISO, IEC, NIST, IATA, ISAGO и пр.).
2. Оценка уровня обеспечения безопасности для СлПО (ТЭК и АК) формируется по модели ИСМ для аудита ИБ, как оценка результативности по множеству возможных критериев (МАИ), оцениваемых в процессе комплексного аудита ИБ всех видов (1, 2 или 3-й стороной). Мерой оценки результативности в предложенной модели аудита ИБ в СМИБ (ИСМ) служат метрики (численные оценки), предложенные командой экспертов и утвержденные ЛПР.
3. Наибольшую ценность при проведении аудита ИБ для СлПО (АК) представляют оперативные и объективные свидетельства о результатах аудита всех видов, а также информация о «*профиле негодяя*» для эффективного противодействия опасным социоинженерным атакам.
4. Для оценки результативности СМИБ (ИСМ) для СлПО предложен **новый** метод «*мгновенных аудитов*» ИБ, основанный на реализации комплекса упреждающих мер, а не только внедрения новых СрЗИ. Ключевой особенностью метода «*мгновенных аудитов*» ИБ является формирование оценки уровня обеспечения ИБ в процессе выполнения аудита ИБ. Методической базой концепции «*мгновенных аудитов*» является семейство стандартов ISO серии 27001 и 19011, дополненное множеством метрик ИБ для формирования количественной оценки уровня обеспечения ИБ СлПО.

4 Глава. Метод исследования динамики сертификации

4.1 Общие положения

За последние несколько лет в развитии теории и практики обеспечения ИБ появились новые тенденции, связанные с применением новых риск-ориентированных подходов, внедрением новых методов и развитием общих стандартизированных подходов к СМИБ (ИСМ) [211], [213], [381]. Изучение зависимости развития различных типов организаций (например, по отраслям) от различных факторов (внутренней или внешней природы *internal issue / external issue*) представляет определенный интерес. Например, такие факторы могут быть экономическими (процессы глобализации), техническими (применение определенных технологий, например, *Cloud Security*), комбинированными или иными. Соответственно, представляет интерес получение достоверных статистических данных о динамике применения международных стандартов ISO, полученных на длительном интервале наблюдений ([97]). Эти данные позволят обеспечить более рациональное принятие решения высшего руководства организаций (ЛПР) в современной сложной экономической обстановке [255]. Для выбора факторов необходимо воспользоваться достоверной и публичной информацией, которая может быть легко проверена различными независимыми группами исследователей.

4.2 Разработка метода исследования динамики сертификации

4.2.1 Общая постановка задачи

Как отмечалось ранее, для обеспечения стабильного развития современных организаций в условиях жесточайшей конкуренции и наличия рисков различного происхождения, представляется целесообразным применение риск-ориентированных стандартов и внедрение ИСМ ([97], [273] – [381]). Очевидно, что для каждой конкретной организации, исходя из своего уникального контекста (ожидания потребителей, требований регуляторов, рыночной ситуации и пр.), для формирования решения ЛПР о выборе того или иного набора международных стандартов ISO, требуется достоверная информация. Отметим, что стандарты ISO в РФ в короткое время становятся национальными

стандартами ГОСТ Р[219]. Также можно отметить, что в опубликованных планах программы «Цифровая экономика» отражено, как в РФ должна снизиться доля закупаемого иностранного ПО с 50% в 2018 г. до 10% в 2024 г[220]. Также представлены важные целевые показатели: среднее время простоя государственных информационных систем в результате компьютерных атак должно снизиться с 65 часов до 1 часа в год. Однако, в этом документе нет планов создания отечественной ОС для киберфизических систем.

Предлагается следующий **новый** метод: на основании публичной статистики ISO за период 7 лет (с 2010 по 2016 г. включительно) выбираются стандарты ISO, по которым доступна аналитика в разрезе конкретных отраслей промышленности. Далее, по каждому стандарту формируется выборка по числу пяти отраслей («**лидеров**»), имеющих наибольшее количество сертификатов. Далее для каждой отрасли, хотя бы один раз включенной в выборку по любому стандарту, подсчитывается количество всех включений и, таким образом, формируется пул «лидеров». Далее для каждой отрасли («лидера») определяется корреляция по разным парам стандартов, исходя из статистики за указанный период наблюдений.

Таким образом, постановка задачи определяется следующим образом: изучение динамики сертификации различных организаций (например, по кодам отраслей EAC) по наиболее применимым международным стандартам ISO (серии 9001 – СМК, серии 27001 – СМИБ и серии 14001 – СЭМ). Достоверная, полная и объективная статистика по указанным стандартам официально публикуется ежегодно на портале ISO (доступная актуальная статистика [310]). Отметим, что в указанной статистике присутствуют данные, собранные с 1995 г., но по разным стандартам предоставляется различная аналитика. К сожалению, по стандартам ISO серии 20000 (системы менеджмента ИТ-услуг), серии 22301 (системы менеджмента непрерывности бизнеса), серии 50001 (системы энергетического менеджмента) не предоставлено детальной аналитики по

---

219 https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty

220 https://www.kommersant.ru/doc/3515334?from=four_economic

различным отраслям экономики, что повысило бы ценность проводимого исследования. Тем не менее, доступная информация [310] представляет собой регулярное, официальное и достоверное издание ISO, содержащее необходимую информацию – по 3-м основным стандартам (СМК, СЭМ и СМИБ), за достаточно длительный срок – 7 лет и содержащее достаточно точную декомпозицию по различным факторам, необходимым для постановки и проведения объективного исследования.

4.2.2 Математическая постановка задачи

Известно, что случайным процессом **X(t)** называется процесс, значение которого при любом фиксированном $\mathbf{t = t_0}$ является случайной величиной $\mathbf{X(t_0)}$. Также известно, что случайная величина $\mathbf{X(t_0)}$, в которую обращается случайный процесс при $\mathbf{t = t_0}$, называется сечением случайного процесса, соответствующим значению аргумента **t** [11]. В конкретном случае известны несколько наборов данных (результаты статистики сертификации по международным стандартам ISO), которые могут быть точно (однозначно) определены по итогам значений аргумента **t** (в конкретном примере – 7 лет). Таким образом, располагаем данными о некоторой реализации случайного процесса (в терминах [11]). Удобно рассматривать реализацию случайного процесса как множество дискретных сечений (счетное множество). Соответственно, исследуемый процесс можно считать процессом с дискретным временем и дискретным состоянием, т.к. в любой момент **t** полагаем множество его состояний конечным (счётным) [11]. Далее, известно, что для дискретной величины закон распределения может быть задан рядом распределения [11]. Для рассматриваемого случайного процесса **X(t),** известно, что сечение **X(t)** при любом фиксированном значении аргумента **t** представляет собой случайную величину, которая имеет следующий закон распределения:

$$\mathbf{F(t, x) = P \{ X (t) < x \}} \qquad (4.1)$$

Очевидно, что эта функция является функцией 2-х аргументов, и это одномерный закон распределения. В работе [11] показано, что более точные и исчерпывающие характеристики дает (в том числе для инженерных приложений)

двухмерный закон распределения, функция четырех аргументов. Для оценки независимости (или зависимости) двух случайных величин применяем формулу (4.2):

$$Corr(\eta,\gamma)=\frac{Cov(\eta,\gamma)}{\sigma(\eta)\bullet\sigma(\gamma)} \qquad (4.2)$$

где:
σ – стандартное (среднее квадратическое) отклонение,

Cov – ковариация между двумя дискретными случайными величинами.

Ковариация Cov из (4.2) определяется по формуле (4.3):

$$Cov(\eta,\gamma)=\sum_{i=1}^{\infty}\sum_{j=1}^{\infty}Pij(Xi-E(\eta))\bullet(Yj-E(\gamma)) \qquad (4.3)$$

где:
E – математическое ожидание.

Отметим, что две случайные величины называются некоррелированными, если корреляция между ними равна 0.

В работе Н. Винера отмечается, что «*основные величины, действующие на общество, не только являются статистическими, но определяются чрезвычайно короткими статистическим рядами*» ([13], стр. 75). Там же показано, что достигнуть требуемой точности весьма проблематично, т.к. все долговременные статистические ряды составляются при весьма изменчивых условиях. Соответственно, не имеет смысла анализировать длительные тренды стандартизации, тем более с учетом ввода новых требований по стандартизации – Annex SL (2012 г.).

4.2.3 Статистика сертификации ISO

Из источника [310] известна актуальная статистика сертификации по наиболее известным стандартам ISO за период 7 лет. Обработанные данные за указанный интервал по выбранным стандартам ISO для аналитических разрезов (в мире, в Европе и в РФ) представлены в таблице 4.1.

Таблица 4.1 – Статистика сертификации ISO (фрагмент)

Показатель	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
ISO 9001							
Кол-во сертификатов в мире	1 076 525,00	1 009 845,00	1 017 279,00	1 022 877,00	1 036 321,00	1 034 180,00	1 105 937,00
Динамика, %		-6,19%	0,74%	0,55%	1,31%	-0,21%	6,94%
Кол-во сертификатов в Европе	530 039,00	459 367,00	469 739,00	458 814,00	453 628,00	439 477,00	451 415,00
Динамика, %		-13,33%	2,26%	-2,33%	-1,13%	-3,12%	2,72%
Кол-во сертификатов в РФ	62 265,00	13 308,00	12 488,00	11 764,00	11 213,00	9 084,00	5 083,00
Динамика, %		-78,63%	-6,16%	-5,80%	-4,68%	-18,99%	-44,04%
ISO 14001							
Кол-во сертификатов в мире	239 880,00	243 393,00	260 852,00	273 861,00	296 736,00	319 496,00	346 147,00
Динамика, %		1,46%	7,17%	4,99%	8,35%	7,67%	8,34%
Кол-во сертификатов в Европе	103 126,00	101 177,00	111 807,00	115 764,00	119 072,00	119 754,00	120 595,00
Динамика, %		-1,89%	10,51%	3,54%	2,86%	0,57%	0,70%
Кол-во сертификатов в РФ	1 953,00	1 093,00	1 090,00	1 272,00	1 238,00	1 156,00	1 037,00
Динамика, %		-44,03%	-0,27%	16,70%	-2,67%	-6,62%	-10,29%
ISO/IEC 27001							
Кол-во сертификатов в мире	15 626,00	17 355,00	19 620,00	21 604,00	23 005,00	27 536,00	33 290,00
Динамика, %		11,06%	13,05%	10,11%	6,48%	19,70%	20,90%
Кол-во сертификатов в Европе	4 800,00	5 289,00	6 379,00	7 952,00	8 663,00	10 446,00	12 532,00
Динамика, %		10,19%	20,61%	24,66%	8,94%	20,58%	19,97%
Кол-во сертификатов в РФ	72,00	31,00	27,00	48,00	43,00	55,00	62,00
Динамика, %		-56,94%	-12,90%	77,78%	-10,42%	27,91%	12,73%
ISO 50001							
Кол-во сертификатов в мире		459,00	2 236,00	4 826,00	6 765,00	11 985,00	20 216,00
Динамика, %			387,15%	115,83%	40,18%	77,16%	68,68%
Кол-во сертификатов в Европе		364,00	1 919,00	3 993,00	5 526,00	10 152,00	17 102,00
Динамика, %			427,20%	108,08%	38,39%	83,71%	68,46%
Кол-во сертификатов в РФ		1	8	25	81	118	174
Динамика, %			700,00%	212,50%	224,00%	45,68%	47,46%

Обработанные данные по динамике сертификации по выбранным стандартам ISO для аналитических разрезов (в мире, в Европе и в РФ) представлены в таблице 4.2.

Таблица 4.2 – Динамика сертификации по выбранным стандартам ISO

Стандарт	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
В мире							
ISO 9001	1	-6,19%	0,74%	0,55%	1,31%	-0,21%	6,94%
ISO 14001	1	1,46%	7,17%	4,99%	8,35%	7,67%	8,34%
ISO 27001	1	11,06%	13,05%	10,11%	6,48%	19,70%	20,90%
ISO 50001	1		387,15%	115,83%	40,18%	77,16%	68,68%
В Европе							
ISO 9001	1	-13,33%	2,26%	-2,33%	-1,13%	-3,12%	2,72%
ISO 14001	1	-1,89%	10,51%	3,54%	2,86%	0,57%	0,70%
ISO 27001	1	10,19%	20,61%	24,66%	8,94%	20,58%	19,97%
ISO 50001			427,20%	108,08%	38,39%	83,71%	68,46%
В РФ							
ISO 9001	1	-78,63%	-6,16%	-5,80%	-4,68%	-18,99%	-44,04%
ISO 14001	1	-44,03%	-0,27%	16,70%	-2,67%	-6,62%	-10,29%
ISO 27001	1	-56,94%	-12,90%	77,78%	-10,42%	27,91%	12,73%
ISO 50001	1		700,00%	212,50%	224,00%	45,68%	47,46%

Представляется полезным получить на портале ISO [310] по выбранным стандартам также и графический результат (см. рисунки 4.1 – 4.3)/

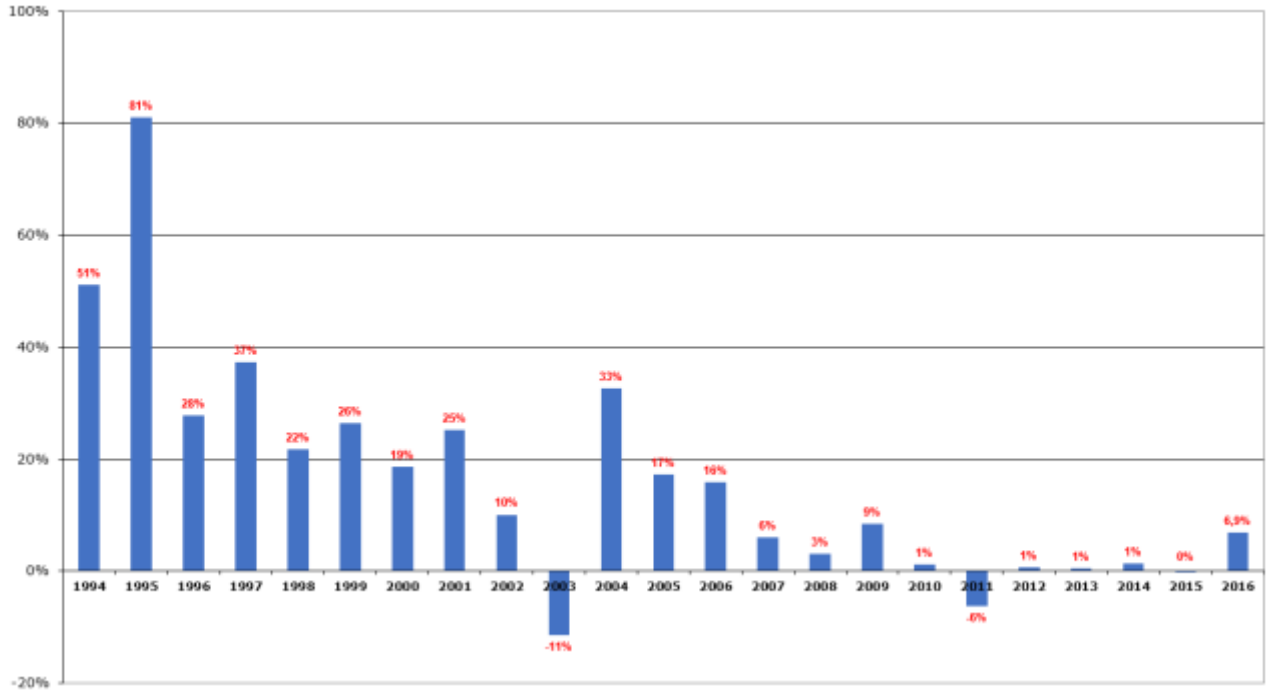


Рисунок 4.1 – Статистика сертификации по стандарту ISO 9001

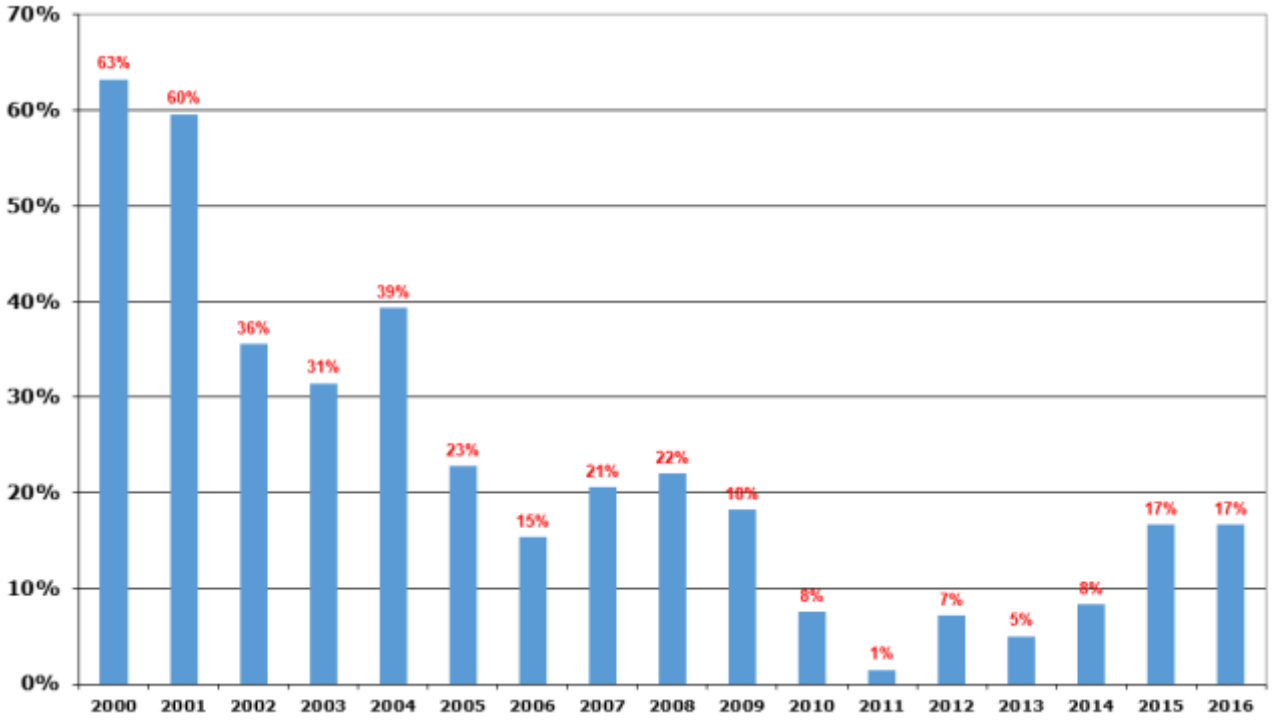


Рисунок 4.2 – Статистика сертификации по стандарту ISO 14001

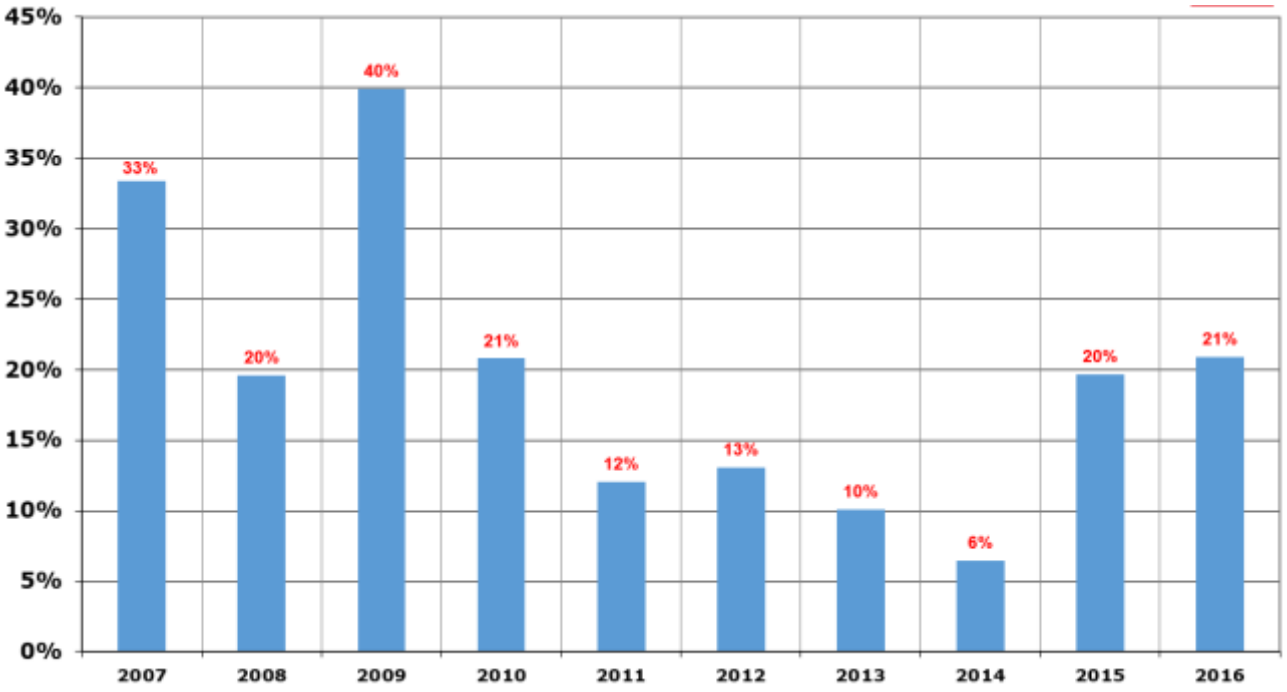


Рисунок 4.3 – Статистика сертификации по стандарту ISO/IEC 27001

Для поставленной цели изучения конкретного влияния сертификации СМИБ различных организаций сопоставим динамику изменения роста количества сертификатов по стандартам ISO серии 9001, 14001 и 27001 (на основании данных, представленных в таблице 4.1) в период всех наблюдений для

организаций в РФ, в Европе и в целом в мире. Результаты представлены на рисунках 4.4 – 4.6.

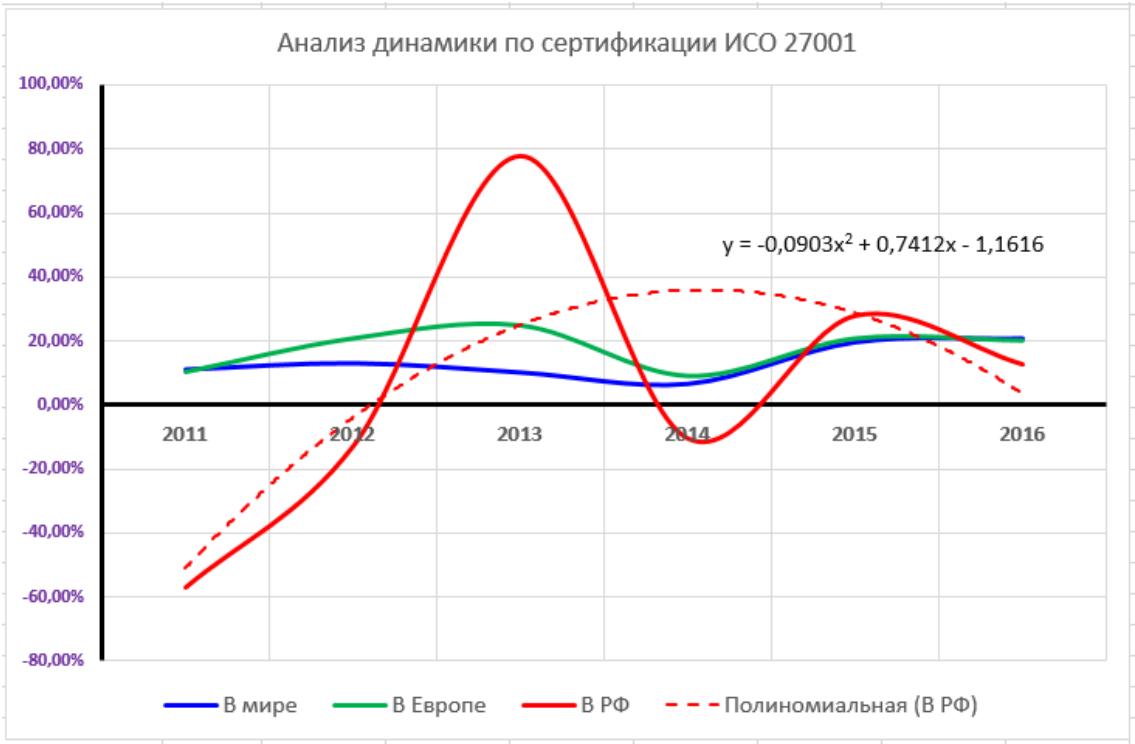


Рисунок 4.4 – Анализ динамики сертификации по стандарту ISO 27001

Отметим, что «пики» динамики в данных статистики по сертификации стандарту ISO 27001 значительно отличаются от значений по иным стандартам. Исключение составляет стандарт ISO 50001, поскольку для нового стандарта в первые годы характерна «взрывная» динамика роста.

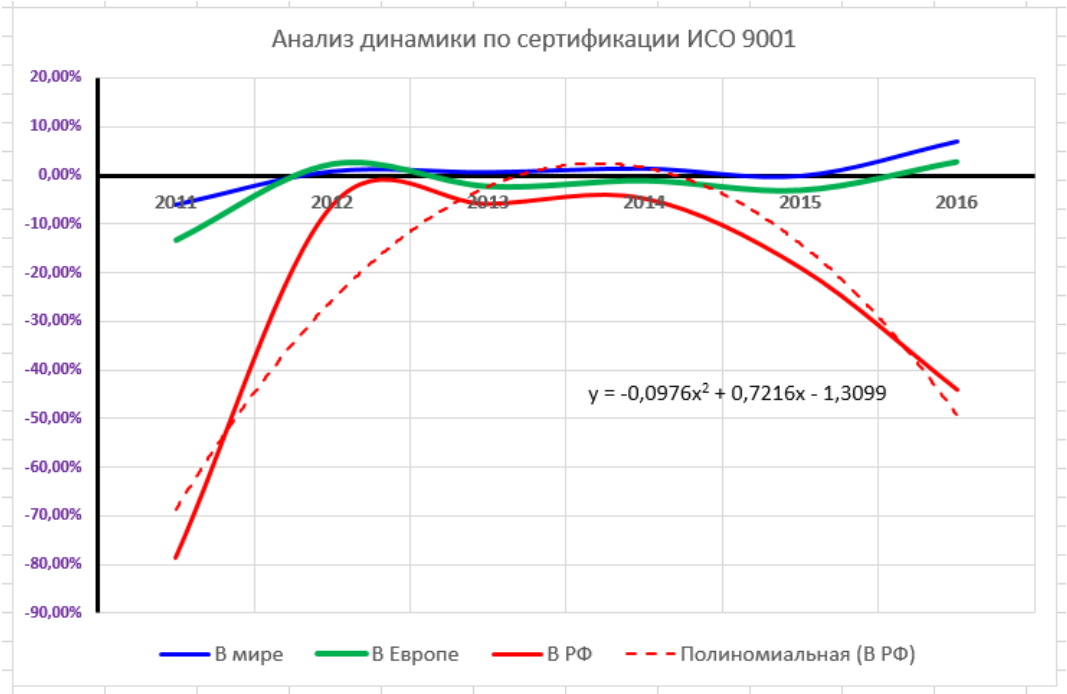


Рисунок 4.5 – Анализ динамики сертификации по стандарту ISO 9001

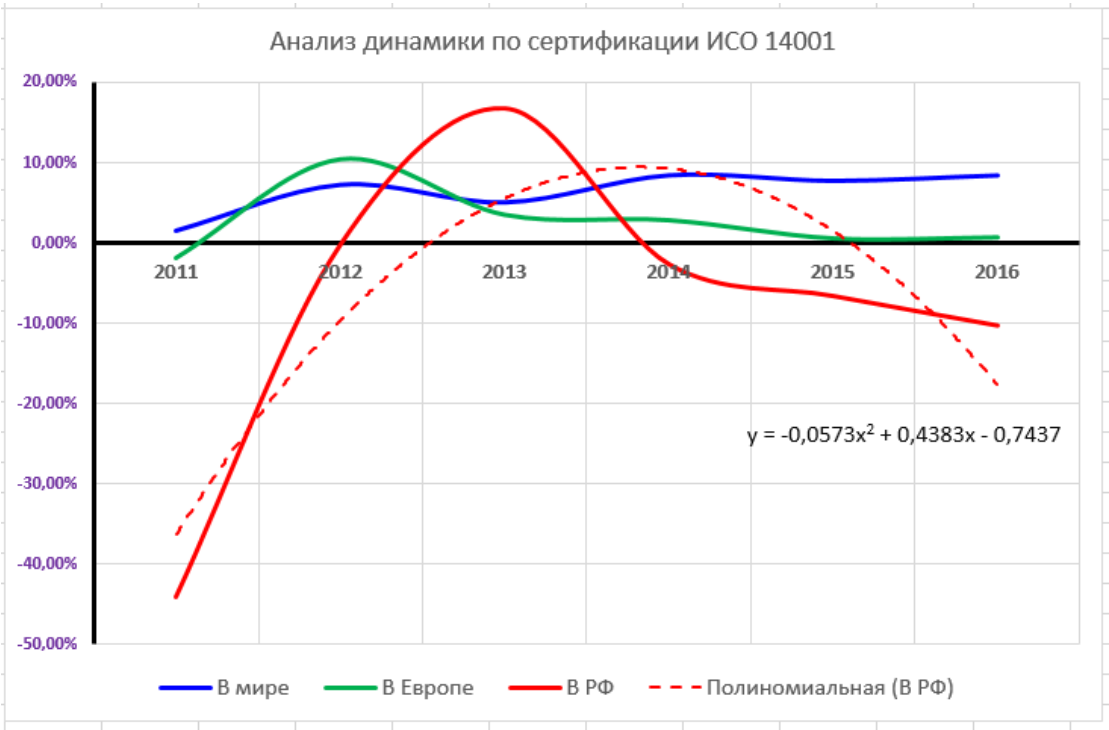


Рисунок 4.6 – Анализ динамики сертификации по стандарту ISO 14001

Для каждого стандарта выведены функции, которые описывают динамику изменения роста количества сертификатов. Эти функции будут изучены далее для оценки коэффициентов корреляции всех рассматриваемых стандартов.

4.2.4 Формирование статистики сертификации

На основании данных сертификации ISO [310] необходимо сформировать достоверные, объективные и точные данные для расчета статистики сертификации по «лидерам». Результаты обработки доступных сертификационных данных по стандартам ISO серии 9001, 14001 и 27001 представлены в таблицах 4.3 – 4.5 соответственно.

Таблица 4.3 – Статистика сертификации ISO 9001 (фрагмент)

EA* Code Nos.	ISO 9001 BY INDUSTRIAL SECTOR	2010	2011	2012	2013	2014	2015	2016
1	Agriculture, fishing and forestry	4595	4683	4883	4953	4701	4236	4474
2	Mining and quarrying	2955	2766	4039	3479	3992	3535	3759
3	Food products, beverages and tobacco	33193	28434	33705	32519	31182	26602	31469
4	Textiles and textile products	12223	13319	15176	14461	13467	12081	14640
9	Printing companies	7624	8341	9161	9223	8769	7500	8287
10	Manufacture of coke & refined petroleum products	1792	1626	1669	1955	1742	1445	3480
11	Nuclear fuel	330	465	321	433	168	569	1002
12	Chemicals, chemical products & fibres	29557	30278	33583	33610	33432	29744	31993
13	Pharmaceuticals	3222	3766	3840	6710	5200	3532	3090
14	Rubber and plastic products	39425	40854	44769	45204	45674	41101	48010
15	Non-metallic mineral products	11480	11305	12392	12367	11380	10441	10634
16	Concrete, cement, lime, plaster, etc.	10656	11567	13065	12250	11979	11234	21872
17	Basic metal & fabricated metal products	95375	101848	115731	116602	118652	104652	116457
18	Machinery and equipment	58685	58427	63723	63497	64817	56413	62118
19	Electrical and optical equipment	81893	79237	85969	87797	86728	75260	88482
20	Shipbuilding	2783	2396	2952	2131	2738	1930	2636
27	Water supply	2602	1535	2658	2318	2341	1948	2777
28	Construction	82262	83864	108396	80920	76915	67354	87605
29	Wholesale & retail trade; repairs of motor vehicles, motorcycles & personal & household goods	53051	55961	70082	73167	73756	66975	79492
30	Hotels and restaurants	3499	3664	5496	5021	5045	4340	5398
31	Transport, storage and communication	22804	24846	31679	31490	30845	27053	30418
32	Financial intermediation, real estate, rental	11057	11423	16445	16198	16469	15621	16532
33	Information technology	18998	20467	24690	27229	28995	29162	35268
34	Engineering Services	32726	31086	38160	38659	38694	36346	38396
35	Other Services	41615	40303	54572	55602	57860	50696	54506
39	Other social services	7620	6987	10601	10240	11579	10017	10711

Таблица 4.4 – Статистика сертификации ISO 14001 (фрагмент)

EA* Code Nos.	ISO 14001 BY INDUSTRIAL SECTOR	2010	2011	2012	2013	2014	2015	2016
1	Agriculture, fishing	1831	1748	1269	2467	2215	2408	2149
2	Mining and quarrying	1745	1772	1996	2532	2520	2548	2674
3	Food products, beverages and tobacco	5438	5848	5878	6890	7219	6842	6693
4	Textiles and textile products	3048	3553	2132	4163	4020	4274	4606
9	Printing companies	2587	2643	2188	3064	3024	3045	2966
10	Manufacture of coke & refined petroleum products	690	664	823	768	783	700	711
11	Nuclear fuel	159	96	82	127	151	148	115
12	Chemicals, chemical products & fibres	9584	9860	7940	11554	11890	11978	12277
13	Pharmaceuticals	1183	1067	946	1237	1341	1146	1195
14	Rubber and plastic products	10362	10545	8950	12957	13410	14007	14741
15	Non-metallic mineral products	2515	2727	2202	3447	3621	3524	3538
16	Concrete, cement, lime, plaster, etc.	2476	2757	1911	3480	3718	3810	15814
17	Basic metal & fabricated metal products	17976	19231	17100	24791	26050	26494	27374
18	Machinery and equipment	10225	10081	8232	12892	13980	15209	16561
19	Electrical and optical equipment	18972	18001	15008	22663	23768	25690	26728
20	Shipbuilding	406	519	540	465	558	453	618
28	Construction	29411	34155	22317	40430	43999	46910	49837
29	Wholesale & retail trade; repairs of motor vehicles, motorcycles & personal & household goods	10377	11753	10035	15516	16878	19396	22554
30	Hotels and restaurants	1420	1344	1666	1511	1873	1772	1786
31	Transport, storage and communication	5261	5849	7137	8666	8729	8607	8961
32	Financial intermediation, real estate, rental	2372	2467	1850	3351	3357	4411	5244
33	Information technology	1871	2008	1503	3064	3858	5395	7237
34	Engineering Services	7467	8189	6042	11850	12551	14438	15389
35	Other Services	6919	7137	8243	9840	10761	11174	12211
39	Other social services	4171	5475	6355	6344	7679	6799	6905

Таблица 4.5 – Статистика сертификации ISO 27001 (фрагмент)

EA* Code Nos.	ISO/IEC 27001 BY INDUSTRIAL SECTOR	2010	2011	2012	2013	2014	2015	2016
1	Agriculture, fishing	8	14	13	13	10	9	5
2	Mining and quarrying	2	12	31	34	25	8	9
3	Food products, beverages and tobacco	6	8	10	24	10	12	61
4	Textiles and textile products	3	2	12	10	4	10	132
5	Leather and leather products	2	5	1	2	0	1	1
6	Wood and wood products	3	5	4	4	1	12	12
7	Pulp, paper and paper products	4	7	13	17	15	9	10
8	Publishing companies	11	20	18	22	20	11	10
9	Printing companies	78	101	121	148	126	143	130
10	Manufacture of coke & refined petroleum products	3	5	4	14	10	4	3
11	Nuclear fuel	0	1	1	2	0	0	0
12	Chemicals, chemical products & fibres	9	9	11	24	12	10	18
13	Pharmaceuticals	6	3	0	3	6	6	9
14	Rubber and plastic products	15	16	16	36	14	16	32
15	Non-metallic mineral products	16	8	0	5	13	3	7
16	Concrete, cement, lime, plaster, etc.	6	14	27	25	26	13	17
17	Basic metal & fabricated metal products	25	28	36	50	42	37	51
18	Machinery and equipment	31	36	43	52	66	51	68
19	Electrical and optical equipment	221	280	342	289	287	296	311
20	Shipbuilding	3	3	4	8	4	1	2
28	Construction	266	350	409	396	454	186	216
29	Wholesale & retail trade; repairs of motor vehicles, motorcycles & personal & household goods	164	214	215	224	206	198	202
30	Hotels and restaurants	10	32	4	5	2	6	7
31	Transport, storage and communication	184	241	288	322	327	301	401
32	Financial intermediation, real estate, rental	185	113	138	169	187	197	250
33	Information technology	3217	3588	4558	5059	4933	5573	6578
34	Engineering Services	122	126	189	211	217	201	245
35	Other Services	579	564	755	849	867	959	1432
39	Other social services	54	75	98	106	102	125	163

Во всех трех выборках (см. таблицы 4.3 – 4.5) серым фоном выделена «пятерка» лидеров, имеющих 5 лучших результатов по единой численной метрике (наибольшее абсолютное количество сертификатов) по каждому из представленных в выборке стандартов. Результаты определения «лидеров» по сертификации ISO для выбранных стандартов представлены в таблице 4.6.

Таблица 4.6 – Результаты определения «лидеров» по сертификации ISO

Стандарт	EAC	Наименование отрасли (Industrial sector)	Ранг
9001	17	Basic metal & fabricated metal products	2
	19	Electrical and optical equipment	1
	28	Construction	1
	29	Wholesale & retail trade, repairs of motor vehicles	2
	18	Machinery and equipment	3
14001	28	Construction	1
	17	Basic metal & fabricated metal products	2
	19	Electrical and optical equipment	1
	29	Wholesale & retail trade, repairs of motor vehicles	2
	14	Rubber and plastic products	3
27001	33	Information technology	3
	35	Other Services	3
	28	Construction	1
	31	Transport, storage and communication	3
	19	Electrical and optical equipment	1

По выборке (см. таблицу 4.6) наблюдаются следующие зависимости:

1. Две отрасли «*Electrical and optical equipment*» и «*Construction*» представлены трижды во всех 3-х выборках в «пятерке» лидеров – будем называть их «**лидером 1-го ранга»;**
2. Две отрасли «*Basic metal & fabricated metal products*» и «*Wholesale & retail trade; repairs of motor vehicles, motorcycles & household goods*» представлены дважды во всех 3-х выборках в «пятерке» лидеров – будем называть их «**лидером 2-го ранга»**;
3. Остальные отрасли представлены по одному разу в «пятерке» лидеров – будем называть их «**лидером 3-го ранга»**.

4.2.5 Расчет динамики сертификации

На основании данных предыдущего подраздела определим динамику сертификации (т.е. изменение по каждой отрасли по каждому стандарту с

установленной ежегодной периодичностью). Помимо абсолютных величин, рассматриваемых в таблицах 4.3 – 4.5 для оценки динамики различных стандартов ISO применительно к выбранным «лидерам», представляется необходимым и целесообразным проанализировать относительные изменения (в процентах), по отношению к предыдущему значению, т.е. получить важную количественную оценку динамики процесса.

Результаты расчета динамики сертификации организаций по отраслям представлены в таблице 4.7.

4.2.6 Порядок определения коэффициентов зависимости (корреляции)

На основании полученных ранее данных обработанной статистики сертификации ISO по «лидерам» (см. таблицу 4.7) возможно определение коэффициентов зависимости (корреляции). На основании формулы (4.2) определим корреляцию для различных выборок (по трем стандартам ISO серии 9001, 14001 и 27001 соответственно) по всему установленному периоду наблюдений.

Таблица 4.7 – Результаты расчета динамики сертификации ISO (по рангам)

Код EAC	Год	ISO 9001		ISO 14001		ISO/IEC 27001	
Лидер 1-го ранга							
19	2016	88 482	17,57%	26 728	4,04%	311	5,07%
	2015	75 260	-13,22%	25 690	8,09%	296	3,14%
	2014	86 728	-1,22%	23 768	4,88%	287	-0,69%
	2013	87 797	2,13%	22 663	51,01%	289	-15,50%
	2012	85 969	8,50%	15 008	-16,63%	342	22,14%
	2011	79 237	-3,24%	18 001	-5,12%	280	26,70%
	2010	81 893		18 972		221	
28	2016	87 605	30,07%	49 837	6,24%	216	16,13%
	2015	67 354	-12,43%	46 910	6,62%	186	-59,03%
	2014	76 915	-4,95%	43 999	8,83%	454	14,65%
	2013	80 920	-25,35%	40 430	81,16%	396	-3,18%
	2012	108 396	29,25%	22 317	-34,66%	409	16,86%
	2011	83 864	1,95%	34 155	16,13%	350	31,58%
	2010	82 262		29 411		266	

Лидер 2-го ранга							
17	2016	116 457	11,28%	27 374	3,32%	51	37,84%
	2015	104 652	-11,80%	26 494	1,70%	37	-11,90%
	2014	118 652	1,76%	26 050	5,08%	42	-16,00%
	2013	116 602	0,75%	24 791	44,98%	50	38,89%
	2012	115 731	13,63%	17 100	-11,08%	36	28,57%
	2011	101 848	6,79%	19 231	6,98%	28	12,00%
	2010	95 375		17 976		25	
29	2016	79 492	18,69%	22 554	16,28%	202	2,02%
	2015	66 975	-9,19%	19 396	14,92%	198	-3,88%
	2014	73 756	0,81%	16 878	8,78%	206	-8,04%
	2013	73 167	4,40%	15 516	54,62%	224	4,19%
	2012	70 082	25,23%	10 035	-14,62%	215	0,47%
	2011	55 961	5,49%	11 753	13,26%	214	30,49%
	2010	53 051		10 377		164	
Лидер 3-го ранга							
18	2016	62 118	10,11%	16 561	8,89%	68	33,33%
	2015	56 413	-12,97%	15 209	8,79%	51	-22,73%
	2014	64 817	2,08%	13 980	8,44%	66	26,92%
	2013	63 497	-0,35%	12 892	56,61%	52	20,93%
	2012	63 723	9,06%	8 232	-18,34%	43	19,44%
	2011	58 427	-0,44%	10 081	-1,41%	36	16,13%
	2010	58 685		10 225		31	
14	2016	48 010	16,81%	14 741	5,24%	32	100,00%
	2015	41 101	-10,01%	14 007	4,45%	16	14,29%
	2014	45 674	1,04%	13 410	3,50%	14	-61,11%
	2013	45 204	0,97%	12 957	44,77%	36	125,00%
	2012	44 769	9,58%	8 950	-15,13%	16	0,00%
	2011	40 854	3,62%	10 545	1,77%	16	6,67%
	2010	39 425		10 362		15	
33	2016	35 268	20,94%	7 237	34,14%	6578	18,03%
	2015	29 162	0,58%	5 395	39,84%	5573	12,97%
	2014	28 995	6,49%	3 858	25,91%	4933	-2,49%
	2013	27 229	10,28%	3 064	103,86%	5059	10,99%
	2012	24 690	20,63%	1 503	-25,15%	4558	27,03%
	2011	20 467	7,73%	2 008	7,32%	3588	11,53%
	2010	18 998		1 871		3217	

35	2016	54 506	7,52%	12 211	9,28%	1432	49,32%
	2015	50 696	-12,38%	11 174	3,84%	959	10,61%
	2014	57 860	4,06%	10 761	9,36%	867	2,12%
	2013	55 602	1,89%	9 840	19,37%	849	12,45%
	2012	54 572	35,40%	8 243	15,50%	755	33,87%
	2011	40 303	-3,15%	7 137	3,15%	564	-2,59%
	2010	41 615		6 919		579	
31	2016	30 418	12,44%	8 961	4,11%	401	33,22%
	2015	27 053	-12,29%	8 607	-1,40%	301	-7,95%
	2014	30 845	-2,05%	8 729	0,73%	327	1,55%
	2013	31 490	-0,60%	8 666	21,42%	322	11,81%
	2012	31 679	27,50%	7 137	22,02%	288	19,50%
	2011	24 846	8,95%	5 849	11,18%	241	30,98%
	2010	22 804		5 261		184	

Результаты определения коэффициентов корреляции по «лидерам» различных рангов получены в программной реализации статистических функций Excel и представлены в таблице 4.8.

Таблица 4.8 – Определение коэффициентов корреляции по рангам

		Коэффициенты корреляции		
Код ЕАС	**Ранг**	**9001 – 14001**	**14001 – 27001**	**9001 – 27001**
19	1	-0,115	-0,878	0,056
28	1	-0,769	-0,121	0,477
17	2	-0,270	0,338	0,633
29	2	-0,422	0,091	0,087
18	3	-0,261	0,058	0,888
14	3	-0,236	0,672	0,301
33	3	-0,318	-0,389	0,664
35	3	0,580	0,329	0,552
31	3	0,608	0,377	0,720

На основании полученных данных из таблицы 4.8 определим:

1. Для «**лидеров 3-го ранга**» только для пары 9001-27001 наблюдается положительная корреляция с низким (для отраслей ЕАС 14 и 35), средним (для отраслей ЕАС 31 и 35) и высоким (для отрасли ЕАС 18) признаком по шкале Чеддока соответственно. Этот факт можно объяснить тем обстоятельством, что, как правило, стандарт ISO/IEC 27001 внедряется

вторым после ISO 9001. Остальные пары сравнения дают различную по направленности корреляцию.

2. Для «**лидеров 2-го ранга**» для пары 9001-27001 наблюдается положительная корреляция с низким (для отрасли EAC 29) и средним (для отрасли EAC 17) признаком по шкале Чеддока соответственно. Этот факт также можно объяснить тем обстоятельством, что, как правило, стандарт ISO/IEC 27001 внедряется вторым после ISO 9001. Для пары 14001-27001 наблюдается положительная корреляция с низким (для всех отраслей EAC) признаком по шкале Чеддока соответственно. Для пары 9001-14001 наблюдается различная по направленности корреляция.
3. Для «**лидеров 1-го ранга**» только для пары 9001-27001 наблюдается положительная корреляция с низким (для отрасли EAC 19) и средним (для отрасли EAC 28) признаком по шкале Чеддока соответственно. Этот факт можно объяснить тем обстоятельством, что, как правило, стандарт ISO/IEC 27001 внедряется вторым после ISO 9001. Остальные пары сравнения дают различную по направленности корреляцию. Однако вызывает определенный интерес для дальнейшего изучения высокий признак по шкале Чеддока во всех парах, где есть ISO 14001.
4. Для пары ISO 9001 – 27001 для всех «лидеров» в целом показана без исключения только положительная корреляция и важно, что успех сертификации по указанной паре стандартов мало зависит от специфики конкретных отраслей (т.е. объективно доказано, что требованиям ИБ привержены не только лишь «специфические» ИТ-компании).

4.2.7 Определение коэффициентов корреляции для регионов

На основании полученных новых данных обработанной статистики по динамике сертификации ISO (см. таблицу 4.1) возможно определение коэффициентов зависимости (корреляции) для трех исследуемых стандартов (ISO серии 9001, 14001, 27001) для трех аналитических разрезов по географии регионов: в РФ, Европе и мире (см. таблицу 4.9).

Таблица 4.9 – Статистика динамики сертификации по регионам (фрагмент)

Регион	Стандарт	Год					
		2011	2012	2013	2014	2015	2016
РФ	ISO 9001	-78,63%	-6,16%	-5,80%	-4,68%	-18,99%	-44,04%
	ISO 14001	-44,03%	-0,27%	16,70%	-2,67%	-6,62%	-10,29%
	ISO 27001	-56,94%	-12,90%	77,78%	-10,42%	27,91%	12,73%
Европа	ISO 9001	-13,33%	2,26%	-2,33%	-1,13%	-3,12%	2,72%
	ISO 14001	-1,89%	10,51%	3,54%	2,86%	0,57%	0,70%
	ISO 27001	10,19%	20,61%	24,66%	8,94%	20,58%	19,97%
Мир	ISO 9001	-6,19%	0,74%	0,55%	1,31%	-0,21%	6,94%
	ISO 14001	1,46%	7,17%	4,99%	8,35%	7,67%	8,34%
	ISO 27001	11,06%	13,05%	10,11%	6,48%	19,70%	20,90%

Представляет интерес графическое представление полученных новых данных (см. таблицу 4.9) обработанной статистики по динамике сертификации в регионах, дополнительно указаны значения для ИСО 27001 (см. рисунок 4.7).

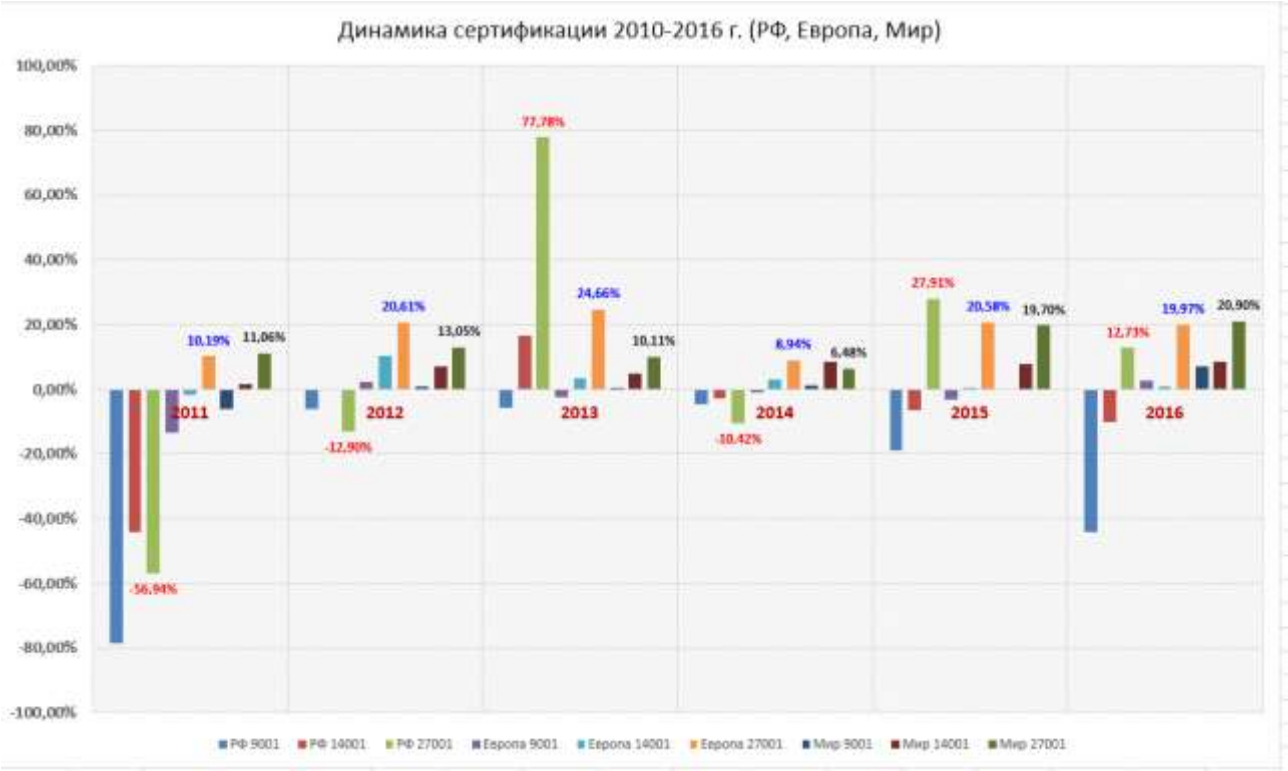


Рисунок 4.7 – Анализ статистики по динамике сертификации по стандартам ISO

На основании данных из таблицы 4.9 определим коэффициенты корреляции для трех исследуемых стандартов (ISO серии 9001, 14001, 27001) для трех аналитических разрезов: в РФ, Европе и мире; результаты представлены в таблице 4.10

Таблица 4.10 – Определение коэффициентов корреляции по регионам

Аналитический разрез	Коэффициенты корреляции		
	9001-14001	14001-27001	9001-27001
Мир	0,825	0,329	0,453
Европа	0,628	0,375	0,509
РФ	0,914	0,843	0,606

Полученные результаты проанализируем на графике (см. рисунок 4.8).

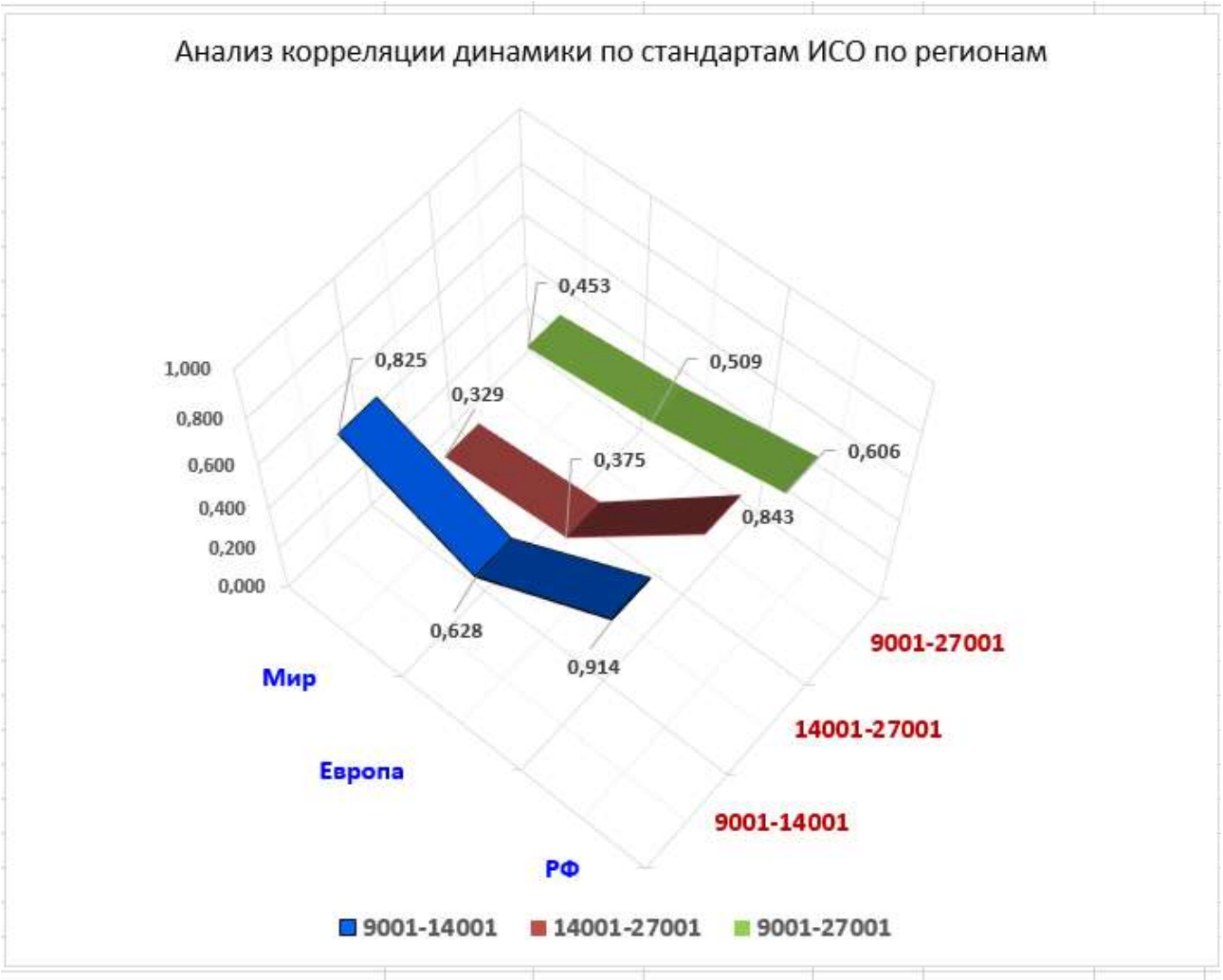


Рисунок 4.8 – Анализ коэффициентов корреляции по стандартам ISO

Отметим следующие особенности:

1. Коэффициенты корреляции для всех трех исследуемых стандартов (ISO серии 9001, 14001, 27001) в РФ показали наибольшие абсолютные значения, что можно обосновать постоянным ростом динамики стандартизации и сертификации ИСМ в РФ в рассматриваемый период наблюдений и повышением внимания к новым стандартам. Также можно сделать

предположение, что все три исследуемых стандарта востребованы в РФ для различных отраслей.

2. Коэффициенты корреляции для всех трех исследуемых стандартов (ISO серии 9001, 14001, 27001) в Европе показали среднюю степень корреляции (по шкале Чеддока), что можно обосновать сохраняющимся умеренным ростом стандартизации в Европе в рассматриваемый период наблюдений.
3. Для всех рассматриваемых пар корреляции с «участием» стандарта ISO 27001 (9001-27001 и 14001-27001) наименьшие абсолютные значения показали данные по мировому совокупному аналитическому разрезу. Этот факт представляется вполне объективным – в мировом аналитическом разрезе анализируется вся совокупность данных.

4.2.8 Анализ оценки динамики сертификации

На основании рассчитанных коэффициентов корреляции для выбранных стандартов ISO (см. таблицу 4.10) отметим закономерность: динамика роста «лидеров» по основным стандартам ISO весьма различна для «лидеров» разных рангов. На примере сечения 2014/2013 гг. (см. рисунок 4.9) показана динамика стандартов: для «лидеров 1-го ранга» динамика ISO серии 9001 и 27001 отрицательна, а для иных лидеров – существенная и положительная.

Рисунок 4.9 – Анализ динамики лидеров по стандартам ISO (сечение 2014 г.)

Кроме того, динамика роста сертификатов в РФ по заданному интервалу по различным стандартам (см. таблицу 4.1) имеет различную временную зависимость:

— по стандартам ISO серии 9001 и 14001 «пики» динамики отстают от мировых и европейских на год;
— по стандарту ISO серии 13485 «пик» динамики опережает мировые и европейские на год;
— по стандартам ISO серии 27001 и 50001 «пики» динамики соответствуют мировым и европейским.

4.3 Практические подходы к выбору стандартов для управления ИБ

4.3.1 Общие положения

Рассмотрим в качестве практического приложения пример обеспечения ИБ для электронных сервисов (ЭС). Этот вид услуг весьма распространен в мире, в Европе и в России, соответственно, может быть принят как достоверный пример, по которому представлена обобщенная аналитика. Решение проблемы обеспечения ИБ для ЭС, в том числе, заключается в получении формализованной оценки соответствия принятых мер (средств) (*controls,* в терминах [317]) требованиям по ИБ, которая будет соответствовать критериям оценки, признанной всеми участниками международного (регионального) информационного взаимодействия.

Проведение независимой оценки может быть возложено на уполномоченных представителей всех участников, например – государств-членов таможенного союза (ТС). С целью консолидации национальных требований Российской Федерации, Республики Беларусь и Республики Казахстан по защите информации, необходимо разработать единый документ, содержащий требования к мерам (средствам) обеспечения ИБ, которые могут быть независимо подтверждены посредством независимой оценки конкретных объектов (*asset,* в терминах [317]) в рамках СМИБ. Оценка соответствия СМИБ проводится в соответствии с требованиями международных стандартов ISO

серии 27001 [317] – [320], принятых на национальном уровне в каждом из государств-членов ТС, например:

— ГОСТ Р ИСО/МЭК 27001-2006 – в Российской Федерации,

— СТБ ISO/IEC 27001-2011 – в Республике Беларусь,

— СТ РК ИСО/МЭК 27001-2008 – в Республике Казахстан.

Представляется актуальным вопрос о необходимости разработки метода и регламента оценки соответствия данным требованиям, обеспечивающих открытый и не противоречащий требованиям национальной нормативной документации государств-членов ТС, приведенных выше. Соответственно, формируется предложение о рассмотрении ОО информационной инфраструктуры ЭС как СМИБ и, соответственно, сертификация данного объекта согласно требованиям национальных стандартов ISO серии 27001, принятых в каждом из государств-членов ТС. При этом решается сложная задача обеспечения международного доверия к уровню обеспечения ИБ на основании объективных и независимых свидетельств в рамках результата аудита. Оценка СМИБ проводится по единому международному признанному стандарту, посредством независимого (сертификационного) аудита 3-й стороной со стороны национальных органов по сертификации, находящихся под строгим контролем IAF (Международного аккредитационного форума).

4.3.2 Требования к реализации электронных сервисов

Рассмотрим общие требования к ЭС, которые должны быть приняты во внимание при реализации и успешной сертификации СМИБ ([162] – [170]). В состав современных ЭС входят технологии, предназначенные для обеспечения деятельности по проверке электронных подписей (ЭП) для электронных документов (ЭД), поддержания инфраструктуры открытых ключей (ИОК) в фиксированный момент времени в отношении респондентов (отправителя или получателя). Реализация ЭС осуществляется провайдерами, которым доверяют все стороны информационного обмена (доверенная третья сторона, ДТС). Функциональная схема работы сервисов ДТС показана на рисунке 4.10.

Спецификации, применяемые при обеспечении ИБ для ЭС определяются конкретным составом ПО и технических решений, используемых в конкретной национальной реализации [26] – [28]. Представляется важным при обеспечении ИБ для ЭС обеспечить всю «вертикаль» доверия ИОК, и особое внимание следует уделять уровню доверия к УЦ.

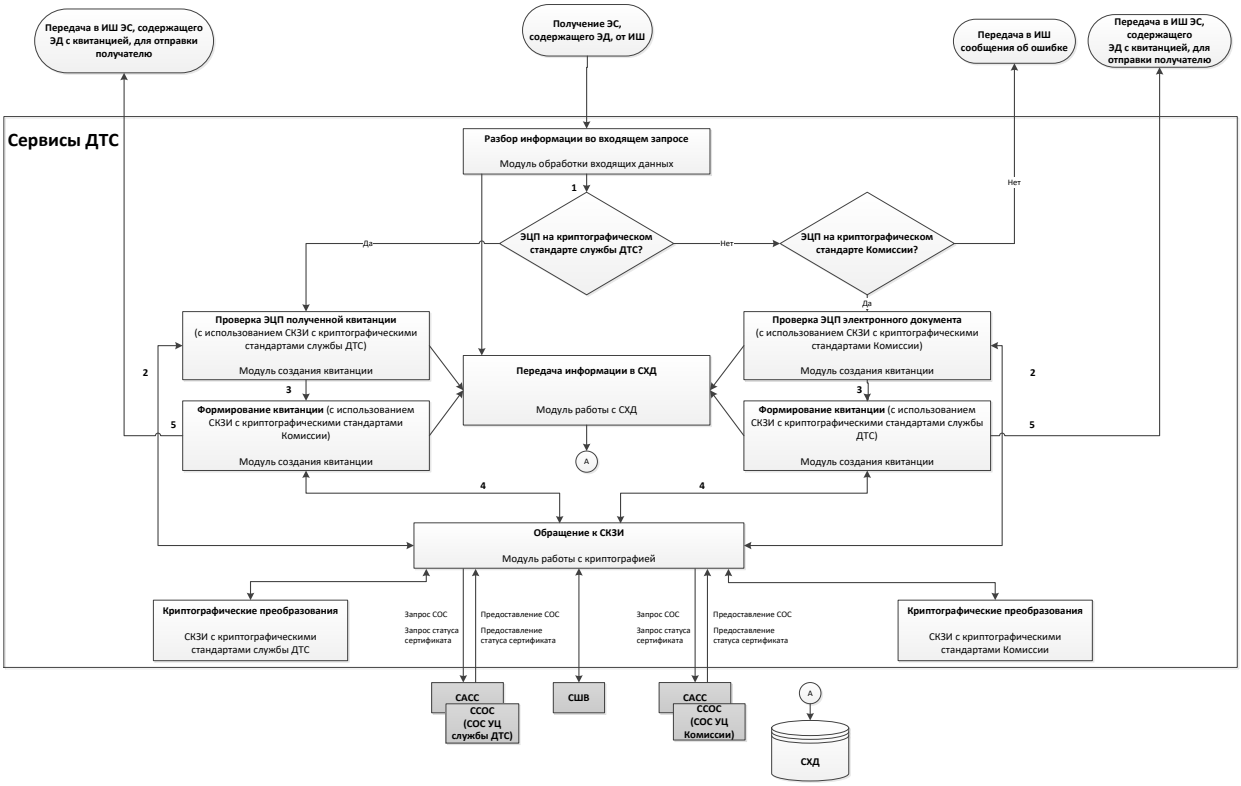


Рисунок 4.10 – Функциональная схема работы сервисов ДТС

В частности, в связи с вступлением в силу в Нидерландах нового закона, позволяющего спецслужбам перехватывать трафик, возможно исключение центра сертификации (Staat der Nederlanden) из списка доверенных[221]. Закон 2018 г. об информации и службах безопасности Нидерландов (Wet op de inlichtingen - en veiligheidsdiensten) предоставил спецслужбам (Algemene Inlichtingen en Veiligheidsdienst, Службе общей разведки и безопасности Нидерландов) полномочия по перехвату трафика. В частности, норма закона такова: «*статья 45.1.b разрешает использование «ложных ключей» в сторонних системах для получения доступа к данным*», соответственно, предоставляемые сертификаты не могут более считаться безопасными[222].

221 http://www.securitylab.ru/news/489398.php

222 https://bugzilla.mozilla.org/show_bug.cgi?id=1408647

4.3.3 Требования к подготовке инфраструктуры ЭС к сертификации ISO 27001

Известно, что требования к СМИБ установлены рядом стандартов ISO серии 27001, в частности, требования к реализации мер (средств) обеспечения ИБ определяются стандартом [317], требования к менеджменту рисков ИБ определяются стандартом [319], требования к измерениям ИБ определяются стандартом [318]. Вместе с тем, представляется целесообразным сопоставить требования, предъявляемые к объекту ЭС, как к объекту информатизации (ОИ) в соответствии с национальными требованиями [153], [40]. Дополнительные термины, касающиеся методических аспектов создания, оценки и реализации ОИ приводятся в [38]. Рассмотрим требования, предъявляемые к ОИ в соответствии с нормативными документами [211] и [153], которые удобно объединить по основным группам, и сопоставим их с аналогичными требованиями, предъявляемыми к СМИБ [317] (см. таблицу 4.11):

Таблица 4.11 – Обобщенные требования к объекту информатизации (фрагмент)

№ п.п.	Группа требований	Пункт требований «Положение по аттестации ОИ»	Пункт требований ISO 27001
1.	Персонал	3.7.1	7.2; 7.3; 7.4
2.	Средства защиты информации	1.5; 1.8; 3.4; 3.7	A.5 – A.18
3.	Документация	1.8; 2.6; 3.1; 3.5; 3.7; 4.1	7.5
4.	Состав ПО и ТС	1.7; 1.8; 3.4; 3.7; 3.8; 3.10; 4.1	A.5 – A.18

В указанных документах [211] и [153] установлена применимость международных схем и СрЗИ при выполнении процессов сертификации в РФ. В целях сопоставления требований различных нормативных документов отметим, что в «Положении» отражено: «*По согласованию с федеральным органом по сертификации могут быть использованы и другие схемы сертификации, включая применяемые в международной практике»* (п. 1.7 [211]) и «*Федеральный орган по сертификации средств защиты информации ... осуществляет взаимодействие с соответствующими уполномоченными органами других стран и международных организаций по вопросам*

сертификации, принимает решение о признании международных и зарубежных сертификатов» (п. 2.2 [211]).

4.3.4 Преимущества и недостатки сертификации ЭС по требованиям ISO 27001

Описание преимуществ и недостатков предложенного нового варианта оценки информационной инфраструктуры ЭС как СМИБ в соответствии с требованиями ISO 27001 приведено в таблице 4.12.

Таблица 4.12 – Описание преимуществ и недостатков оценки ЭС как СМИБ

Достоинства	Недостатки
▪ Международная унифицированные требования выполнения аудита СМ (ISO 19011). ▪ Международный стандарт касательно требований к СМИБ, в том числе – перечень рекомендуемых мер (средств) ИБ (ISO 27001). ▪ Дополнительная сертификация ЭС как ИТ-услуг в соответствии с ISO 20000. ▪ Дополнительная сертификация ЭС в области непрерывности бизнес-процессов в соответствии с ISO 22301. ▪ Высокая унификация выполнения работ на любом национальном уровне ТС – единый план аудита, единые критерии аудита. ▪ Доступность материалов аудита для информационного обмена государств-членов ТС. ▪ Получение Сертификата соответствия как свидетельство оценки объективным аккредитованным национальным и международным органом (IAF). ▪ Доступность периодического контроля над качеством и сроками проведения независимого и объективного аудита СМИБ. ▪ Возможность независимого контроля не только экспертной оценки документации на объект аудита, но и осуществление контроля аудита СМИБ непосредственно на объекте.	▪ Возможная трудоемкость организации процесса аудита с учетом формирования национальной команды аудита. ▪ Требование проведения двух этапов аудита, в том числе обязательно проведение аудита на объекте (*on-site audit*). ▪ Возможные проблемы при выполнении национальных требований по ИБ в силу выбора и применения различных средств (мер) обеспечения ИБ, например, криптографических средств.

4.3.5 Оценка соответствия инфраструктуры ЭС требованиям ISO 27001

Принятие объекта (информационной инфраструктуры ЭС) с установленными границами (*boundaries*), областью сертификации (*scope*),

совместно с мерами (средствами) обеспечения ИБ (*controls*), системой документации (*documented information*) в качестве СМИБ и выполнение сертификации в рамках единых и признанных всеми государствами-членами ТС требований национальных регуляторов – стандарта ISO 27001 позволит:

— разработать и утвердить единый документ, определяющий требования ИБ;
— разработать план проведения аудита, в том числе для сертификации СМИБ на соответствие критериям стандарта ISO 27001;
— назначить группу компетентных и аттестованных аудиторов ТС;
— провести независимый аудит 3-й стороной (сертификацию) СМИБ на соответствие утвержденным критериям стандарта ISO 27001;
— предоставить заключение группы аудиторов национальным органам ТС.

4.3.6 Математическое обоснование выбора схемы сертификации ЭС по ISO 27001

Представляется необходимым подготовить математическое обоснование для объективного оптимального выбора схемы оценки инфраструктуры ЭС для целей предоставления международной признанной сертификации именно на базе ISO 27001. Для планирования этого процесса, как правило, учитывают определенное множество критериев ИБ, которые тесно увязаны с вопросами измерений [318], анализа полученных данных, своевременной интерпретации и сообщения всем заинтересованным лицам (как внутренним, так и внешним).

Известно, что принципиальная сложность выбора при многих критериях заключается в невозможности априорного определения единственного самого наилучшего и оптимального решения; более того, в ряде работ уделяется достаточно внимания проблеме незначительных (небольших) изменений ([141], [55]) или малых возмущающих воздействий, которые могут с течением времени привести к изменению смысла наилучшего решения, или, в пределе, к катастрофическим последствиям. Известно, что многокритериальность подразумевает такое решение управленческих задач, при котором допустимые решения оцениваются по нескольким показателям (или критериям) одновременно [141], [55]. Известно, что существует принципиальная сложность

решения указанных выше задач – невозможность априорного определения наилучшего (оптимального) решения из множества допустимых решений. Отметим, что наилучшее выбранное решение должно удовлетворять ожиданиям всех заинтересованных сторон (*stakeholders,* в нотации [315]), перечень которых является счетным множеством [105], [111].

Установим набор числовых функций $f_1, f_2 \ldots f_m, m \geq 2$, определенных на множестве возможных решений X как критерии оптимальности (целевые функции). Вектор $f = (f_1, f_2, \ldots, f_m)$ называют векторным критерием, который принимает значения в m-мерном пространстве $\mathbf{R^m}$, называемым критериальным пространством или пространством оценок.

Векторной оценкой возможного решения $\mathbf{x} \in \mathbf{X}$ для векторного критерия f называют:

$$\mathbf{f(x) = (f_1(x), f_2(x), \ldots f_m(x)) \in R^m}$$

Все возможные векторные оценки образуют множество возможных оценок:

$$\mathbf{Y = f(x) = \{ y \in R^m \mid y = f(x) \text{ при } x \in X \}}$$

Все возможные выбираемые оценки образуют множество выбираемых векторов (оценок):

$$\mathbf{C(Y) = f(C(X)) = \{ y \in Y \mid y = f(x) \text{ при } x \in C(X) \}}$$

Многокритериальной задачей (задачей многокритериальной оптимизации – МКО) называют задачу выбора, которая включает множество допустимых значений X и векторный критерий f. Также говорят, что задача МКО состоит в отыскании множества выбираемых решений **C(X),** таких, что $\mathbf{C(X) \subset X}$ с учетом отношения предпочтения $\succ_X$ на основе заданного векторного критерия f, установленного в соответствии с целями (предпочтениями) ЛПР. Крайне важно, чтобы данная задача не оказалось чрезмерно сложной, но эта проблема может быть решена за счет определения степени детализации на этапе постановки задачи ЛПР и определения приемлемого состава векторного критерия.

Известно, что решение $\mathbf{x^* \in X}$ называют оптимальным по Парето (или парето-оптимальным), если не существует такого возможного решения $\mathbf{x \in X}$,

для которого выполняется неравенство $\mathbf{f(x) \geq f(x^*)}$ ([141], [55]). Парето-оптимальные решения образуют множество Парето $P_j(X)$:

$P_j(X) = \{ x^* \in X \mid$ не существует такого $x^* \in X$, для которого $f(x) \geq f(x^*)\}$.

Важно, что парето-оптимальное решение – допустимое решение, при котором не может быть улучшение ни по одному из имеющихся критериев без ухудшения иного другого имеющегося критерия. Множество парето-оптимальных решений – множество компромиссов, при которых ЛПР осознанно принимает решение о выборе определенного «выигрыша» и принятия потерь, минимально по одному критерию. Задача может быть несколько упрощена, если ЛПР предлагает несколько критериев оптимальности, и тогда формируется так называемое «направление заинтересованности» ЛПР. Но в этом случае также нужно фиксировать ограничения для доминирования решений $\mathbf{X\ (x^1 \succ_X x^2;\ x^2 \succ_X x^3;\ldots)}$, что может привести к пустому множеству (в пределе).

Обратим внимание, что в работе Р. Кини и Х. Райфа приведено обоснование применения теории полезности фон Неймана и Моргенштерна для рационального поведения ([64], стр. 10). В соответствии с предположением о рациональном поведении ЛПР для каждой альтернативы следует определить специальный показатель («полезность»), который удовлетворял бы двум критериям: чем выше «полезность», тем выше должен быть показатель, и шкала «полезности» должна отражать выбор наилучшей из альтернатив. Вообще алгоритм полезности включает и экспериментальные оценки и оценку рисков ЛПР, что выгодно подчеркивает его применимость для реализации практических задач и, в частности, для оценки уровня ИБ. В качестве примера можно привести проект «*предсказательного технического обслуживания*» (*Predictive Maintanance*)[223], в рамках которого требовался опыт многопараметрической МКО применительно к разработке и внедрению компьютерных моделей. Известно, что принцип Эджворта-Парето гласит – если ЛПР ведет себя «разумно», то выбираемые решения обязательно должны быть парето-

[223] http://www.cnews.ru/news/top/2017-05-29_aeroflot_zajmetsya_diagnostikoj_samoletov_s

оптимальными [141]. Здесь «разумность» поведения ЛПР подразумевает выполнение двух минимальных условий:

1. Выполнение аксиомы исключения доминирующих векторов: для любой пары допустимых векторов $\mathbf{y^1}$, $\mathbf{y^2} \in \mathbf{Y}$, для которых выполнятся $\mathbf{y^1} \succ_Y \mathbf{y^2}$, выполнено $y^2 \notin C(Y)$
2. Выполнение аксиомы Парето: для всех пар допустимых решений $\mathbf{x^1}, \mathbf{x^2} \in \mathbf{X}$, для которых выполняется неравенство $\mathbf{f(x^1) \geq f(x^2)}$, выполняется и $\mathbf{x^1} \succ_X \mathbf{x^2}$

В практическом аспекте необходимо принять к рассмотрению ценное свойство множества Парето – существования непустого множества парето-оптимальных векторов. Это означает, например, что при известных фиксированных критериях $\boldsymbol{f}$ (например, бюджет, цели, сроки, персонал), есть принципиальная возможность выбора, например, оптимального набора мер (средств) обеспечения ИБ в проекте реализации инфраструктуры ЭС для целей сертификации СМИБ. В работе Р. Кини и Х. Райфа неоднократно подчеркивается важность учета и политических рисков ([64], стр. 14).

В данном конкретном приложении учет именно данной категории рисков следует признать ключевым для оценки так называемых «последствий» - т.е. совокупных затрат и приобретений при реализации именно данной конкретной альтернативы ([64], стр. 19). Анализ затрат следует готовить к защите перед различными категориями (группами по интересам), т.к. эта объективная групповая экспертная оценка позволит выявить все потенциально «слабые» места в существующих альтернативах и, при необходимости, предложить («конструировать» в терминах Т. Саати) новые альтернативы.

4.3.7 Учет новых альтернатив при экспертизе

Экспертиза должна поддерживать возможность учета новых альтернатив, например, перспективы компании Intel прекратить поддержку BIOS к 2020 г. По словам B.Richardson поддержка BIOS будет полностью удалена из клиентских платформ и дата-центров[224]. С исчезновением режима на устройствах перестанут

[224] http://www.uefi.org/sites/default/files/resources/Brian_Richardson_Intel_Final.pdf

запускаться 16-разрядные ОС, которые применяются в диагностике жестких дисков и, кроме того, невозможно будет запустить 32-ти битные версии Windows, в том числе Windows 7. Как отмечают в Intel, с прекращением поддержки BIOS возрастет безопасность системы, поскольку появится возможность постоянного использования режима Secure Boot[225]. Эта альтернатива существенно изменит рынок СрЗИ и/или СКЗИ и потребует разработки иных мер защиты.

Следующим примером является демонстрация на саммите CyberSat удаленного взлома компьютерных систем коммерческого самолета Boeing 757 вне лабораторных условий[226]. В ходе взлома удалось получить доступ к системам Boeing посредством радиочастотной связи. Отмечено, что исправление уязвимостей в каждом самолете – дорогостоящая процедура: стоимость изменения одной строки кода в авиационном оборудовании составляет более 1 млн. долл. Следует отметить, что появление новых результатов более углубленного тестирования критических компонент СлПО приведет к необходимости учитывать новые альтернативы и продумывать новые методы защиты.

4.3.8 Формирование критериев оценки уровня ИБ

Для целей формирования критериев оценки ИБ для решения поставленной задачи – формирование международных признанных оценок ИБ инфраструктуры ЭС, могут быть предложены **новые** критерии:

f_1 – стоимость проекта сертификации,

f_2 – стоимость консалтинга для сертификации,

f_3 – длительность проекта сертификации,

f_4 – объем документации, требуемой для сертификации,

f_5 – стоимость новых контрактов (международных) после сертификации,

f_6 – стоимость признания сертификата соответствия в ТС.

f_7 – доступность национальных экспертов для выполнения сертификации.

---

225 https://www.securitylab.ru/news/489782.php

226 https://www.securitylab.ru/news/489622.php

Критерии этой группы могут выбираться на основании доступных рейтингов, например: «Крупнейшие ИТ-консультанты в России 2017»[227]. В этом рейтинге по категории «Рост выручки от оказания услуг консалтинга и аудита в сфере ИТ» подразумеваются, в силу специфики данных компаний, и аудит ИБ. Обратим внимание, что трехзначные результаты продемонстрировали только 2 компании, признанные лидеры в области и ИТ и ИБ: «Информзащита» (121,4%) и InfoWatch (337,4%). Эти же критерии могут быть применены и для формирования перспективных оценок. Например, «Коммерсант»[228] публикует данные, что в 2017 г. рынок консалтинга в ИТ в России составил почти $30,9 млн, а в 2021 г. достигнет $37,8 млн. В частности, наиболее высокие темпы роста будут у тестирования на проникновение и уязвимости (4,7% в год) и планирования стратегии безопасности (5,9%). Подчеркивается, что «*расходы на консалтинг будут расти — в том числе, из-за необходимости проводить аудиты и проверки соответствия растущему числу нормативно-правовых требований*».

В работах [141] и [55] отмечается, что нахождение парето-оптимальных векторов путем прямого перебора при неограниченной размерности возможных векторов – невозможно. Соответственно, требуется либо специальные знания ЛПР (что на практике встречается недостаточно часто), либо система необходимых (достаточных) условий парето-оптимальности.

В рассматриваемом примере оптимизации по Парето имеем:

— 3 варианта $Y = \{ y^{(1)}, y^{(2)}, y^{(3)} \}$,

— 7 критериев ($m = 7$),

— количественную (балльную) шкалу – 5 баллов.

Кроме того, нужно минимизировать ряд критериев:

$f_1 \rightarrow f_1 = 5 - f_1$

$f_2 \rightarrow f_2 = 5 - f_2$

$f_3 \rightarrow f_3 = 5 - f_3$

---

227 http://www.cnews.ru/reviews/rynok_ituslug_2017

228 https://www.kommersant.ru/doc/3546784

Рассмотрим спецификацию вариантов:

— $y^{(1)}$ = Аттестация инфраструктуры ЭС как ОИ (документы Гостехкомиссии);

— $y^{(2)}$ = Сертификация инфраструктуры ЭС как системы ИТ (ISO/IEC 15408);

— $y^{(3)}$ = Сертификация инфраструктуры ЭС как СМИБ (ISO/IEC 27001).

Детальный анализ вариантов по всем критериям представлен ниже (см. таблицу 4.13):

Таблица 4.13 – Описание преимуществ и недостатков оценки ЭС как СМИБ

Вектор оценок	$\mathbf{f_1}$	$\mathbf{f_2}$	$\mathbf{f_3}$	$\mathbf{f_4}$	$\mathbf{f_5}$	$\mathbf{f_6}$	$\mathbf{f_7}$
$y^{(1)}$	2	2	1	1	3	3	3
$y^{(2)}$	2	3	2	1	3	4	3
$\mathbf{y^{(3)}}$	**2**	**4**	**2**	**2**	**4**	**5**	**5**

Очевидно, что $\mathbf{y^2 \succ_Y y^1}$ (в силу более низкой трудоемкости, национального признания результатов оценки ЭС как объекта оценивания по требованиям ISO/IEC 15408), а также, в свою очередь, $\mathbf{y^3 \succ_Y y^2}$ (в силу более рационального требования к документации, универсальности модели оценки ЭС, доступности технических экспертов для проектирования и оценки, а также широкого национального и международного признания сертификатов ISO 27001). Таким образом, вектор y^3 доминирует над иными векторами $\mathbf{(y^2, y^1)}$, что позволяет исключить их из множества парето-оптимальных: $\mathbf{y^1 \notin C(Y)}$, $\mathbf{y^2 \notin C(Y)}$. Соответственно, можно считать доказанным оптимальное выполнение оценки инфраструктуры ЭС как СМИБ. Формирование заключения с выдачей сертификата о соответствии требованиям стандарта ISO 27001 (как национального, так и международного) возможно для любого государства-члена ТС; также обеспечивается признание доверия к такому сертификату в рамках ТС, а при необходимости – для всех участников информационного обмена и пользователей инфраструктуры ЭС в мире.

4.3.9 Пример исследования сложных промышленных объектов

Рассмотрим несколько крупнейших СлПО, на которых автору в течение периода 2010 – 2017 гг. приходилось выполнять аудит ИБ:

— «КАМАЗ-Дизель» (машиностроение);

— «Водоканал Санкт-Петербург» (коммунальные услуги);

— «Газпром трансгаз» (транспортировка газа);

— Омский НПЗ группы компаний «Газпром нефть» (ОНПЗ);

— Московский НПЗ группы компаний «Газпром нефть» (МНПЗ).

Все данные (на 31.12.2017) об имеющихся сертификатах ISO и иных стандартах (ГОСТ, ГОСТ Р и ГОСТ РВ) сведены в таблице 4.14.

Таблица 4.14 – Данные о сертификации промышленных предприятий РФ

Наименование	Стандарты ISO	Национальные стандарты ГОСТ	Доступный официальный источник
«КАМАЗ-Дизель»	9001 14001 18001 16949 27001	РВ 0015-002-2012	http://www.kamaz.ru/about/policy/labor-protection/; http://www.kamaz.ru/about/quality/system/
«Водоканал Санкт-Петербург»	9001 14001 18001 50001 27001		http://www.vodokanal.spb.ru/o_kompanii/ohrana_okruzhayuwej_sredy/ http://www.regcon.ru/index.php/konsalting/ohsas-18001
«Газпром трансгаз»	9001 14001 18001 50001 27001		http://moskva-tr.gazprom.ru/ecology/ http://www.rusregister.ru/press-center/association-news/?ELEMENT_ID=15701
Омский ПНЗ	9001 14001 18001 50001		http://armtorg.ru/news/1349/ http://www.chemmarket.info/ru/news/view/25184/
Московский НПЗ	9001 14001 18001		http://mnpz.gazprom-neft.ru/search/index.php?q=9001&x=0&y=0 http://mnpz.gazprom-neft.ru/development/ecology/index.php?sphrase_id=15229

В рассматриваемом примере оптимизации по Парето (см. таблицу 4.14) имеем:

— 3 варианта $Y = \{ y^{(1)}, y^{(2)}, y^{(3)} \}$,

— 7 критериев ($m = 7$), как в предыдущем примере,

— количественную (балльную) шкалу – 5 баллов, как в предыдущем примере.

Также нужно минимизировать ряд критериев: f_1, f_2, f_3.

Рассмотрим спецификацию вариантов:

- $y^{(1)}$ = Разработка, внедрение и сертификация ИСМ (в том числе СМИБ в соответствии с требованиями ISO серии 27001);
- $y^{(2)}$ = Разработка, внедрение и сертификация ИСМ (без СМИБ);
- $y^{(3)}$ = Разработка, внедрение и сертификация ИСМ (минимальный «классический» вариант).

Детальный анализ вариантов по всем критериям представлен ниже (см. таблицу 4.15):

Таблица 4.15 – Описание преимуществ и недостатков оценки ИСМ

Вектор оценок	$\mathbf{f_1}$	$\mathbf{f_2}$	$\mathbf{f_3}$	$\mathbf{f_4}$	$\mathbf{f_5}$	$\mathbf{f_6}$	$\mathbf{f_7}$
$y^{(1)}$	2	2	2	4	4	3	3
$y^{(2)}$	3	3	3	3	3	2	5
$y^{(3)}$	4	4	3	2	3	2	5

Очевидно, что выделить явный доминирующий вектор из представленных вариантов $\{ \mathbf{y^{(1)}, y^{(2)}, y^{(3)}} \}$ при заданных критериях $\{ f_1 - f_7 \}$ не представляется возможным, т.к. в данный момент в РФ нет объективных факторов, способствующих более широкому применению и независимой оценке международных стандартов в области ИБ. Это обстоятельство подтверждается, в том числе, и более чем «скудной» практикой сертификации по требованиям стандарта ISO 27001 и единичными примерами внедрения СМИБ в различных отраслях (ТЭК, машиностроение, см. рисунок 4.3). В работе Р. Кини и Х. Райфа отмечается, что даже опытные аналитики «*часто оказываются не в состоянии детально и точно разработать и предложить альтернативы действий, ориентированных на процесс*» ([64], стр. 24). Отчасти это обстоятельство можно объяснить тем, что множество переменных, существенных для принятия взвешенного экспертного решения ЛПР, становится известным уже только в процессе. Также как и предварительное формирование «схемы дерева решений» может оказаться практически неприменимым – по той же причине.

4.4 Пример реализации проекта управления ИБ

4.4.1 Постановка задачи для практического применения

На данном этапе развития технологии обеспечения ИБ, одним из важнейших по-прежнему является вопрос эффективного управления данным процессом, основанным на выборе наиболее «подходящих» для конкретной отрасли стандартов ISO. Минимально необходимо учитывать два аспекта указанного процесса: технический – собственно управление средствами (мерами) обеспечения ИБ (задача результативности) и экономический – обоснование ресурсов, выделяемых на нормальное функционирование указанного процесса (задача эффективности). Технический аспект в настоящее время достаточно отработан – комплекс средств (мер), направленных на обеспечение ИБ, принято объединять в ИСМ, создаваемую в рамках всей организации, подчиненную высшему руководству и периодически оцениваемую по определенным метрикам. Для ИСМ выполняется требование по оценке результативности – как оценки степени достижения всех установленных целей и мероприятий, направленных на обеспечение определенного уровня ИБ.

4.4.2 Экономический аспект процессов обеспечения ИБ

Экономический аспект процессов обеспечения ИБ разработан недостаточно, т.к. наблюдается широкий диапазон разноплановых подходов и методов к задаче обоснования бюджета для функционирования ИСМ. Поскольку напрямую невозможно установить однозначную зависимость между бюджетом и достижимым уровнем результативности (т.е. уровень обеспечения ИБ не зависит явно только от размера выделения финансовых средств), представляется необходимым предложить некоторые численные метрики. Наиболее оптимальным и удобным для практического применения представляется подход анализа зависимости бюджета ИСМ посредством оценки последствий инцидентов ИБ.

Проблема получения оценок бюджета СМИБ достаточно хорошо известна [98]. И эта проблема длительное время «консервировалась» высшим руководством предприятий с позиции «необходимости разрабатывать, закупать

и внедрять». Организационные вопросы доминировали над «техническими» задачами и, в том числе, вопросы обеспечения ИБ также были отнесены к остаточному распределению бюджета. Мотивация высшего руководства в части финансирования СМИБ (ИСМ) должна опираться как на внутренние аспекты (обеспечение комплексной безопасности для достижения плановых показателей), так и на внешние – требования регуляторов, которые накладывают известные ограничения именно на технические системы организации. Кроме того, должны быть приняты во внимание и новые вызовы («*таргетированные*» атаки ATR на КВО, недобросовестные подрядчики и ограничения вендоров в силу санкционных требований и пр.), способные стать причинами техногенных катастроф и привести к значительным убыткам. Например, авария 15.06.2014 г. на Ачинском НПЗ привела к гибели 8 человек, 6 месяцам простоя по выпуску товарного бензина и убыткам более чем в 1 млрд. руб. (по данным издания «Коммерсант»). Что касается ограничения вендоров, то известны наиболее яркие примеры отказа поставщиков ПО (в 2014 г. компания Red Hat прекратила работу с 20 компаниями, в т.ч., с несколькими банками), оборудования (в 2016 г. Nokia Networks отказался продолжать обслуживать сети принадлежащих «Мегафону» сотовых операторов «Аквафон» и «Остелеком») и услуг (в 2015 г. после взрыва в Тяньцзине был срочно остановлен в ручном режиме суперкомпьютер Tianhe-1A в Национальном суперкомпьютерном центре).

Для получения общих оценок бюджета для обеспечения безопасности наиболее известен подход применения простого коэффициента к бюджету, выделяемого на обеспечение функционирования всей ИТ-инфраструктуры. Например, по данным отчета [381], около 25% организаций применяют автоматизированные системы для поиска и устранения «чувствительных» данных. Однако, поскольку конфиденциальные данные распределены по всему предприятию, ЛПР не обладает полной информацией о том, где эти данные хранятся в произвольный момент времени и кто имеет к ним доступ. Соответственно, эти оценки не дают «полной картины» возможных нарушений

и размера потенциального ущерба (в т.ч НМА) для организации при негативном сценарии реализации инцидентов ИБ, в частности:

- Риски репутации. По данным отчета [365], реализуются риски, порождаемые социальными сетями: сотрудники могут «выносить сор из избы» и легко организовать репутационную атаку, особенно при согласованной поддержке «заинтересованных» СМИ;
- Риски нарушения ИБ со стороны третьих лиц. По данным отчета [395], крупные организации часто не разглашают данные о нарушениях ИБ своих поставщиков и субподрядчиков (пример Э. Сноудена, сотрудника компании – подрядчика АНБ).

С учетом сказанного выше, предлагается следующая постановка задачи: определение комбинированной метрики, расчет которой с учетом оценки последствий инцидентов ИБ, позволит сформировать общую оценку бюджета для реализации проекта ИСМ с целью обеспечить заданный уровень обеспечения ИБ. В качестве нормативной базы рассматриваются национальные стандарты ГОСТ Р ИСО/МЭК серии 18044, 20000, 22301 и 27001 [28], [30], [315], [317]. Для определения метрик ИБ применяется метод оценки результативности СМИБ, представленный в ([89], [99]). Дополнительно предлагается использовать ранги «лидеров» отраслей, представленные в работе [105] и выполнить уточнения с учетом статистических данных ISO.

4.4.3 Оценка требуемого уровня обеспечения ИБ для бизнеса

Дополнительно обратим внимание на статистику сертификации СМИБ по стандарту ISO 27001, с учетом расчетов по рангам «лидеров» [105], [97]. Исследования показали, что рост количества выданных сертификатов на СМИБ составил в 2014 г., для «лидеров» 1-го ранга максимально – до 14%, а минимально -0,7%; для «лидеров» 2-го ранга зафиксировано падение минимально до 8%, и для «лидеров» 3-го ранга – рост максимально до 27%, причем отрасль «Information technology» показала падение на 2,5%. Необходимо принять во внимание, что не все компании в процессе обеспечения ИБ создают именно «официальную» СМИБ и, также верно, что не все организации проводят

для СМИБ внешнюю независимую оценку (сертификацию) в международных аккредитованных органах по сертификации. Эти оценки являются значимыми для решения поставленной задачи – иначе говоря, какие требования бизнес готов определить и выполнять для обеспечения требуемого (заданного) ЛПР уровня ИБ. Далее предлагается кратко рассмотреть основные требования бизнеса, способные оказать значительное влияние на решение поставленной задачи.

Требование обеспечения 100 % защиты

При данной постановке организация требует, чтобы для всех активов были внедрены соответствующие меры (средства) обеспечения ИБ. Это требование, очевидно, представляется логичным (в терминах «разумного поведения ЛПР» [141]) для организаций, которых можно отнести к объектам критичной инфраструктуры (СлПО). В иных случаях вполне достаточно получить пороговые значения стоимости активов и/или бюджета на реализацию мер (средств) обеспечения ИБ от ЛПР ([317], [322]). В качестве примера можно привести опубликованные данные о подходах службы ИБ компании «Эльдорадо»[229] и компании МГТС[230].

Требование контроля привлекаемых подрядчиков

Современные стандарты [28], [30], [315], [317] в явном виде содержат требования к процессам аутсорсинга (иногда говорят «внешнее обеспечение»), которые позволяют организациям более эффективно выполнять специфические процессы через уполномоченных посредников. Однако, не все процессы и не всегда можно передавать «на сторону», в том числе и по соображениям экономического порядка. В качестве примера приведем данные исследования EMC[231], посвященного системам защиты данных. Аутсорсинг процессов, связанных с чувствительными данными, может привести к значительным издержкам – при выборе 2 и более посредников затраты превышали 20%, чем при схеме с 1 подрядчиком, а при выборе 3 подрядчиков затраты на инфраструктуру защиты данных превышали в среднем 1 млн. долларов США.

229 http://www.cnews.ru/news/line/index.shtml?2015/03/04/593449
230 http://safe.cnews.ru/reviews/index.shtml?2015/03/13/593760
231 http://www.cnews.ru/news/line/index.shtml?2014/12/09/590643

Эти же опасения подтверждаются в отчете [389] – крупные компании часто уделяют минимальное внимание мониторингу безопасности своих поставщиков и цепочек поставок.

Применение организационных мер ИБ

ЛПР логично полагают уместным не тратить значительные средства на реализацию технических систем обеспечения ИБ, когда можно реализовать организационные меры в ИСМ, например, в рамках реализации СМИБ – именно как функциональной СМ. В продолжение анализа проблемы безопасности (*safety*) производственных систем рассмотрим, как решается проблема сложности ИБ решений. По данным CISCO 46% профессионалов в области обеспечения безопасности на производственных объектах заявили, что они используют 6 и более поставщиков; 20% заявили, что количество их поставщиков превышает 10. На вопрос о продуктах 63% профессионалов в области обеспечения безопасности ответили, что они используют 6 и более продуктов; а 30% ответили, что используют более 10 продуктов[232].

4.4.4 Влияние на активы организации

В отчете [389] отмечено, что количество и качество обнаружения инцидентов ИБ является зависимостью от размера компании, соответственно, применение специальных мер (средств) обеспечения ИБ может влиять, в определенной мере, на количество детектируемых инцидентов. Согласно представленным оценкам, общее число обнаруженных инцидентов ИБ по сравнению с 2013 г. превышает 42,8 млн. в мире в год, что составляет порядка 117.000 инцидентов каждый день. Отметим, что речь идет только об обнаруженных и категорированных инцидентах, но есть серьезные опасения, что не все компании, особенно крупные, готовы публично подтвердить факты нарушения ИБ в своих ИТ-системах [389].

Принято разделять финансовые и не финансовые издержки в результате инцидентов ИБ. К финансовым издержкам относят, традиционно, потери доходов, прерывания доступности бизнес-систем, санкции со стороны

---

232 blogs.cisco.com/security/talos/locky-returns-necurs

регуляторов и снижение доверия со стороны клиентов. К не финансовым издержкам относят снижение репутации, утечки данных о продуктах (услугах), потери ценной исследовательской информации (инновациях), а также «неуместное» разглашение чувствительной информации о бизнес-планах, стратегии развития, процессах производства и пр.

Рассмотрим пример инцидента массового сбоя в сети «Мегафон»[233], после которого, по данным ПАО (МТС), 19.05.2017, объем дневных продаж SIM-карт в Москве вырос в 2 раза, а в Поволжском регионе было реализовано в 5 раз больше SIM-карт. Соответственно, для руководства оператора «Мегафон» произошедший крупнейший в истории сбой сети получил вполне четкую финансовую оценку потерь (как прямых – продажи SIM-карт, так и репутационных). Следующий пример касается оценки потерь авиакомпании British Airways[234] после сбоев в работе своих компьютерных систем, вследствие их масштабного отказа 27.05.2017. После перебоев с электроснабжением вышли из строя ИТ-системы British Airways, были отменены несколько рейсов, в результате тысячи пассажиров были блокированы в аэропортах. По словам экспертов, ИТ-системы British Airways стали работать с перебоями с 2016 г., когда был уволен ряд сотрудников, и часть операций перенесены в Индию. Как сообщает Reuters, только прямые убытки за 1 день простоя обходится British Airways в $38,5 млн., не считая компенсаций пассажирам.

Рассмотрим еще один пример оценки ущерба для транснациональной компании. Maersk опубликовала финансовый отчет за второй квартал 2017 г., в котором сообщила о последствиях атаки вируса NotPetya[235]. Стало известно, что вирус попал в компьютерную систему компании Maersk через украинскую программу M.E.Doc, которая использовалась для заполнения отчетности в Украине. В компании Maersk особо подчеркнули, что заботятся о кибербезопасности, однако применяемые антивирусы оказались неэффективны для отражения атаки. Maersk оценивает финансовые потери от кибератаки в 200

---

233 https://www.rspectr.com/novosti/50800/prodazhi-sim-kart-mts-vyrosli-vdvoe

234 http://www.securitylab.ru/news/486324.php

235 http://www.maersk.com/en/the-maersk-group/press-room/press-release-archive/2017/8/a-p-moller-maersk-interim-report-q2-2017

– 300 млн. долларов США. Не менее интересен анализ борьбы с последствиями прошедшей атаки. В рамках выступления на экономическом форуме в Давосе Председатель совета директоров Джим Хагеман Снабе (Jim Hagemann Snabe) сообщил, что для восстановления IT-инфраструктуры вся корпорация Maersk на 10 дней перешла на ручной учет текущих операций[236]. Эта задача нетривиальная, учитывая, что каждые 15 минут проходит до 20 тыс. контейнеров. За этот срок специалисты Maersk заново переустановили около 4 тыс. серверов, около 45 тыс. персональных ОС и более 25 тыс. приложений[237]. Соответственно, вопрос «доказательства» для ЛПР размера запрашиваемого бюджета ИБ должен быть увязан с уровнем финансовой ответственности за обеспечение непрерывности бизнес-процессов и принятой финансовой дисциплиной в каждой организации – расчет уровня возврата инвестиций (IRR), стоимости полного цикла поддержки мер (средств) обеспечения ИБ (TCO) и пр.

4.4.5 Оценка стоимости выбранного варианта системы управления ИБ

Очевидно, что любой владелец актива обладает всей полнотой информации (в т.ч. в части оценки уровня обеспечения ИБ) и, следовательно, может обосновать как минимальные, так и максимальные риски, которые напрямую определяют размер потенциального ущерба в случае негативного сценария реализации инцидента ИБ. Именно по данной причине в предлагаемом **новом** методе оценки в ИСМ выбранного варианта СМИБ реализованы все возможные типы аудита, т.к. проверка умысла владельца актива возможна лишь посредством равной по уровню компетенции экспертизы аудитором.

Отдельно рассмотрим вопрос страхования рисков, например, Всероссийский союз страховщиков (ВСС) направил Банку России проект создания национального риск-офиса — центра по управлению социальными и экономическими рисками РФ, в котором бы обрабатывалась статистика различных ведомств. В проекте карта российских рисков наложена на глобальную карту, которая регулярно готовится к Давосскому экономическому

---

236 https://threatpost.ru/maersk-vs-expetr/24310/

237 http://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/

форуму. Из этого сравнения следует, что российские риски выше глобальных по 5 пунктам, в том числе и масштабные техногенные катастрофы[238]. Также в ВСС отмечают, что у экономики РФ нет систематизированного риск-профиля, поэтому страховщики не в состоянии провести полноценные актуарные расчеты. По данным отчетов [54], [78] существуют определенные сложности с оценкой объективности представленных обоснований в отношении как рисков, так и размеров потенциального ущерба. Рассмотрим несколько примеров того, как официальные органы надзора формально выполняли плановые надзорные проверки на объектах предприятий ТЭК, в частности, на базах хранения нефтепродуктов (см. рисунок 4.11 и рисунок 4.12).

Рисунок 4.11 – Нарушения в серверном помещении на компрессорной станции

Рисунок 4.12 – Разукомплектованный противопожарный щит насосной станции нефтебазы

На первом этапе оценки определяется «базовый коэффициент», который содержит общую оценку защищаемых активов и применяемых мер (средств) обеспечения ИБ:

$$К_{Эфф.базовая} = \frac{\sum_{i=1}^{m} M_{ИБ\,i}}{\sum_{j=1}^{n} А\,j} \qquad (4.4)$$

238 https://www.kommersant.ru/doc/3479334

где:

$М_{иб\,i}$ – стоимость меры (средства) обеспечения ИБ;

$А_j$ – стоимость защищаемых активов

Данная обобщенная оценка по формуле (4.4) дает удобный инструмент для числового анализа двух крайних концептуальных оценок:

При $\mathbf{К_{Эфф.} \rightarrow 0}$, называем ситуацией «*Тришкин кафтан*», которая характеризуется низким уровнем применяемых технических СрЗИ, высокой долей ручного труда и, как следствие, наблюдается запаздывание реакции, что может привести в результате к потере контроля над критичными активами в случае негативного сценария инцидента ИБ.

При $\mathbf{К_{Эфф.} \rightarrow 1}$, называем ситуацией «*Золотая безопасность*», которая характеризуется применением, часто весьма избыточного, дублирующего количества дорогостоящих мер (средств) обеспечения ИБ, приближающихся по стоимости к защищаемым активам.

Однако, необходимо принять во внимание, что при защите КВО, высокий уровень затрат на обеспечение ИБ установлен регуляторами и не подлежит произвольному сокращению [142] – [145]. Отметим, что оценки стоимости даже для серьезных инцидентов могут быть получены из доступных источников, в частности, известна оценка «стоимости» теракта в метро в 2017 г. в Санкт-Петербурге: 150 тыс. руб.[239] В Приказе ФСТЭК России № 235[240] представлены 4 группы требований к системе безопасности значимых объектов КИИ РФ. Но этот приказ содержит ряд противоречий, например, с ФЗ-184 ([243]), т.к. ограничивается только двумя видами оценки соответствия (сертификация, испытания или приемка в соответствии с программой и методикой испытаний). Также содержится указание на фиксированные модели УБИ и годовой цикл внутренних проверок. К сожалению, введено исключение для внешнего аудита (если проводится внешний аудит), а внешний аудит проводится по «усмотрению» руководителя. Также не представлено явно критериев и метрик

239 https://www.kommersant.ru/doc/3447751

240 http://rulaws.ru/acts/Prikaz-FSTEK-Rossii-ot-21.12.2017-N-235/

оценки степени защищенности для КИИ или ссылок на них[241]. В продолжение темы оценки соответствия по требованиям ФЗ-184 ([243]), отметим ситуацию, на которую обратил внимание М. Емельянникова по итогам Международной конференции «Защита персональных данных» Роскомнадзора (2017 г.): что представитель ФСБ А.Бодров определил оценку соответствия СКЗИ только в форме сертификации в системе ФСБ, а просто признать угрозу перехвата ПДн в канале связи неактуальной и не применять сертифицированные СКЗИ нельзя[242]. При этом отсутствие модели угроз является административным правонарушением.

С учетом того, что в мае 2018 г. в Европе вступают в силу обновлённые правила обработки ПДн, установленные Общим регламентом по защите данных (Регламент ЕС 2016/679 от 27 апреля 2016 г. или GDPR — General Data Protection Regulation), целесообразно обратить внимание, что Регламент GDPR и ФЗ-152 в РФ имеют различное действие в пространстве, по кругу лиц и во времени[243]. Обобщенно можно сказать, что Регламент GDPR и ФЗ-152 в РФ, регулирующие сферу ПДн, имеют самостоятельную территориальную и юрисдикцию применения; при этом некоторая общность подходов регулирования не дает основания сделать вывод относительно легкости и прозрачности их «гармонизации»[244].

Пример расчета эффективности показан на рисунке 4.13. Левая шкала показывает оценки стоимости активов, средств (мер) обеспечения безопасности и данные по результативности ИСМ (в составе, минимально СМК и СМИБ). Правая шкала отдельно отражает рост издержек от инцидентов безопасности, способных негативно повлиять на активы организации. В представленном примере на основе разработанного математического аппарата ([98], [101]), учитываются численные метрики (важно, что именно количественные оценки), которые позволяют варьировать показатели защищаемых активов организации:

---

241 http://elvis.ru/competency/expert_comments/1727/

242 https://www.securitylab.ru/blog/personal/emeliyannikov/342969.php

243 https://www.osp.ru/cio/2017/07/13052947/

244 https://habrahabr.ru/company/cloud4y/blog/347870/

(определены активы начальной стоимостью 1 млн. руб.), стоимость комплекса средств (мер) обеспечения ИБ (определена начальная стоимость 180 тыс. руб.) и 4 значения результативности реализованных средств (мер) обеспечения безопасности (определяемых, например, по результатам всех типов аудита ИСМ (внутренних и внешних) – 0,5; 0,7; 0,9 и 0,99).

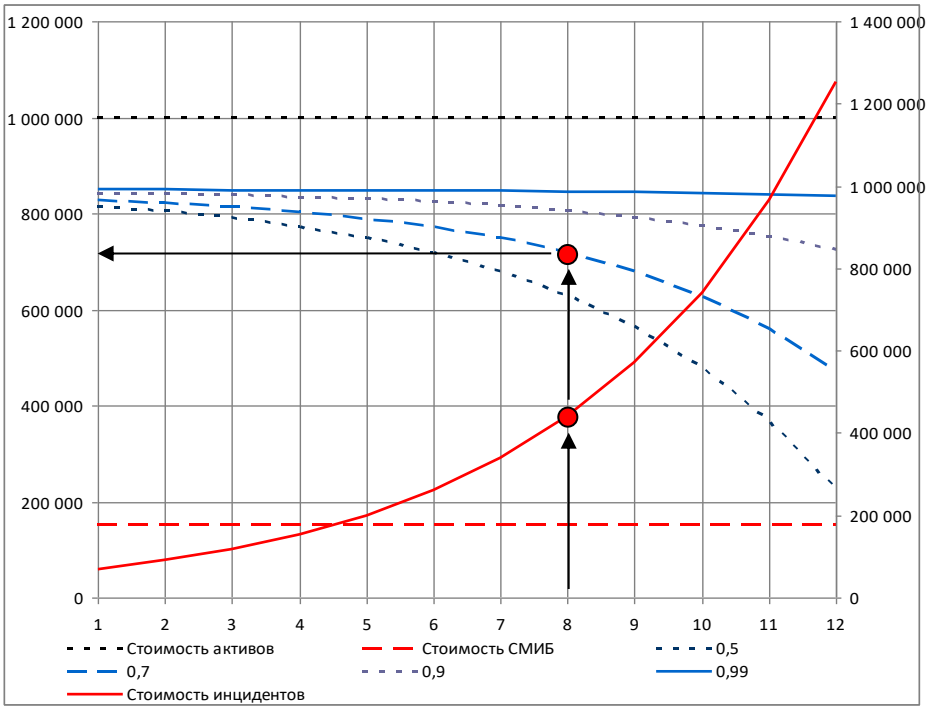


Рисунок 4.13– Оценка экономической эффективности ИСМ

Предположим, что количество инцидентов ИБ, способных нанести ущерб активам организации, растет неравномерно в течение года (по закону, близкому к экспоненциальному). В определенный момент, если не предпринять адекватных действий, ущерб может сравняться со стоимостью активов организации, т.е. полностью разрушить бизнес [315]. Необходимо отметить, что стандарты [315], [317] и [311] содержат требования к обеспечению непрерывности бизнеса и предлагают ряд сценариев для управления снижением ущерба при возможных воздействиях (*business impact*).

Рассмотрим пример противодействия ДД для ИСМ: на 8 месяцев размер потенциального ущерба от инцидентов безопасности $\mathbf{C_{инц}}$ составит 420 тыс. руб. (правая шкала), что уже превышает стоимость реализованного комплекса средств (мер) обеспечения безопасности $\mathbf{C_{моб}}$ (180 тыс. руб.), стоимость активов организации $\mathbf{C_{акт}}$ составляет 1 млн. руб., степень результативности системы

безопасности ИСМ $\mathbf{Р_{ИСМ}}$ определим равной 0,7. В данном примере актуальная стоимость активов организации $\mathbf{А_{ИСМ}}$ (благодаря реализованному комплексу средств (мер) обеспечения безопасности), составит:

$$\mathbf{А_{ИСМ}} = \mathbf{С_{акт}} - \mathbf{С_{моб}} - \mathbf{С_{инц}} * (1 - \mathbf{Р_{ИСМ}}) = 694.000 \text{ руб.}$$

Заметим, что без внедрения комплекса средств (мер) обеспечения безопасности, стоимость активов $\mathbf{А_{ИСМ}}$ при $\mathbf{С_{моб}} = 0$ и том же размере $\mathbf{С_{инц}}$ составит всего лишь на 16 % меньше:

$$\mathbf{А_{ИСМ}} = \mathbf{С_{акт}} - \mathbf{С_{инц}} = 1.000.000 - 420.000 = 580.000 \text{ руб.}$$

Также отметим, что с увеличением времени работы ИСМ (в составе СМИБ) экономическая эффективность будет только возрастать. Кроме того, будет накапливаться положительный опыт противодействия попыткам негативного воздействия на ценные активы организации («*приработка системы*»), что в конечном итоге повышает оценку результативности подсистемы ИБ (СМИБ) в составе ИСМ и, как следствие, общую устойчивость бизнеса. Также можно отметить, что применение современных риск-ориентированных стандартов ISO позволяет формировать экономические оценки применения СМИБ (ИСМ), основанные на постоянном измерении результативности, что обеспечивает условия для снижения издержек и повышения экономической устойчивости организации.

4.5 Выводы к Главе 4

1. Предложен **новый** метод исследования динамики сертификации по международным стандартам, учитывающая публичные статистические данные ISO, влияние «лидеров» разного ранга, приоритеты ведущих отраслей в соответствии с международными кодами EAC и позволяющая оценить изменения предпочтений СМ в составе ИСМ.
2. Опубликованная статистика сертификации ISO дает возможность на основе длительного периода наблюдений оценить целесообразность и обосновать возможность выбора наиболее оптимального «набора» требований для внедрения ИСМ. Это положение справедливо для различных отраслей промышленности, что подтверждается анализом статистики ISO для различных «*лидеров*» сертификации.
3. Представленная статистика сертификации за последние 7 лет показывает, что внимание в РФ к стандарту ISO 27001 значительно возрастает даже по сравнению с мировыми и европейскими показателями для обеспечения безопасности критичных для бизнеса активов в целом для СлПО.
4. Для организации, которая планирует обеспечить экономический рост, могут быть предложены варианты внедрения определенного «набора» ИСМ (СМК, СМИБ, СУУ, СМНБ и пр.), которые объективно позволят достигнуть поставленные высшим менеджментом цели ИБ – на уровне «лучшей мировой практики». Важно, что эти варианты могут быть оценены ЛПР на основе **новых** численных метрик заблаговременно.
5. Предложенная **новая** численная оценка затрат на обеспечение ИБ основывается на использовании достоверных и объективных публичных данных по сертификации ISO и учитывает оценки результативности мер и средств обеспечения ИБ. Дополнительно используются оценки последствий инцидентов ИБ (подтвержденные объективными наблюдениями аудита), что позволяет формировать обоснованную оценку бюджета для внедрения СМИБ (ИСМ) с целью достижения заданного ЛПР уровеня обеспечения ИБ.

5 Глава. Метод многошаговой оптимизации аудита ИСМ для СлПО

5.1 Общие положения

Известны различные подходы к формализации моделей и методов аудита ИСМ. В частности, на ежегодных отраслевых конференциях («АСУ ТП КВО», «Комплексная защита информации», «Банки. Процессы. Стандарты. Качество», «IT & Security Forum») обсуждаются различные аспекты проведения таких аудитов – как правило, основываясь на принятых «обычаях делового оборота», которые могут весьма существенно различаться для разных отраслей. Рассмотрим наиболее применимые на практике модели для выполнения аудита ИБ в ИСМ.

5.2 Модели СТО БР

5.2.1 Научно-практические подходы

На научно-практических конференциях «Банки и финансовые организации: Процессы. Стандарты. Качество», проходящих ежегодно в Национальном банке Республики Башкортостан, на отдельной секции постоянно обсуждаются общие вопросы оптимизации системы внутреннего аудита (СВА). В докладах отмечается, что трансформация международных стандартов, как правило, проходит через «призму» национальной нормативно-правовой базы и демонстрирует сбалансированное сочетание эмпирического и теоретического подходов. В докладе руководителя СВА АО «Россельхозбанк» Туруева И.Б. отмечено, что «Росимущество» довело до сведения профессионального сообщества свое видение СВА в формате методических рекомендаций [204]. Далее эти методические указания были одобрены поручением Правительства РФ от 24.06.2015 № ИШ-П13-4148. Но в отношении кредитно-финансовых институтов эти рекомендации не были согласованы с ЦБ России и не учитывают сложившуюся практику.

В докладе проф. Финансового университета при Правительстве РФ Поморина М.А. рассмотрены вопросы организации процессов риск-менеджмента в банках РФ [205]. Международная практика в области стандартизации СВА для КО банковской системы РФ рассмотрена в докладе

представителя «ПрайсвотерхаусКуперс Консультирование» Морозова В.Е. [206], процесс рассматривается с 3-мя уровнями зрелости (см. рисунок 5.1).

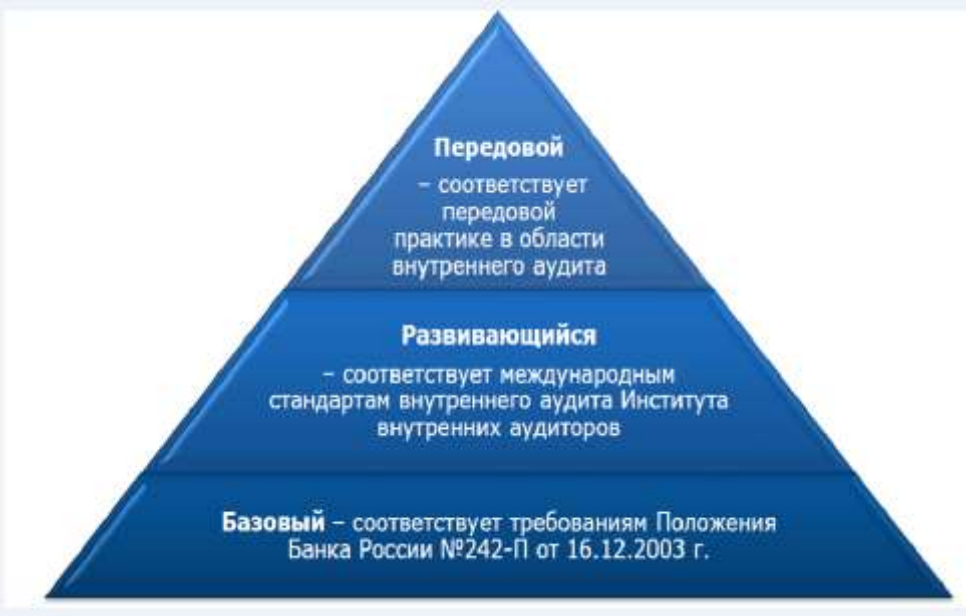


Рисунок 5.1 – Модель АРБ процесса внутреннего аудита на базе Cobit

В основе лежит модель, разработанная Ассоциацией российских банков (АРБ) на основе модели зрелости процессов, определенной методологией COBIT. Отметим, что собственная «ветка» развития данной методологии завершилась и, начиная с версии COBIT 5, соответствует, в определенной мере, спецификации стандарта ISO/IEC 38500[245].

5.2.2 Совершенствование банковского надзора и аудита

В аспекте совершенствования банковского надзора весьма интересна роль аудитов[246], реакция представителя ЦБ показывает, что централизация позволяет уйти от субъективности. В частности, упоминалось, что «*территориальные подразделения порой принимали не такие жесткие меры, как сотрудники ЦБ из Москвы*». Кроме того, отмечено, что «*территориальные подразделения медленнее внедряли новые инструменты надзора, обосновывая это тем, что все банки в регионе у них «как на ладони» — для понимания их рисков достаточно и проверенных подходов*».

245 https://www.isaca.org/Knowledge-Center/Documents/COBIT-Focus-ISO-38500-Why-Another-Standard.pdf
246 http://www.rbc.ru/finances/13/06/2017/593fe8639a7947f825c52161?from=newsfeed

В тоже время централизованный надзор поможет оценивать ситуацию в конкретном банке через призму ситуации в банковской системе в целом и минимизировать время реакции на проблемы банка. Эти вопросы широко обсуждаются в банковском сообществе РФ[247].

5.2.3 Применение комплекса СТО БР ИББС

В практике проведения аудита в области ИБ для КО БС РФ применяется комплекс стандартов СТО БР ИББС [217] – [220]. В стандарте СТО БР ИББС-1.0-2014 указаны важные определения «*оценка соответствия ИБ*» и «*аудит ИБ*». Так же указано (п. 8.14.1 [217]), что аудит ИБ организации БС РФ должен проводиться в соответствии с требованиями стандартов Банка России СТО БР ИББС-1.1 [219] и СТО БР ИББС-1.2 [220]. Определены основные аспекты выполнения аудита ИБ БС РФ: цели – аудит ИБ проводится как для собственных целей самой организации БС РФ, так и с целью повышения доверия со стороны других КО; периодичность – оценка соответствия ИБ в виде аудита ИБ или самооценки ИБ проводится КО БС РФ не реже одного раза в два года (п.п. 9.4 и 9.8 [217], соответственно). Основные принципы проведения аудита ИБ организаций БС РФ указаны в стандарте [219].

5.2.4 Применение системы групповых и частных показателей

Отметим, что в библиографии стандартов [217], [219] приведены ссылки на стандарт ИСО 27001 [317], а общие принципы аудита поддерживают преемственность стандарта аудита ИСО 19011 [20]. Эти факторы обеспечивают реализацию «замкнутого» цикла PDCA, применительно к менеджменту ИБ, в точном соответствии с требованиями СТО БР ИББС (пп. 5.25, 8.1.1. [217]). Также в стандарте [219] отмечается в разделе «Проведение самооценки информационной безопасности» обязательство включения в состав работ по проведению самооценки ИБ организаций БС РФ этапа формирования результатов самооценки ИБ и информирование руководства организации БС РФ о результатах проведенной самооценки ИБ (п. 8.4). В стандарте [220] (раздел 6) установлено, что для оценки степени соответствия обеспечения ИБ КО

247 https://www.kommersant.ru/doc/3481820

требованиям СТО БР ИББС-1.0 используются групповые и частные показатели ИБ. Групповые показатели ИБ образуют простую структуру для трех направлений оценки, детализируя оценки текущего уровня ИБ организации, менеджмента и уровня осознания ИБ. Необходимо сделать предложения, связанные с развитием процесса планирования стратегических (тактических) улучшений, которые высшее руководство КО может реализовывать на основании оценки степени соответствия обеспечения ИБ (п.п. 8.17.1 [217] и 8.18.1 [217], соответственно). Пример практического выполнения периодической оценки степени соответствия обеспечения ИБ для КО по **новому** предложенному методу показан в Главе 3.

Отметим, что в процессе выполнения аудита ИБ в КО по требованиям СТО БР ИББС формируются последовательно частные критерии, которые затем группируются в соответствующие оценки групповых показателей M_i и «свертки» по направлениям оценки EV_k. При этом, например, один частный показатель $M_{11.1}$ участвует в формировании нескольких групповых показателей: M_{11} и M_{28}, аналогично – для $M_{16.1}$ (участвует в групповых показателях M_{16} и M_{29}) и вносит свой вклад в решение максимизации критерия по предложенным в Главе 3 формулам (3.7) – (3.9). Соответственно, в случае, предположим, расчета R — итогового уровня соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0, представляется экономически целесообразным определение для улучшения такого минимального множества показателей (метрик) ИБ, которое позволит перейти к рекомендованному $R \geq 4$ (п. 11.4 в [220]) с минимальными временными и финансовыми издержками. Требования стандартов СТО БР ИББС нельзя трактовать выборочно, поэтому высшее руководство должно обеспечить, во-первых, достижение и постоянный мониторинг требуемого уровня соответствия ИБ $R \geq 4$ ([220]) и, во-вторых, обеспечить формирование и оптимизацию множества показателей (метрик), которые обеспечивают достижение требуемого уровня ИБ.

5.3 Модели СТО Газпром СОИБ

5.3.1 Применение отраслевой практики

В модели СТО Газпром СОИБ применяется отраслевая практика оценки объектов защиты (ОЗ) [221] – [229]. В целом, можно отметить, что СТО Газпром СОИБ (в частности, СТО Газпром 4.2-5-001-2009 «Оценка соответствия объектов защиты») содержит описание порядка оценки соответствия АС. Также отметим, что в СТО Газпром СОИБ даются ссылки на ГОСТ Р ИСО/МЭК ТО 15446-2008 и ГОСТ Р ИСО/МЭК ТО 19791-2008, однако, важно отметить, что эти документы хоть и заимствованы из системы ИСО/МЭК, но не являются в «классическом» понимании стандартами, а только техническими отчетами. Это обстоятельство подчеркивает тот факт, что система СТО Газпром СОИБ в целом не устанавливает требований к ИБ в отрасли том виде, как они приняты в мире – в частности, в соответствии с требованиями NIST, NERC, ИСО/МЭК, Basel, SOX, ITIL, TOGAF и пр.

В указанном документе СТО Газпром 4.2-5-001-2009 под критериями оценки понимается «*совокупность требований ИБ, определенных в ПАО «Газпром», дочерних обществах, характеризующая некоторый уровень ИБ*». При этом сами объекты оценки ограничены – только ИУС ПХД, АС и АСУ ТП. Отмечается, что подтверждение соответствия АС проводится в форме добровольной сертификации в системе Газпромсерт (одна из национальных систем добровольной сертификации в РФ), но не отменяет и не заменяет аттестацию ОИ по требованиям безопасности информации ФСТЭК России.

Также установлена частота проведения внутренней оценки – не реже одного раза в год. Как правило, такие оценки и проводятся с ежегодной периодичностью на основании предварительно утвержденного стандартного плана внутренних проверок. Следует заметить, что опрос в СТО Газпром – простое заполнение типовых опросников («чек-листов») с уже определенными вариантами ответов, что значительно отличается от принятого порядка проведения международных аудитов (например, ISO, ISAGO), порядка формирования «аудиторской выборки», требований непредвзятости и независимости суждений [20], [326].

Далее следует отметить норму по оценке адекватности модели угроз, оценке рисков ИБ по СТО Газпром СОИБ 4.2-3-003 [226]. Этот документ содержит требования по фиксации выявленных несоответствий, а также рекомендации по пересмотру плана обработки рисков. Тем не менее, указанный документ отмечает, что внешняя оценка проводится только по инициативе самого общества (что не следует ни де-юре, ни де-факто из любых требований СТО Газпром СОИБ). Дополнительно отметим, что новые рекомендации в системе СТО Газпром СОИБ (по данным ВНИИГАЗ[248] на 01.11.2017) также «наследуют» заданные ранее ограничения применительно к внедрению СМИБ. Например:

— Р Газпром 4.2-3-005-2016. В этом руководстве процесс управления рисками не соответствует ни ISO (ГОСТ Р) серии 31000, ни ISO (ГОСТ Р) серии 27005, нет ссылок ни на один общепринятый каталог мер защиты ISO (ГОСТ Р) или NIST SP 800 и, по-прежнему, реагирование на риски только в отношении информационных активов (АС или ИС);
— Р Газпром 4.2-3-006-2016. В этом руководстве процессы не соответствуют ISO (ГОСТ Р) серии 27001, выбранные процессы дублируются (например, «Управление эффективностью процессов информационной безопасности», стр. 35 и стр. 43), вместо обязательного процесса аудита вводится оценка эффективности (не результативности) и полностью исключен раздел оценки результативности корректирующих мер.

В качестве примера обеспечения непредвзятости отметим факт приостановки членства аудиторской компании «Топ-Аудита» в СРО[249]. По данным «Коммерсант» «Топ-Аудит» оказывал одному из своих клиентов и консалтинговые услуги, и услуги по аудиту и именно по этой причине получил официальное жесткое предписание.

Крупнейшие аудиторские компании в мире очень дорожат своей репутацией. В частности, это подтверждается готовностью незамедлительно признать свою вину в случае подозрения в предвзятом аудиторском заключении.

---

248 http://vniigaz.gazprom.ru/activities/other/standardization-and-certification/zakaz-dokumentov-sistemy-stand/

249 https://www.kommersant.ru/doc/3373603?utm_source=kommersant&utm_medium=finance&utm_campaign=four

Например, совет по финансовой отчетности Великобритании (FRC) оштрафовал компанию PwC и аудитора Бодена за ошибки, допущенные при аудите компании RSM Tenon Group[250]. PwC должна выплатить 5,1 млн. фунтов, размер штрафа персонально для Бодена составил 114 тыс. фунтов. В FRC отметили, что PwC и Боден признали, что проведенный аудит не соответствовал профессиональным стандартам. В общей практике аудита немного компаний добровольно готовы пригласить независимых экспертов для выполнения внешней оценки с позиции непредвзятого, объективного и независимого (насколько это возможно) профессионального аудитора.

5.3.2 Применение системы групповых и частных показателей

Согласно требованиям СТО Газпром 4.2-3-004-2009 все объекты оценки строго классифицируются как ОЗ. В соответствии с п. 5.8 [227] каждый из идентифицированных ОЗ должен быть отнесён только к одному из следующих типов:

— информационные активы (ИА),

— технические средства обработки, хранения и передачи информации,

— программное обеспечение (ПО).

В соответствии с п. 7.1 [227], исходя из полученного уровня критичности ОЗ, следует относить только к одной из следующих групп:

— ОЗ максимального уровня критичности,

— ОЗ среднего уровня критичности,

— ОЗ минимального уровня критичности.

Анализ и оценка рисков ИБ выполняется в соответствии с требованиями СТО Газпром 4.2-3-003-2009 [226]. При этом введена только качественная шкала как для оценивания тяжести последствий, так и вероятности реализации угрозы. В целом, это положение можно признать соответствующим требованиям стандарта ISO по управлению рисками ИБ [319]. Также можно отметить, что определенные правила обработки рисков (известные по ISO 27005 как метод

[250] https://www.frc.org.uk/News-and-Events/FRC-Press/Press/2017/August/Sanctions-against-senior-auditor-and-PwC-in-relati.aspx

«4Т»), в целом, могут быть приняты в отрасли, но могут быть применены и дополнительные правила обработки рисков ИБ.

5.4 Разработка метода многошаговой оптимизации аудита ИСМ

5.4.1 Принципы организации гибких аудитов

Рассмотрим несколько основных принципов, на которых строится **новая** концепция гибких аудитов и, соответственно, модель многошаговой оптимизации аудита ИСМ:

1. Вводится понятие интегральной оценки (ИО) ИБ для ОЗ, которая включает определенный групповой показатель оценки всех вынесенных на аудит ИБ вопросов – R_{ISMS}. Этот групповой показатель определяется с помощью частных показателей – R_{PR}, помноженных на их весовые коэффициенты в зависимости от важности процесса в организации ИБ для конкретного ОЗ.
2. После проведения начального (первичного) аудита ИБ по каждому проверяемому процессу оценивается его состояние на предмет соответствия требованиям критериев аудита (стандартам ISO, ГОСТ, СТО и пр.), а также его влияние на ИО ИБ конкретного ОЗ.
3. Последующий аудит ИБ проводится по новому предложенному методу, использующему гибкий подход: наиболее детально и тщательно подвергаются проверке те процессы, по которым на предыдущем аудите выявлены существенные несоответствия (например, в нотации ISO 17021), и которые имеют наибольший приоритет для конкретного ОЗ.
4. Частота и детальность, которая должна быть дифференцирована для различных проверяемых процессов, также связывается с ИО. Например, определенные группы процессов, которые в ИО имеют приоритетное значение (например, в зависимости от модели угроз ИБ ОЗ в соответствии с СТО Газпром СОИБ) подвергаются аудиту более детально и чаще. Процессы, имеющие более низкий приоритет в ИО ИБ ОЗ, проверяются реже и менее детально.
5. Глубина проверки и частота аудита каждый раз определяется в зависимости от приближения функции ИО ИБ ОЗ к установленному целевому

показателю – R_{target} (в пределе, очевидно, равным 100%) для оценки уровня обеспечения ИБ каждого конкретного ОЗ.

Дополнительно отметим важность внедрения нового стандарта по управлению активами – ISO 55000 [322], т.к. многие активы (в «классическом» понимании ISO серии 27001) не управляются так, как надо (в частности, в силу применения устаревших процедур. Например, СТО Газпром СОИБ не оперирует такими активами, как персонал, контрагенты, здания, сооружения, НМА и пр.), некоторые управляются несколькими службами (например, службы связи, ИТ, СКЗ), некоторые – принадлежат иным ДОО в составе ПАО "Газпром" (специальные сооружения, трансформаторные подстанции и пр.). Обратим внимание, проблема экспертного выбора (в частности, так, как показано в [151], стр. 259) касается и повторного выбора как итерационного многократного выбора. Также весьма важно учесть применение данного подхода при ликвидации некоторой конкретной проблемы. Рекомендуется (см. [151], стр. 276) выполнять два этапа – выявление проблемы (в данном случае это означает формирование задачи для аудита ИБ) и анализ собранной информации (в данном случае это означает последовательный подбор аргументов программы аудита ИБ). Аудит ИБ должны «доказать», что выбрано правильное множество стандартов, программа аудита ИБ выполняется корректно.

Также крайне ценно обеспечить для ЛПР (как заказчику любого аудита) получение нового качества системы – эмерджентности, как свойства внутренней целостности (устойчивости, безопасности, надежности и п. [151], стр. 290). Например, при сравнении надежности магнитных носителей необходимо рассмотреть несколько параметров: тип носителя (жесткий диск или ленточный накопитель LTO), скорость чтения (по данным Fujifilm, стандартный диск обеспечивает скорость чтения — 210 Мбайт/с, а LTO7 — 300 Мбайт/с), срок хранения информации (на дисках – до 4 лет, на лентах – 30 лет) и надежность хранения информации (на лентах реже встречаются ошибки хранения: на 200

тыс. картриджей LTO-7 встречается только одна ошибка, а на 20 дисков SATA объемом по 6 ТБ будет по одной ошибке)[251].

В то же время, следует объективно оценивать влияние внешних факторов на корректное выполнение программы аудита ИБ с целью контроля управляемости СлПО. Например, известен случай, когда компании Microsoft не удалось провести инспекцию ИС российского производителя троллейбусов[252]. Более того, Microsoft не смогла доказать свое право на проведение аудита в арбитражном суде Саратовской обл. В суде был представлен контракт, в котором указано, что Microsoft «*имеет право за свой счет проверять соблюдение условий лицензии на продукты*» и компания «Тролза» должна немедленно предоставить независимому аудитору все запрашиваемые сведения, а также доступ к ИС, на которых используется ПО.

Соответственно, применение требований уже внедренного одного стандарта (например, ISO 27001) значительно облегчает решение «типовых» задач безопасности, которые решаются параллельно (учет активов, документирование информации, управление рисками, оценка компетенции и пр.), а, следовательно, должны параллельно проверяться в рамках аудита всех функциональных подсистем в ИСМ организации (например, ISO серии 9001, 50001, 27001 и пр.).

5.4.2 Общие аспекты управления аудитом в ИСМ

С точки зрения управления аудитом в ИСМ важно отметить необходимость решения следующих важных практических задач (далее указаны пункты стандарта ИСО 19011 [20]):

1. Задача выделения ресурсов для программы аудита (5.1):
2. Задача учета факторов, влияющих на глубину программы аудита (5.3);
3. Задача сбора верифицируемой информации (6.4.6);
4. Задача обеспечения специальных знаний и навыков (7.2.3.3).

---

251 http://www.cnews.ru/news/for_print/2017-11-23_v_moskve_zapustili_tsod_na_magnitnyh_lentah_dlya

252 http://www.cnews.ru/news/top/2017-11-08_microsoft_ne_smog_popast_s_auditom_po_k_krupnejshemu

Приведем далее несколько примеров крупнейших утечек[253] и покажем, насколько важными для планирования и общего управления аудитом в ИСМ являются эти примеры с практической точки зрения:

— Сентябрь 2016 г., компания Yahoo! сообщила о взломе и краже данных более 500 млн. пользователей в 2013 г.
— Май 2016 г., компания LinkedIn сообщила, что злоумышленники в 2012 г. получили доступ к персональным данным 100 млн. пользователей.
— Май 2016 г., Time Inc. подтвердила, что похищена база данных электронных адресов и паролей 360 млн. пользователей Myspace.
— Май 2014 г., компания eBay Inc. сообщила о хакерской атаке и попросила 145 млн. пользователей сменить пароли.

Дополнительно отметим, что в ИСМ должны быть приняты к сведению и рекомендации PAS-99 [362], что дополнительно позволяет учесть специфические требования выполнения комбинированных аудитов, учета рисков, гибкого управления объемом программы аудита ИСМ с учетом предшествующих результатов и важности процессов.

В продолжение темы устаревшего оборудования рассмотрим актуальный для 2017 г. анализ атаки Bad Rabbit. Как отмечалось, эпидемия выявила проблему с огромным количеством устаревшего оборудования и ПО, а также халатность со стороны системных администраторов. В частности, о возможности атаки было известно за два месяца до ее начала, но многие не приняли никаких мер (в мае 2017 г). Вскоре после первой волны атаки Bad Rabbit пошла вторая (июль 2017 г.), использовалась та же уязвимость ПО, и снова были серьезные проблемы. И только спустя несколько месяцев в ЕС собираются повышать штрафы за слабые меры киберзащиты[254]. В РФ мониторинг результатов атаки Bad Rabbit выполнял ФинЦЕРТ и публично заявил, что не зафиксировано фактов компрометации ресурсов финансовых организаций[255].

253 http://www.rbc.ru/technology_and_media/13/07/2017/596792f99a7947a7ada72d82?from=newsfeed
254 https://www.kommersant.ru/doc/3428093?from=four_tech
255 https://www.cbr.ru/fincert/fincert04/

В работе Н. Винера приведен характерный пример – сражение кобры и мангусты ([13], стр. 259). Главный вывод, который предлагается из анализа данного сражения в том, что мангуста, в отличие от змеи, выполняет последовательность быстрых точных действий, направленных на достижение единственной цели – вытянуть змею во всю длину и обеспечить для себя доминирование. В конкретном случае многошаговая оптимизация аудита ИБ как раз напоминает такой процесс – постоянный «фокус» на достижение превосходства в противоборстве, разбиение «сражения» на последовательность «мини-циклов» PDCA, достижение доминирования при отражении потенциальных атак на защищаемые активы (см. рисунок 1.7– общую модель аудита ИСМ в Главе 1).

5.4.3 Определение показателей управления процессом аудита ИСМ

Для оценки степени соответствия подсистемы обеспечения ИБ в составе ИСМ предъявляемым требованиям используются частные и групповые показатели ИБ. Как показано в базовом примере (формулы (3.7) – (3.10) в Главе 3), расчет результативности ИСМ может быть принят во внимание как оценка результативности подсистемы ИБ. Например, для целей проведения аудита ИСМ в аспекте обеспечения ИБ предлагается применять показатель результативности ИСМ R_{ISMS}, вычисляемый в каждом цикле k-го аудита по **новой** аддитивной формуле. Весовой коэффициент *i*-го процесса обозначим как – $\boldsymbol{\alpha_i}$ и показатель результативности *i*-го процесса ИБ обозначим как – $R_{PR\,i}$.

$$R_{ISMS} = \varphi \sum_{i=1}^{n} \alpha_i * R_{PR\,i} \qquad (5.1)$$

где:

$\boldsymbol{\varphi}$ – степень охвата, определяемая как отношение $\boldsymbol{r}$ – количества процессов, оцениваемых в каждом цикле k-го аудита к $\boldsymbol{n}$ – общему количеству идентифицированных процессов СМИБ (ИСМ):

$$\varphi = \frac{r}{n}$$

При этом сумма весовых коэффициентов $\boldsymbol{\alpha_i}$ нормируется:

$$\sum_{i=1}^{n} \alpha_i = 1$$

Показатель результативности конкретного *i*-го процесса ИБ R_{PRi}, в свою очередь, вычисляется также по **новой** аддитивной свертке метрик ИБ (*j*-ю метрику ИБ для *i*-го процесса ИБ обозначим как K_{KPIij}, а весовой коэффициент – как β_{ij}). Допускается ситуация, когда количество метрик m не будет одинаковым для разных циклов, соответственно, необходимо говорить об m_i:

$$R_{PR\,i} = \mu \sum_{j=1}^{m} \beta_j * K_{PKI\,j} \qquad (5.2)$$

где:

μ – степень достоверности оценки результативности каждого конкретного процесса аудита $R_{PR\,i}$, оцениваемая в зависимости от вида аудита данного процесса, например:

$$\mu = \begin{cases} 0{,}6 - \text{для аудита 1} - \text{й стороной} \\ 0{,}7 - \text{для аудита 2} - \text{й стороной} \\ 0{,}9 - \text{для аудита 3} - \text{й стороной} \end{cases}$$

При этом сумма весовых коэффициентов β_j нормируется:

$$\sum_{j=1}^{m} \beta_j = 1$$

Сумма весовых коэффициентов частных показателей ИБ, используемых при вычислении группового показателя ИБ, должна быть равной 1, что обеспечивает нормирование всех показателей в аддитивных формулах. Показатель результативности СМИБ R_{ISMS} должен быть в пределе равен 1. В процессе аудита ИСМ постоянное измерение «невязки» текущего для k-го аудита R_{ISMS} измеряется как рассогласование с целевым показателем $R_{ISMStar}$, и крайне важно обеспечить его минимум.

Следовательно, задача оптимизации может быть отнесена к типу задач статической оптимизации для процессов управления, протекающих в установившемся режиме. Необходимо реализовать оптимизационную модель для процесса аудита ИСМ в условиях детерминированных ограничений и задачи многомерной дискретной условной оптимизации:

$$F\ (y)\ \rightarrow max$$

где:

$F\ (y)\ \in\ R^m$,

$f\ (y)\ \in\ R^1$

f (y) – целевая функция ***m***-мерного векторного аргумента ***y***:

$y = (y_1, y_2, y_3, \dots y_m)$

Область допустимых значений: $y\ \in\ D\ \subset R^m$.

Переменные ***m***-мерного векторного аргумента ***y*** могут быть, например, для значимого территориально-распределенного СлПО с внедренной ИСМ (в составе СМИБ) следующими:

— T– длительность аудита ИБ (час.);

— S– плановая стоимость аудита ИБ (руб.);

— O – перечень посещаемых объектов в ходе аудита ИБ;

— V– объем аудита ИБ (количество подразделений на объекте);

— F– перечень функциональных вопросов (чек-лист) в ходе аудита ИБ;

— R_{ISMS} – оценка результативности аудита ИБ.

Рассмотрим пример решения варианта оптимизационной задачи с установленными ограничениями (II-го рода, в виде неравенства):

$$\left.\begin{array}{c} R_{ISMS}\ (S,T,F,V,O) \rightarrow max \\ S < 1000 \\ T < 8 \\ F < 200 \\ V < 10 \\ O < 10 \\ R_{ISMS}\ < 1 \\ S > 0, T > 0, F > 0, V > 0, O > 0, R_{ISMS}\ > 0 \end{array}\right\}$$

Данная постановка оптимизационной задачи в текстовой нотации формулируется как выбор параметров процесса аудита ИБ, при котором достигается максимальная оценка результативности (R_{ISMS}) аудита ИБ при заданных ограничениях плановой стоимости аудита ИБ (S), длительности аудита

ИБ (T), количества посещаемых объектов (O), проверяемых подразделений (V) и перечня функциональных вопросов (F).

По итогам оценки всех процессов аудита, выполняемых в строгом соответствии с программой аудита ИСМ ([362], [20], [21]), заполняется следующая матрица (см. таблицу 5.1).

Таблица 5.1 – Схема размещения результатов аудита процессов ИБ

Аудит / Процесс	1	2	…	k
PR_1	KPI_{11}	KPI_{12}		KPI_{1k}
PR_2	KPI_{21}	KPI_{22}		KPI_{2k}
…	…	…	…	…
PR_i	KPI_{i1}	KPI_{i2}		KPI_{ik}

Представленные выше выкладки для $R_{ISMStar}$ интересно сопоставить с реальными данными, полученными из объективных независимых различных зарубежных источников. В частности, отмечается, что после событий «9-11» в США не было получено никаких существенных данных о подготовке актов терроризма. В официальном правительственном отчете[256] сказано: «*authorizes the government to collect "any tangible things"*». В другом источнике[257] подтверждается, что такие данные собирали 17 правительственных агентств и ничего достоверного не было выявлено, и ничего существенного не было собрано за 7 лет.

При условии равенства всех весовых коэффициентов $\boldsymbol{\beta_{ij}}$ для каждой метрики и двух значений коэффициента достоверности оценки результативности $\boldsymbol{\mu}$ = 0,9 (для аудита 3-й стороной) и $\boldsymbol{\mu}$ = 0,6 (для аудита 1-й стороной), и двух значений коэффициента степени охвата $\boldsymbol{\varphi}$ = 0,1 и $\boldsymbol{\varphi}$ = 0,5, и равных коэффициентов $\boldsymbol{\alpha_i}$ получаем следующее решение (см. рисунок 5.2)

256 http://www.washingtontimes.com/news/2015/may/21/fbi-admits-patriot-act-snooping-powers-didnt-crack/

257 https://www.thenewamerican.com/usnews/constitution/item/20956-fbi-report-adds-fuel-to-fire-over-expiring-patriot-act-snooping-powers

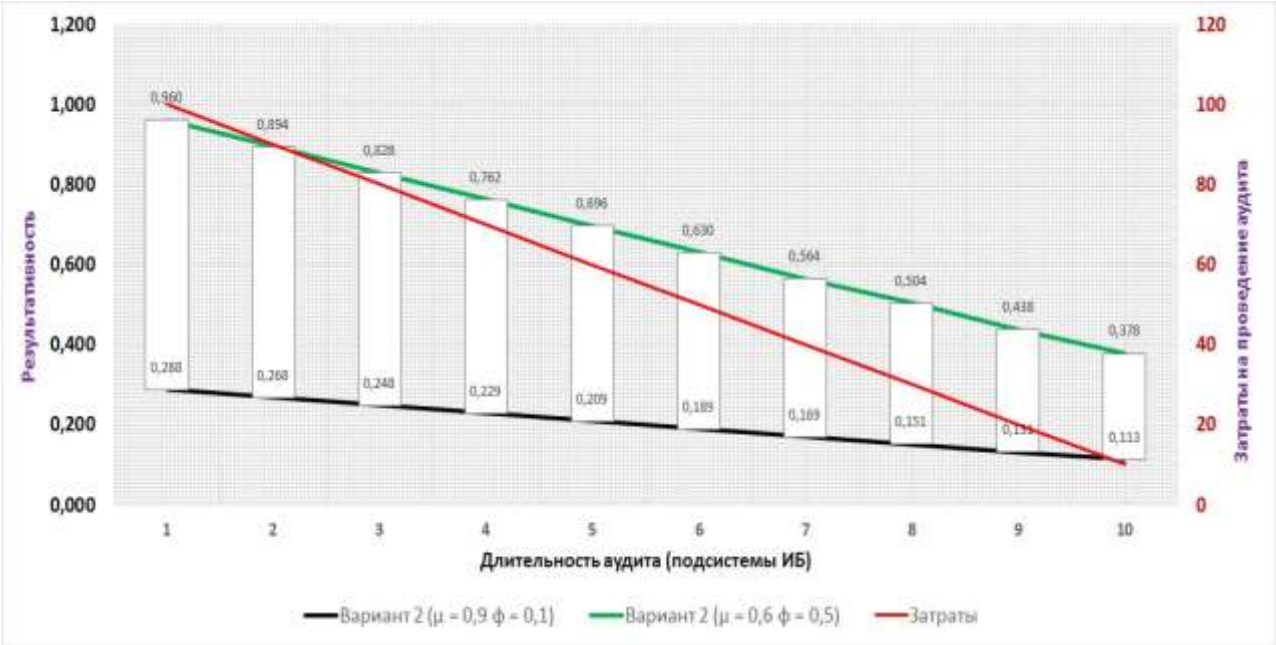


Рисунок 5.2 – Пример решения оптимизационной задачи при одинаковых $\boldsymbol{\beta_{ij}}$

При условии различных весовых коэффициентов $\boldsymbol{\beta_{ij}}$ для каждой метрики и тех же двух значений коэффициента достоверности оценки результативности $\boldsymbol{\mu}$ = 0,9 (для аудита 3-й стороной) и $\boldsymbol{\mu}$ = 0,6 (для аудита 1-й стороной), и тех же двух значений коээфициента степени охвата $\boldsymbol{\varphi}$ = 0,1 и $\boldsymbol{\varphi}$ = 0,5, и равных коэффициентов $\boldsymbol{\alpha_i}$ получаем следующее решение (см. рисунок 5.3)

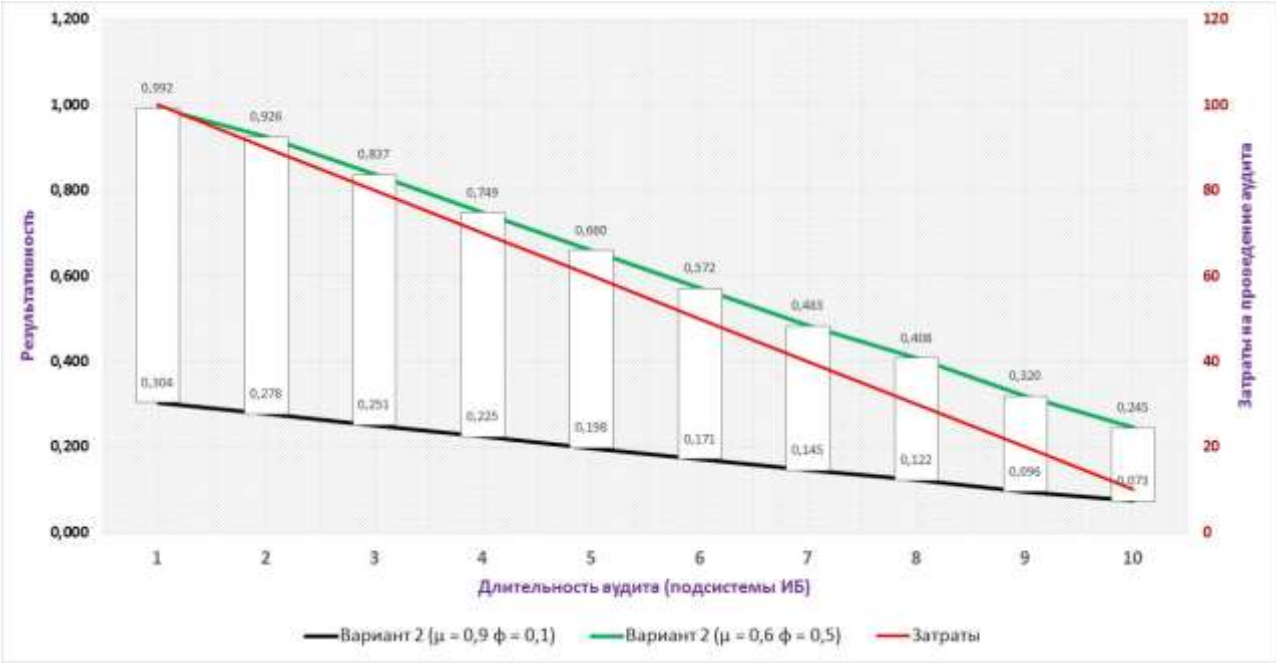


Рисунок 5.3 – Пример решения оптимизационной задачи при разных $\boldsymbol{\beta_{ij}}$

Для более сложных вариантов (несколько подсистем, несколько десятков процессов ИБ, несколько метрик ИБ и пр.) был разработан программный модуль, реализующий решение задач линейного программирования. Примеры расчета для различных значений переменных оптимизации представлены ниже.

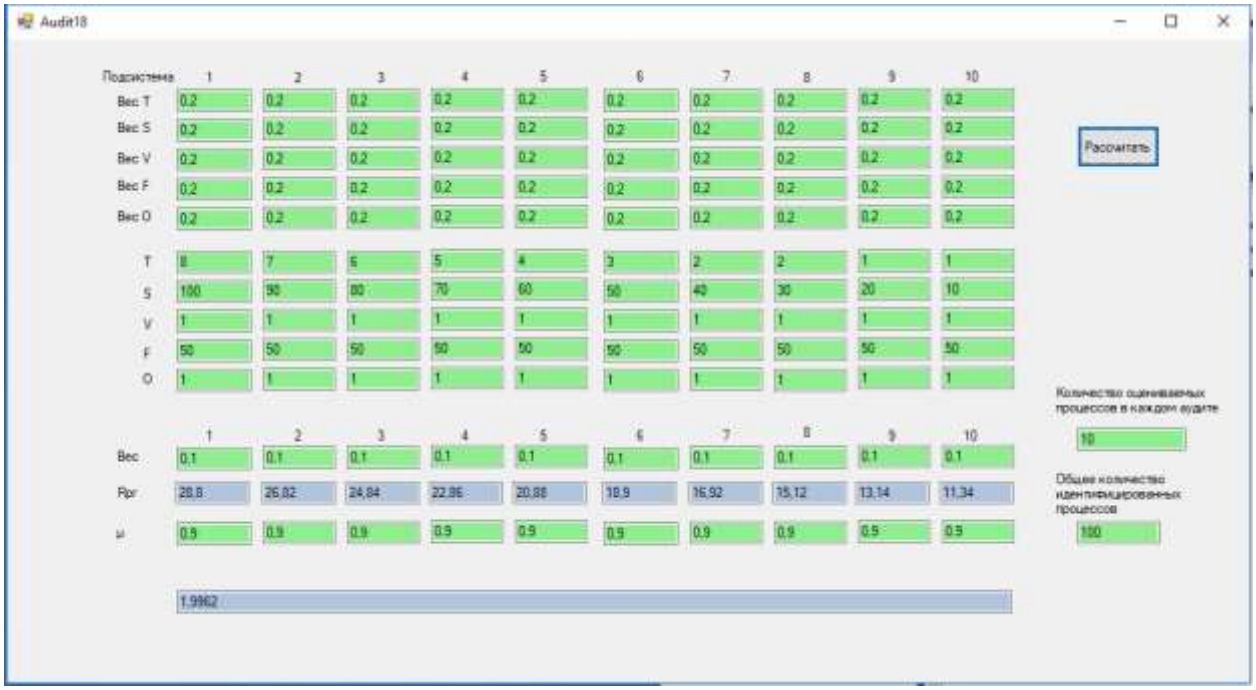


Рисунок 5.4 – Пример решения оптимизационной задачи ($\mu = 0{,}9$, $\varphi = 0{,}1$ и все β_{ij} равны)

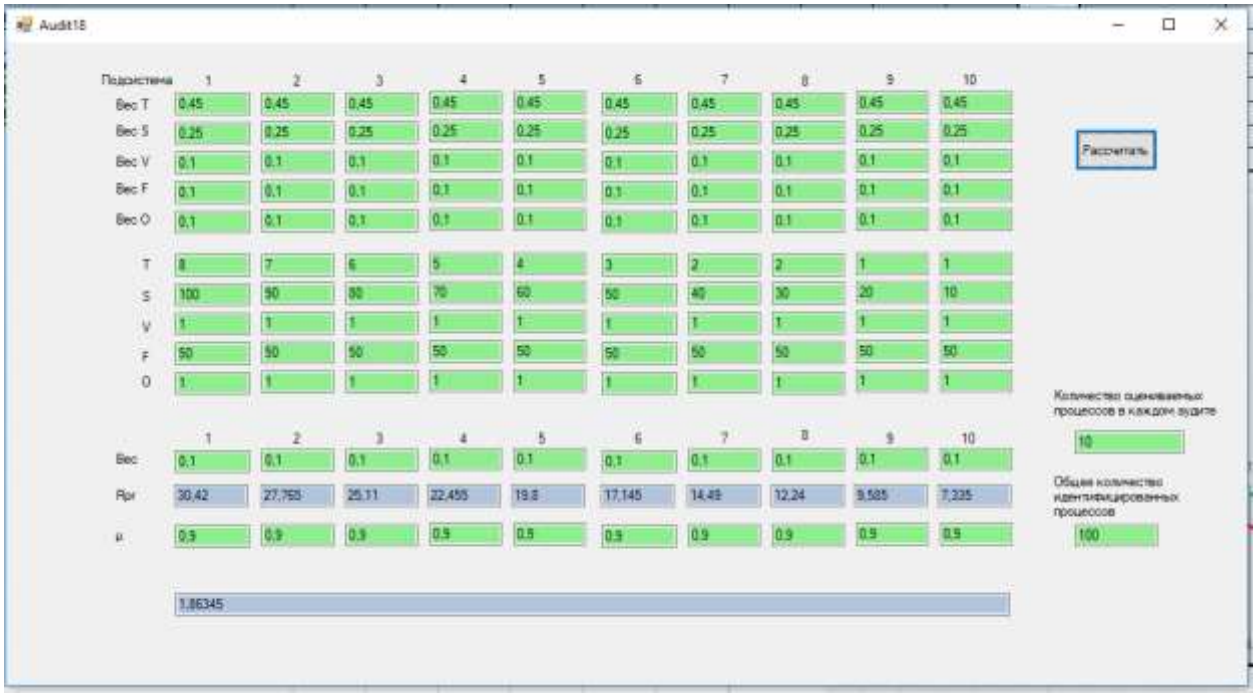


Рисунок 5.5 – Пример решения оптимизационной задачи ($\mu = 0{,}9$, $\varphi = 0{,}1$, и все β_{ij} различные)

5.4.4 Метрики аудита

5.4.5 Метрики для планирования аудита ИСМ

В работе Н. Винера отмечается важность обеспечения обратной связи, для чего необходимы количественные оценки (в оригинальной работе см. [13], стр. 47 говорится о регулировании движения устройства). В конкретном применении для целей аудита ИБ важность именно количественных оценок крайне высока – для оценки характеристик процессов ИБ. Определенно, для проведения аудита ИСМ могут быть предложены метрики, которые будут способствовать получению численных оценок результативности аудита ИБ (см. таблицы 5.2 – 5.4).

Таблица 5.2 – Метрики аудита ИБ и событие ИБ (фрагмент)

Событие ИБ	Пример метрики
Нарушение конфиденциальности	Количество зафиксированных инцидентов ИБ, связанных с утечками информации, имеющей установленный гриф конфиденциальности
Нарушение целостности	Количество зафиксированных инцидентов ИБ, связанных с утечками информации, имеющей установленный гриф конфиденциальности
Нарушение доступности	Количество зафиксированных инцидентов ИБ, связанных с нарушением установленных регламентов доступности (непрерывности), сверх параметров, установленных в SLA
Нарушение неотказуемости	Количество зафиксированных инцидентов ИБ, связанных с отказами от простановки цифровой подписи и/или отказами от приема внешними контрагентами цифровой подписи.

Таблица 5.3 – Метрики аудита ИБ (Оценка последствий событий ИБ)

Последствия событий ИБ	Пример метрики
Время, необходимое для восстановления нормального функционирования оборудования, ПО или средств ИБ	▪ превышение нормативного времени на восстановление ▪ эффект «домино»
Прерывание деятельности организации или отдельного процесса	▪ Время простоя ▪ Финансовые издержки
Нарушение требований внутренних нормативных документов	▪ Количество нарушений ▪ Тяжесть нарушений ▪ Финансовые издержки

Последствия событий ИБ	Пример метрики
Нарушение законодательных или нормативных требований	▪ Количество нарушений ▪ Тяжесть нарушений ▪ Финансовые издержки
Возникновение аварий на производственных объектах	▪ Количество нарушений ▪ Тяжесть нарушений ▪ Финансовые издержки

Таблица 5.4 – Метрики аудита ИБ для оценки мер и средств ИБ

Мера и средство ИБ (*control*)	Пример метрики
Количество уровней защиты	▪ Численная (0 – k)
Вероятность обнаружения уязвимостей	▪ Численная (0 – 1)
Результативность меры и средства ИБ	▪ Численная (0 – 1)
Наличие технической документации, регламентирующей использование меры и средства ИБ	▪ Бинарная («есть», «нет»)
Возможный ущерб при успешной атаке на средства ИБ	▪ Численная
Наличие обслуживающего персонала, имеющего необходимую квалификацию	▪ Бинарная («есть», «нет»)
Результаты контроля выполнения (аудита) меры и средства ИБ	▪ Бинарная («есть», «нет»)

5.4.6 Базовый оптимизационный цикл программы аудита ИСМ

На основании известных стандартов аудита (в частности – [362], [20], [21]) и отраслевых методик (СТО ИББС БР, СТО Газпром СОИБ и пр.), предложим **новый** метод многошаговой оптимизации процесса аудита ИСМ для СлПО, который позволяет обеспечить систему координации, распределения ресурсов и оперативного доведения результатов аудита ИСМ до ЛПР. Предложенный метод заключается в научно обоснованном и целенаправленном оперативном функционировании подсистемы ИБ в составе ИСМ, отличающийся от существующих методов циклической непрерывной оценкой результативности на основе оптимальной системы численных показателей (метрик) ИБ.

Предложенный метод состоит из 2-х циклов оптимизации программы аудита ИБ в ИСМ, отличающихся следующими новациями:

1. Базового оптимизационного цикла, который характеризует эффективное выполнение аудита ИБ в ИСМ в терминах оценки результативности для

каждого PR_i – процесса ИБ и каждой KPI_j – метрики ИБ, а также определяет циклы оптимизации ресурсов в программе аудита: глубины, размера аудиторской выборки, количества привлекаемых аудиторов (технических экспертов) и пр.

2. Быстрого блока оценки результативности мер коррекции и корректирующих действий в текущем k-м аудите, затрагивающих изменения – как следующего процесса, так и следующего в программе (k+1)-го аудита. Также обеспечивается быстрый переход к оценке показателей результативности СМИБ – R_{ISMS} в k-м аудите и (k+1)-м аудите для постоянной и оперативной оптимизации всей программы аудита ИБ.

Рассмотрим базовый оптимизационный цикл программы аудита ИБ в ИСМ, построенный с учетом формальных требований стандартов ISO по аудиту СМ, стандартов ISAGO, стандартов СТО Газпром и СТО БР ИББС, и дополненных **новыми** компонентами (см. рисунок 5.6).

Состав новых компонентов представлен далее:

— Формирование оценок результативности по каждому k-му аудиту.

— Формирование оценок по каждому PR_i – процессу ИБ.

— Формирование оценок по каждой KPI_j – метрики ИБ.

— Оценка ИО уровня обеспечения ИБ.

5.4.7 Описание базового оптимизационного цикла программы аудита ИСМ

Предусловия (входные данные) для старта базового оптимизационного цикла программы аудита ИБ в ИСМ для СлПО представлены далее.

Заданы:

— T_0 – базовый период аудитов ИБ,

— S_0 – базовая (плановая) стоимость аудита ИБ,

— V_0 – базовый объем аудита ИБ (количество подразделений),

— F_0 – базовый перечень функциональных вопросов аудита ИБ,

— O_0 – базовый перечень посещаемых объектов аудита ИБ.

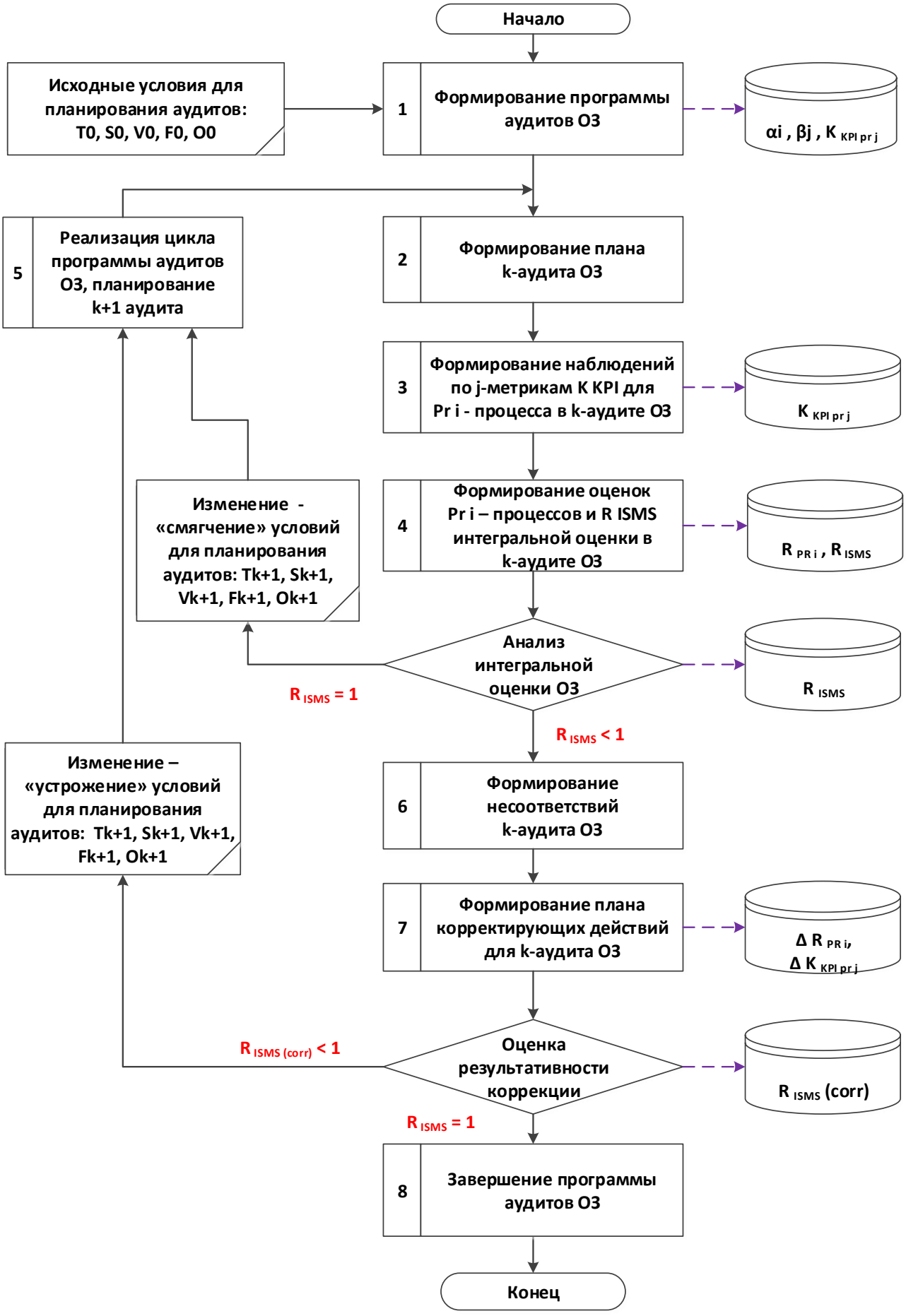


Рисунок 5.6 – Базовый оптимизационный цикл программы аудита ИСМ

Описание базового оптимизационного цикла программы аудита ИБ в ИСМ для СлПО представлено далее по основным шагам.

Шаг 1. Формирование программы аудита, оценивается $R_{ISMS} \geq R_{ISMS\ tar}$ (в соответствии с (5.1) и (5.2)). В результате определяются:

- α – весовой коэффициент для групповой метрики процесса ИБ;
- β – весовой коэффициент для частной метрики процесса ИБ;
- k – количество аудитов ИБ в программе аудита;
- R_{ISMS}– текущая ИО результативности СМИБ;
- $R_{ISMS\ tar}$ – целевая ИО результативности СМИБ;
- γ – количество аудитов в программе аудита;
- Δ – допустимая «невязка» показателя $R_{ISMS\ tar}$;
- $К_{PR\ i}$ – целевой показатель результативности *i*-процесса;
- $К_{KPI\ j}$– целевой показатель результативности *j*-метрики для *i*-процесса

Шаг 2. Формирование плана k-го аудита. В результате утверждается план k-го аудита.

Шаг 3. Выполнение k-го аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 4. Выполняется сбор наблюдений по итогам k-го аудита, соответственно, $К_{PR\ i}$ и $К_{KPI\ j}$. В результате заполняется база данных аудита показателями $К_{PRi}$ и $К_{KPI\ j.}$

Шаг 5. Выполняется формирование оценки R_{ISMS} – интегральной оценки на k-м аудите. В результате заполняется база данных аудита показателем R_{ISMS} для k-го аудита.

Шаг 6. Выполняется оценка степени достижения R_{ISMS} по итогам k-го аудита целевого показателя $R_{ISMS\ tar}$. В результате заполняется база данных аудита показателем R_{ISMS} для k-го аудита.

Шаг 7. В случае, если $R_{ISMS} \geq R_{ISMS\ tar}$, т.е. достигается установленный показатель результативности, выполняется информирование руководителя программы аудита о возможном «смягчении» условий планирования

(k+1)-го аудита. В частности, могут быть снижены частота или объем программы аудита, что, соответственно снизит и затраты на выполнение аудита. Далее переход на шаг 13 к реализации (продолжению) программы аудита, выполнению (k+1)-го аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 8. В случае, если $R_{ISMS} < R_{ISMStar}$, т.е. не достигает установленный показатель результативности, выполняется формирование перечня несоответствий на k-м аудите. Выполнение далее (k+1)-го аудита может быть приостановлено по решению руководителя программы аудита с целью снижения расходов. В результате формируется отчет по итогам k-го аудита.

Шаг 9. На основании сформированного перечня несоответствий на предыдущем шаге формируется план коррекции и корректирующих действий для выявленных несоответствий на k-м аудите. В результате выполняется заполнение базы данных аудита показателями, соответственно, $\Delta К_{PRi}$ и $\Delta К_{KPIj}$ для k-го аудита, который характеризует степени отклонения, соответственно, по целевому показателю PR_i-процесса ИБ в целом и $К_{KPI\ j}$ по отдельным (частным показателям).

Шаг 10. Выполняется оценка результативности коррекции и корректирующих действий по несоответствиям, выявленным по итогам k-го аудита. В результате выполняется заполнение базы данных аудита показателем R_{ISMS} (corr) для k-го аудита.

Шаг 11. В случае, если $R_{ISMS\ (corr)} \geq R_{\ ISMS\ tar}$, т.е. достигается полностью установленный показатель результативности корректирующих мер для всех выявленных несоответствий по итогам k-го аудита, выполняется информирование руководителя программы аудита и, в случае отсутствия иных несоответствий за период реализации корректирующих мер, завершение программы аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 12. В случае, если $R_{ISMS(corr)} < R_{\ ISMS\ tar}$, т.е. не достигается установленный показатель результативности корректирующих мер для всех выявленных несоответствий по итогам k-го аудита, выполняется информирование

руководителя программы аудита о возможном «устрожении» условий планирования аудита. В частности, могут быть увеличены частота или объем программы аудита для тех PR*i*-процессов ИБ, по которым были выявлены несоответствия. Очевидно, это увеличит затраты на выполнение аудита в дальнейшем. Далее переход на шаг 13 к реализации (продолжению) программы аудита, выполнению (k+1)-го аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 13. В случае, если подтверждена результативность корректирующих мер для всех выявленных несоответствий на k-м аудите, выполняется переход к дальнейшей реализации (продолжении) программы аудита и выполнению (k+1)-го аудита.

5.4.8 Детализация базового оптимизационного цикла программы аудита ИСМ

Рассмотрим детализацию базового оптимизационного цикла программы аудита ИБ ИСМ в СлПО с учетом формальных требований стандартов по аудиту (ISO, ISAGO, СТО Газпром), дополненных **новыми** компонентами (см. рисунок 5.7).

5.4.9 Описание детализации базового оптимизационного цикла программы аудита ИСМ

Предусловия (входные данные) для старта детализированного базового оптимизационного цикла программы аудита ИБ ИСМ в СлПО представлены далее.

Заданы:

— T_0 – базовый период аудитов ИБ,

— S_0 – базовая (плановая) стоимость аудита ИБ,

— V_0 – базовый объем аудита ИБ (количество подразделений),

— F_0 – базовый перечень функциональных вопросов аудита ИБ,

— O_0 – базовый перечень посещаемых объектов аудита ИБ.

Дополнительно заданы:

— ожидания ЛПР по срокам реализации мер коррекции,

— оценки ЛПР по градациям несоответствий,

— перечень несоответствий, переданный из базового цикла.

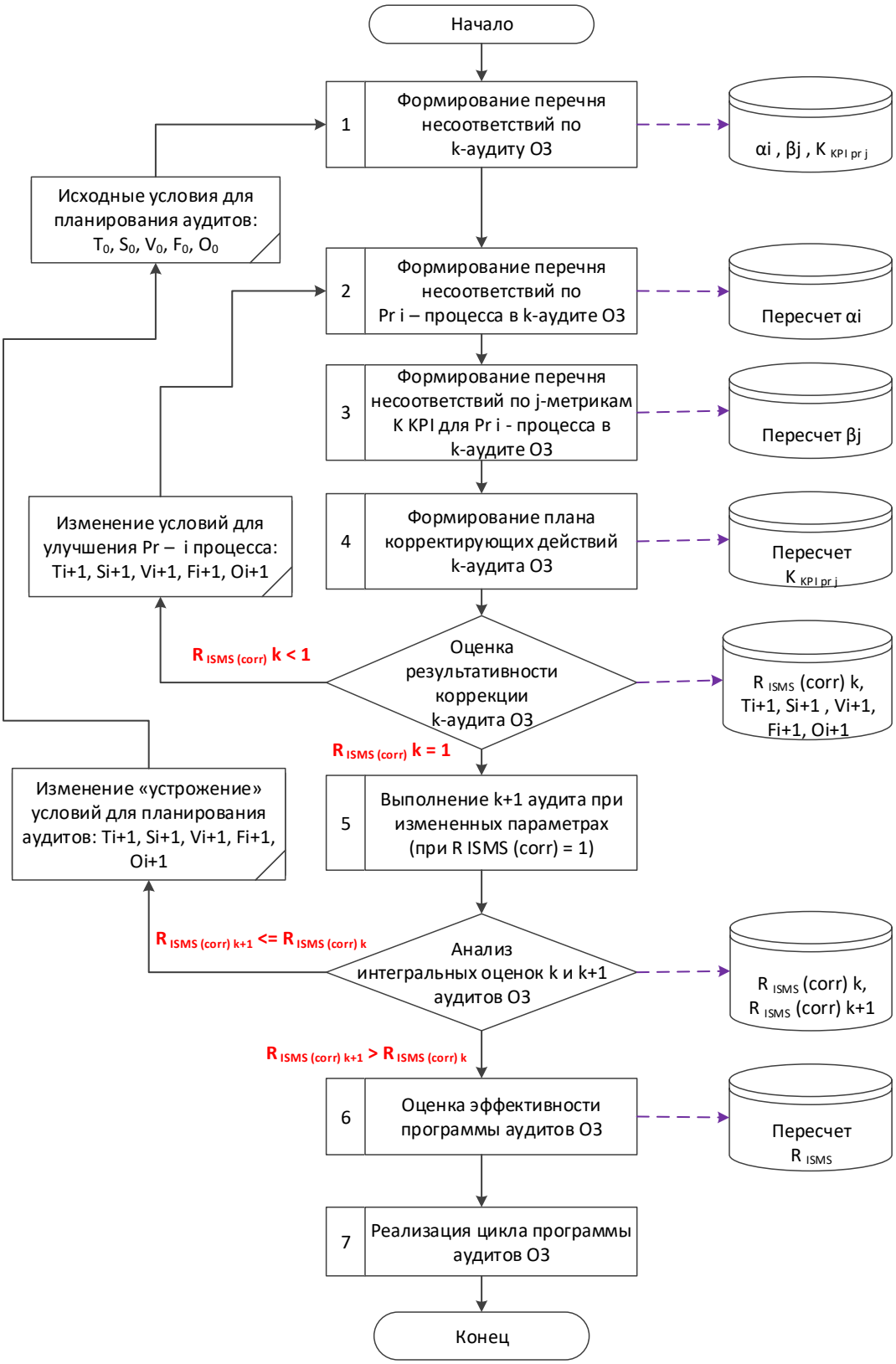


Рисунок 5.7 – Детализация базового оптимизационного цикла программы аудита ИСМ

Описание детализированного базового оптимизационного цикла программы аудита ИБ ИСМ в СлПО представлено далее по основным шагам.

Шаг 1. Формирование программы аудита. В результате определяются:

— α – весовой коэффициент для групповой метрики процесса ИБ;

— β – весовой коэффициент для частной метрики процесса ИБ;

— k – количество аудитов ИБ в программе аудита ОЗ;

— R_{ISMS}– текущая ИО результативности СМИБ;

— $R_{ISMS}\ tar$ – целевая ИО результативности СМИБ;

— γ – количество аудитов в программе аудита;

— Δ – допустимая «невязка» показателя $R_{ISMS\ tar}$;

— $К_{PR\ i}$ – целевой показатель результативности j-процесса;

— $К_{KPI\ j}$– целевой показатель результативности i-метрики для j-процесса

Шаг 2. В случае выявленных несоответствий по установленным (базовым) критериям аудита, формируется перечень несоответствий k-го аудита. В результате формируется перечень несоответствий k-го аудита.

Шаг 3. Каждое выявленное несоответствие последовательно соотносится с определенным PRi-процессом ИБ. В результате выполняется пересчет весовых коэффициентов (групповых) α PRi-процессов ИБ. Заполнение базы данных аудита новым показателем α.

Шаг 4. Каждое выявленное несоответствие последовательно соотносится с j-метрикой и показателем $К_{PRi}$ по определенному PRi-процессу ИБ. В результате выполняется пересчет весовых коэффициентов (частных) β для метрик PRi-процессов ИБ. Заполнение базы данных аудита новым показателем β

Шаг 5. Выполняется формирование плана корректирующих действий по k-му аудиту. В результате выполняется пересчет PRi–целевого показателя результативности i–го процесса. Заполнение базы данных аудита новым показателем $К_{PR\ i.}$

Шаг 6. Выполняется оценка результативности коррекции и корректирующих действий по несоответствиям, выявленным по итогам k-го аудита. В результате

выполняется заполнение базы данных аудита показателем R_{ISMS} (corr) для k-аудита и новыми значениями T_j , S_j , V_j , F_j , O_j

Шаг 7. В случае, если $R_{ISMS\ (corr)} < R_{ISMS\ tar}$, т.е. для k-аудита не достигается установленный показатель результативности корректирующих мер для всех выявленных несоответствий, выполняется информирование руководителя программы аудита о возможном «устрожении» условий планирования аудита. В частности, могут быть увеличены частота или объем программы аудита для тех PR_j-процессов ИБ, по которым были выявлены несоответствия. Очевидно, это увеличит затраты на выполнение аудита в дальнейшем. Далее переход на шаг 5 к формированию плана корректирующих действий для k-го аудита и пересмотра групповых (α) и частных (β) коэффициентов для каждого несоответствия. В результате формируется отчет по итогам k-го аудита.

Шаг 8. В случае, если $R_{ISMS\ (corr)} \geq R_{ISMS\ tar}$, т.е. для k-го аудита достигается установленный показатель результативности корректирующих мер для всех выявленных несоответствий, выполняется реализация следующего по программе аудита: (k+1)-го аудита с учетом новых измененных параметров по итогам успешной реализации корректирующих действий по предыдущему k-му аудиту. В результате формируется отчет по итогам k-го аудита.

Шаг 9. Выполняется анализ интегральных оценок для k и (k+1) аудита соответственно: $R_{ISMS(corr)\ k}$, и $R_{ISMS\ (corr)\ k+1}$. В результате заполняется база данных аудита показателем R_{ISMS} (corr) $_{k}$ для k-го аудита и R_{ISMS} (corr) $_{k+1}$ для (k+1)-го аудита.

Шаг 10. В случае, если $R_{ISMS(corr)\ k+1} <= R_{ISMS\ (corr)\ k}$, выполняется информирование руководителя программы аудита о возможном «устрожении» условий планирования аудита. В частности, могут быть увеличены частота или объем программы аудита для тех PR_j -процессов ИБ, по которым были выявлены несоответствия. Очевидно, это увеличит затраты на выполнение аудита в дальнейшем. Далее переход на шаг 5 к формированию плана корректирующих действий для k-го аудита и пересмотра групповых (α) и частных (β)

коэффициентов для каждого несоответствия. В результате формируется отчет по итогам k-го аудита.

Шаг 11. В случае, если R_{ISMS} (corr) $_{k+1}$ > R_{ISMS} (corr) $_{k}$, выполняется информирование руководителя программы аудита о возможном возврате к базовым условиям планирования аудита. Далее переход на шаг 5 к формированию плана корректирующих действий для (k+1)-го аудита и пересмотра групповых (α) и частных (β) коэффициентов для каждого несоответствия. В результате формируется отчет по итогам k-го аудита.

Шаг 12. В случае повышения уровня результативности программы $R_{ISMS\ (corr)\ k+1} > R_{ISMS\ (corr)k}$ выполняется оценка программы аудита в целом, в том числе – в экономическом аспекте (минимизация S-параметра). В результате формируется отчет по итогам k-го аудита.

Предложенный метод оптимизации программы аудита ИБ в ИСМ для СлПО основана на современных риск-ориентированных стандартах и позволяет обеспечить постоянную оптимизацию процесса выполнения проверок (аудита) ИБ на основе гибких связанных адаптивных алгоритмов.

Экспериментальная проверка предложенного метода проведена в период 2014-2016 гг. при выполнении проектов в ООО «Газинформсервис» (в Приложении предоставлен акт внедрения). Применение указанных конкретных блоков оптимизации в методе для иных ИСМ может, вероятно, потребовать иных параметров (например, при выборе в качестве критериев ИБ иных отраслевых стандартов или иного количества и состава векторного аргумента оптимизации)[258]. Частично это предположение подтверждается в отчете Центра стратегических разработок[259].

5.5 Пример кейсов для расчета по модели аудита ИСМ

5.5.1 Проблемы управления документированной информацией

Рассмотрим кейс на примере аудита одного из важнейших процессов в ИСМ (в составе СМК, СМИБ и СУУ) для СлПО – управления документированной

---

258 https://www.securitylab.ru/news/490527.php

259 https://www.csr.ru/issledovaniya/runet-v-rezhime-informatsionnoj-bezopasnosti-dialog-ili-izolyatsiya/

информацией в проектах в ИТСК (в Приложении предоставлен акт внедрения). Известны следующие основные наблюдения:

1. Не установлен порядок предоставления и формы отчетности (нарушение требований ISO 9001:2008 (п. 7.6) и ISO/IEC 20000:1-2011 (п. 4.3).
2. Не определена процедура мониторинга процесса предоставления услуг (нарушение требований ISO/IEC 20000:1-2011 (п. 4.3) и ISO/IEC 20000:2-2005 (п. 6.1.3).
3. Не определен порядок оценки удовлетворенности заказчика услугами (нарушение требований Cobit 4.1 (DS1, ME1) и ITIL v.3 (ST 4.1.7);

5.5.2 Проблемы управления программой аудита ИСМ

В практике аудитора известны следующие основные типовые ошибки, выявляемые при экспертизе договоров (на соответствие ISO 20000:1):

1. Не установлен исчерпывающий перечень требуемых атрибутов, предоставляемых сервисов по договору.
2. Не установлен полный перечень контролируемых параметров услуг.
3. Не установлена схема эскалации обращений.
4. Не указаны точные реквизиты коммуникации Исполнителя.

Рассмотрим примеры оценки наблюдений аудита (категорируемых как несоответствия и наблюдения в соответствии с [20], [21]). Результаты анализа СМК показывают по каждому процессу стандарта ISO 9001 динамику несоответствий и наблюдений – потенциальных несоответствий, если не предпринимать корректирующих действий (см. рисунок 5.8).

Ценность данного кейса в том, что прослеживается прямая зависимость между основными ошибками в управлении и последующими проблемами в выделении ресурсов и, соответственно, в процессах оказания услуг. Приведенный выше пример находит свое подтверждение в наши дни, например, инцидент с доступностью известного сервиса аутсорсинга «Битрикс 24». В 2018 г. в результате серьезного сбоя около 30% пользователей «Битрикс 24» в России столкнулись с длительными перебоями в работе сервиса[260]. Причина сбоя

[260] http://www.news.ru/news/top/2018-02-09_ruhnuvshij_bitriks_24_paralizoval_rabotu_svoih

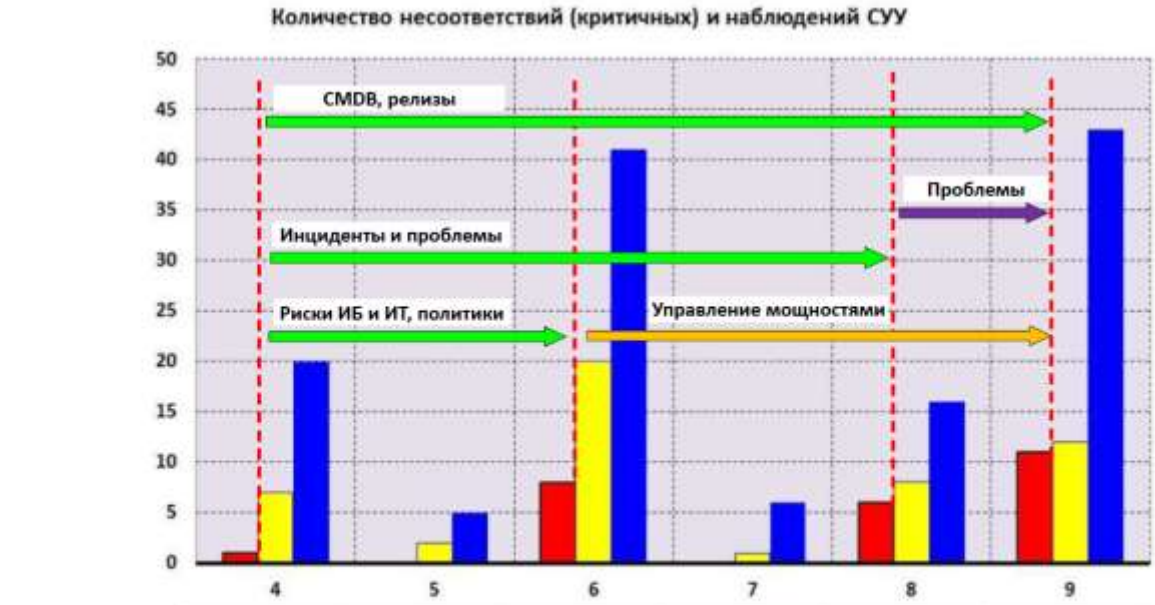
заключалась в отказе сетевого оборудования уже другой компании: «Корп софт», которая являлась хостинг-провайдером сервиса «Битрикс 24». Есть данные, что, несмотря на все заранее предпринятые меры по обеспечению бесперебойной работы инфраструктуры, из-за ошибки проектирования сети у провайдера сломался коммутатор, который вывел из строя оба зарезервированных дата-центра.

	4	5	6	7	8
Кол-во н/с	4	6	6	12	2
Кол-во набл.	12	3	7	20	0

Рисунок 5.8 – Оценка несоответствий и наблюдений по разделам ISO 9001

Результаты оценки наблюдений аудита СУУ показывают по каждому процессу стандарта ISO 20000:1 динамику несоответствий (критичных и некритичных) и наблюдений – потенциальных несоответствий, если не предпринимать корректирующих действий (см. рисунок 5.9).

Ценность данного кейса в том, что прослеживается прямая зависимость между ошибками в управлении (делегирования полномочий), недостаточного внимания к управлению рисками и последующими проблемами при появлении инцидентов и проблем в процессах оказания услуг.



	4	5	6	7	8	9
Кол-во кр. н/с	1	0	8	0	6	11
Кол-во н/с	7	2	20	1	8	12
Кол-во набл.	20	5	41	6	16	43

Рисунок 5.9 – Оценка критичных несоответствий по разделам ISO 20000:1

Отметим, что в работе И. Пригожина и И. Стенгерс [150] отмечено: «*По Аристотелю, живые существа не подчиняются никаким законам. Их деятельность обусловлена их собственными автономными внутренними причинами*». Достаточно интересно проследить этот тезис с точки зрения «полезности» именно механизма внутренних аудитов для оценки отклонений. В указанной выше работе И. Пригожина и И. Стенгерс [150] отмечены труды Лукреция, Лейбница, Тагора и др., посвященные формированию оценки отклонений самого различного типа: «*клинамена*», поведения монарха, вариантов ведения «открытого диалога» и пр.

В определенном смысле, в работе И. Пригожина и И. Стенгерс [150] открывается новый класс сложных процессов – «микрособытий». Подчеркивается, что это «микрособытие» может описывать небольшую модификацию, в пределе – получение нового качества (более высокой скорости воспроизведения и иных характеристик популяции, в примере теории возникновения видов Ч. Дарвина). В качестве подтверждения реализации «*собственных автономных причин*» (по Аристотелю) рассмотрим результаты

утечки приватных данных из Facebook[261]. В результате глава службы ИБ покинул компанию по причине конфликта при рассоедовании, а команду, которая вела расследование под руководством ИБ-директора, сократили со 120 до 3 сотрудников[262].

Дополнительно рассмотрим кейс распределения несоответствий по циклам PDCA для представленных выше примеров аудита ИСМ (в составе СМК и СУУ). Результаты представлены в таблице 5.5.

Таблица 5.5 – Распределение несоответствий аудита ИСМ по фазам PDCA

Фаза	Пример несоответствия (фрагмент)
Plan (План)	Не предоставлено объективных свидетельств достижения установленных целей (CSI = 4,05), т.к. последовательно 2 ежемесячных протокола за январь и февраль 2013 г. содержат оценку 3,8 (без достаточной мотивировки со стороны Заказчика), кроме того, фактически CSI вычисляется по 4 факторам вместо установленных 5.
Do (Делай)	Не обеспечивается распределение руководством ответственности и полномочий в рамках подразделения, на аудите выявлены несколько фактов подписания актов (апрель и февраль 2013 г.) по договору № XXX сотрудником, формально не имеющим доверенности
Check (Проверяй)	Не выполнено требование анализа способности выполнить установленные потребности Заказчика (отчет по критичному инциденту по обращению SD_XXX от 04.03.2013). Инцидент зафиксирован по инструкции XXX, документ не подписан со стороны заказчика с 2011 г., но требуется к исполнению.
Act (Действуй)	На аудите выявлены факты, когда выполняется мониторинг «тикетов» (ticket) в системе оператора, но, тем не менее, по этим объектам мониторинга далее подаются претензии (например, по инциденту ticket XXX, АЗС-X) или простои АЗС-XX (50 час.), при согласованном уровне 4 часа привели к претензии № XXX от 06.02.2013.

Примеры аналитических выкладок по результатам оптимизации процесса управления документированной информацией показаны на рисунке 5.10 (пример снижения объема сверхплановых инструкций с 438 до 25) и на рисунке 5.11 (пример снижения несоответствий по иным разделам стандарта ИСО 9001

261 https://www.securitylab.ru/blog/company/securityinform/343548.php
262 https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

версии 2008 после оптимизации процесса управления документированной информацией), соответственно.

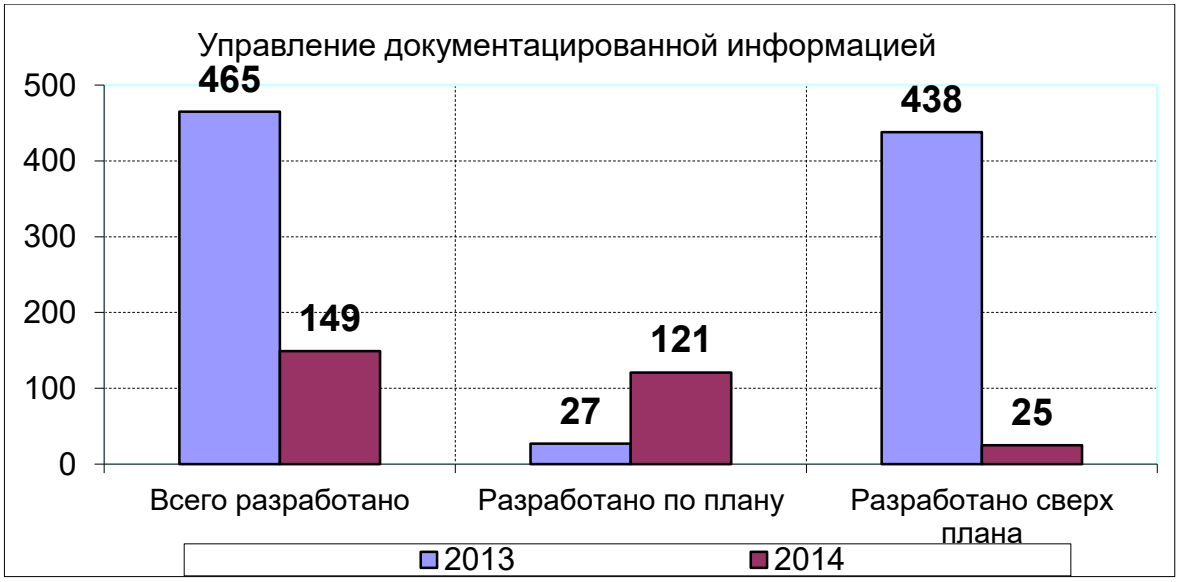


Рисунок 5.10 – Оценка процесса управления документированной информацией

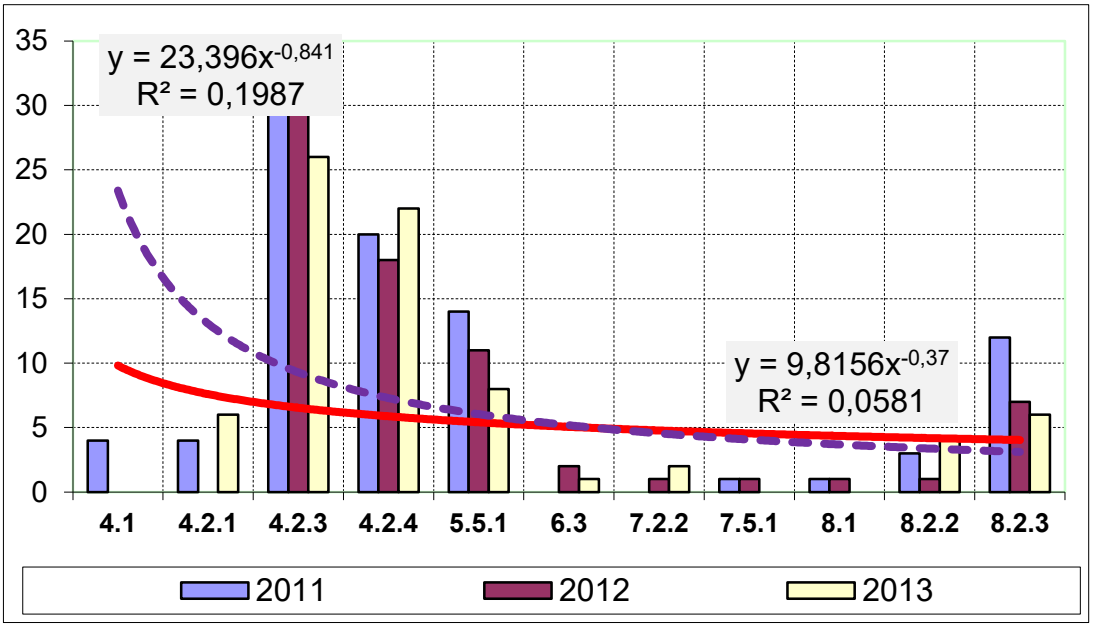


Рисунок 5.11 – Внутренняя оценка распределения несоответствий по процессам

5.5.3 Сложности формирования метода измерения результативности ИСМ

Сложности формирования метода измерений результативности ИСМ заключаются в том, что требуется, минимально:

1. Сформировать метод измерения, дающий воспроизводимые и достоверные результаты оценки.

2. Предложить метод сравнения с мерой (различных разновидностей – дифференциальный, замещения, дополнения, совпадения и пр.).
3. Доказать ЛПР, что выделенный бюджет на ИСМ позволяет достигать поставленных задач, в том числе, и в области обеспечения ИБ.
4. Определить перечень применяемых средств измерений, алгоритмов обработки результатов измерений и оценки показателей точности.

Очевидно, формируемый метод выполнения измерений СМИБ как подсистемы ИБ в составе ИСМ, должна объективно оценивать все аспекты ИБ со стороны заинтересованных сторон. Для процесса формирования, анализа и сравнения метрик ИБ «базовым» является применение «целевого» стандарта ISO 27001 [317]. Ниже представлен метод измерения результативности ИБ и пример формирования численных показателей (метрик ИБ) для выполнения независимой оценки [317], [20], [311].

5.5.4 Необходимые термины и определения

Для решения поставленной проблемы рассмотрим несколько необходимых терминов из [28], [316], [94]:

1. Событие информационной безопасности (*information security event*). Отметим, что это определение совпадает по п. 3.5 в [28] и по п. 3.2 [315].
2. Инцидент информационной безопасности (*information security incide*nt): (п. 3.3. по [315]). Но в стандарте [28] представлено иное определение (п. 3.6. по [28]).

Обратим внимание, что «целевой» стандарт по сертификации СМИБ 27001 [317] трактует термин «инцидент ИБ» иначе, чем стандарт по управлению инцидентами ИБ – ГОСТ ИСО 18044 [28]. Прежде всего, стандарт [28] устанавливает четкую логическую последовательность – инцидент ИБ является следствием событий ИБ. В то же время, определение по [28] объективно более емкое – дает четкую «привязку» на бизнес-активы и угрозы ИБ, что подразумевает некоторый «операционный» анализ, выполняемый в организации, исходя из внутренних потребностей и целей ИБ.

Обратим внимание, что эксперт А.В. Полещук ([98]) рекомендует следующее практическое разделение событий ИБ и инцидентов ИБ:

1. События ИБ (компрометация паролей, НСД, нарушение доступа);
2. Инциденты ИБ (вирусные заражения, отказ в обслуживании, утрата оборудования).

Следующие термины важны для ясного и однозначного понимания «предмета измерения». Исторически оценка СМ формируется как количественное отношение, предполагающее получение величин, сравниваемых в количественных шкалах [28]. Но в ряде проектов в практике аудита ИБ наблюдалась подмена понятий, отчасти связанная с неоднозначностью английского перевода терминов. Выполним расчет результативности СМИБ в точном соответствии в терминах по ГОСТ Р, в котором приведены следующие два термина:

3. Результативность (*effectiveness*) (п. 3.2.14);
4. Эффективность (*efficiency*): (п. 3.2.15).

В методическом плане представляется рациональным говорить именно об оценке результативности ИСМ, т.к. для оценки эффективности нужно оперировать ресурсами: финансовыми параметрами деятельности организации и динамикой их изменения (бюджет службы ИБ, штатная численность, стоимость ТС, внешние услуги и пр.).

5.5.5 Ключевые сущности при расчете результативности ИСМ

Одной из основных задач ИСМ является управление инцидентами ИБ. Эта задача решается следующим образом:

- обнаружение событий ИБ и их дальнейшая обработка с целью выявления инцидентов ИБ,
- оценка инцидентов ИБ с целью выработки соответствующих мер реагирования,
- своевременное предотвращение возможных негативных воздействий и оперативное восстановление инфраструктуры после инцидента,
- внесение необходимых изменений в политики ИБ.

Обнаружение событий ИБ должно осуществляться работниками структурных подразделений организации или автоматически с помощью ТС. Источниками информации о событии ИБ, как правило, являются:

— сообщения от различных ТС и СрЗИ, таких, как системы обнаружения вторжения IDS/IPS, DLP, защиты от вредоносного ПО, МЭ и др.,

— обращения внешних организаций (например, аудиторов).

Для оценки результативности ИСМ необходимо выполнять последовательный анализ всей информации, которая может поступать от ТС, сотрудников компании, подрядчиков и иных третьих лиц. В новом способе расчета результативности ИСМ применяются 3 ключевые сущности [98]:

1. Событие;
2. Событие ИБ;
3. Инцидент ИБ.

5.5.6 Установленные предположения для сущностей

Практическая реализация выбранных ключевых сущностей для оценки результативности ИСМ требует фиксации определенных предположений:

1. **Событие** – любое изменение установленного состояния контролируемых объектов. (event, alert, «сработка» ТС и/или СрЗИ). Важно, что событие всегда «идентифицировано», т.е. является материальным фактом, может быть извлечено, проанализировано «оператором», передано на дальнейшую обработку, протестировано на стенде и пр. Важно также, что событие само по себе не приводит к угрозам ИБ, тем более – к ущербу ИБ (бизнесу). Предполагается, что число событий может быть велико и достигать нескольких тысяч в день. Это обстоятельство накладывает ограничения на «глубину» архива и временной лимит для анализа (обработки) «сырых» событий со стороны оператора. *Должно выполняться*: Кол-во событий > 0.
2. **Событие ИБ** – результат анализа множества «сырых» событий со стороны оператора. Важно, что в качестве событий ИБ могут выступать записи аудита, которые также являются фиксированными событиями (см. выше).

Предполагается, что по факту события ИБ может быть предпринято расследование (при эскалации как инцидент ИБ). Предполагается, что число событий ИБ может достигать сотни в год. *Должно выполняться*: Кол-во событий > Кол-во событий ИБ.

3. **Инцидент ИБ** – в нотации ГОСТ 18044 [28] это следствие проявления событий ИБ, что возможно приведет к компрометации бизнеса или угрозе ИБ. Важно, что инцидент является именно следствием события ИБ, на основании решения оператора по итогам анализа события ИБ. По инциденту ИБ всегда проводится расследование с отражением факта преодоления (попытки) существующих мер обеспечения ИБ (*controls*), оценке конкретного ущерба ИБ. Предполагается, что число инцидентов ИБ может достигать десятков в год. *Должно выполняться*: Кол-во событий ИБ > Кол-во инцидентов ИБ.

5.5.7 Установленные дополнительные ограничения для сущностей

Практическая реализация выбранных сущностей требует фиксации дополнительных ограничений [98]:

1. Область сертификации (*scope*).
2. Временной интервал.
3. Техническая возможность.
4. Оператор.
5. Норма результативности
6. Зрелость СМИБ.

5.5.8 Формулы расчета результативности ИБ

С учетом сказанного выше, для недавно введенной в эксплуатацию подсистемы ИБ в составе ИСМ, еще не прошедшей полный сертификационный цикл, предлагается следующая формула расчетов:

$$\text{К смиб} = \left(\mathbf{1} - \left(\frac{\text{И иб}}{\text{С иб}}\right)\right) * \mathbf{100\%} \qquad (5.3)$$

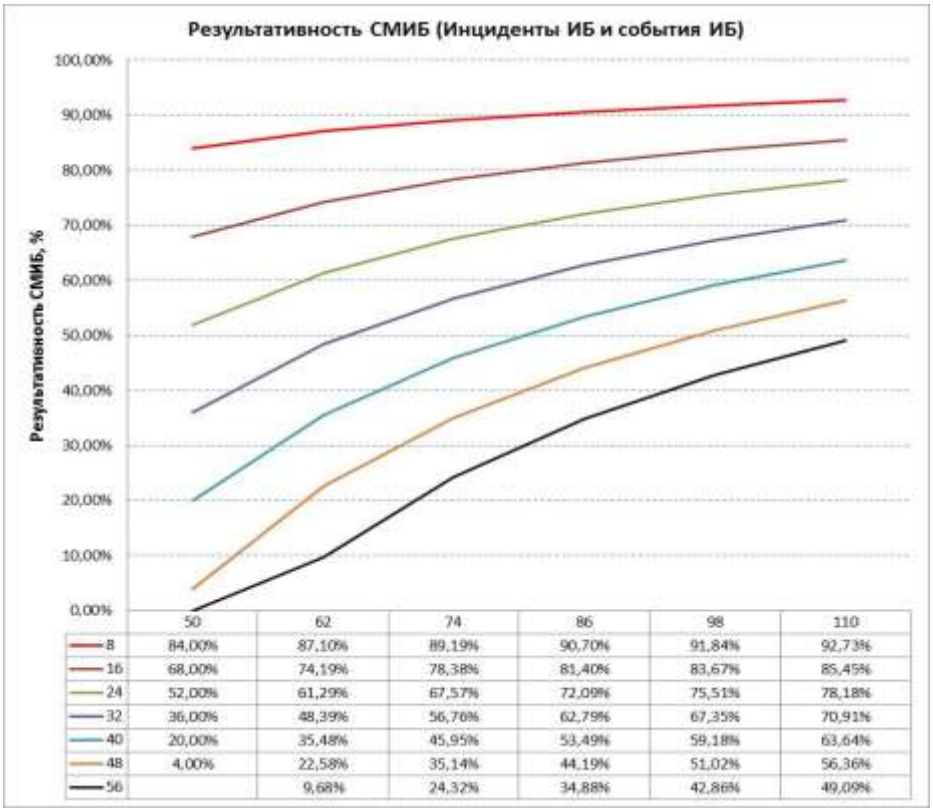
где:

$\text{К}_{\text{смиб}}$ – коэффициент результативности ИСМ;

И **ИБ** – идентифицированное количество событий ИБ;

С **ИБ** – идентифицированное количество инцидентов ИБ.

Формула (5.3), иначе называемая [98] «*мешок на мешок*», позволяет быстро оценить результативность ИСМ в текущей конфигурации *scope*, т.е. насколько ИСМ позволяет выявлять критичные с позиции бизнес-операций и угроз ИБ события (в нотации стандарта [28]). Формула (5.3) позволяет сопоставлять отношения по состоянию до внедрения подсистемы ИБ в ИСМ и любой последующий год. К недостаткам формулы (5.3) следует отнести ситуации (с ненулевой вероятностью), при которой СМИБ в текущей конфигурации не сможет идентифицировать события ИБ, которые, тем не менее, могут привести к инциденту ИБ. На рисунке 5.12 показан пример расчета результативности СМИБ по базовой формуле (5.3).



	50	62	74	86	98	110
8	84,00%	87,10%	89,19%	90,70%	91,84%	92,73%
16	68,00%	74,19%	78,38%	81,40%	83,67%	85,45%
24	52,00%	61,29%	67,57%	72,09%	75,51%	78,18%
32	36,00%	48,39%	56,76%	62,79%	67,35%	70,91%
40	20,00%	35,48%	45,95%	53,49%	59,18%	63,64%
48	4,00%	22,58%	35,14%	44,19%	51,02%	56,36%
56		9,68%	24,32%	34,88%	42,86%	49,09%

Рисунок 5.12 – Расчет результативности СМИБ по формуле (5.3).

Обратим внимание, что снижение $И_{ИБ}$ объективно приводит к повышению предложенной оценки результативности ИСМ, как фактор снижения (предотвращения ущерба организации).

Для СМИБ (и ИСМ), стоящих на более высоком уровне зрелости, можно рекомендовать к применению более сложные формулы, учитывающие раздельно события ИБ и инциденты ИБ. В этом варианте особую роль приобретает техническая оснащенность «оператора», о чем указывалось выше. В частности, реализованный в ИСМ комплекс ТС (*control*) должен позволять «селектировать» из многих тысяч событий в режиме, близком к РРВ, события, относящиеся к сотрудникам одной службы, даже если они находятся, предположим, в разных подсетях (VLAN). Соответственно, результативность ИСМ рассчитывается следующим образом:

Расчет результативности событий ИБ:

$$К\,с = \left(\mathbf{1} - \left(\frac{С\ тек.}{С\ max}\right)\right) * \mathbf{100\%} \qquad (5.4)$$

где:

Кс – коэффициент результативности по идентификации событий ИБ;

С***тек*** – идентифицированное количество событий ИБ;

С***max*** – максимально возможное количество событий ИБ за предыдущий период.

Расчет результативности инцидентов ИБ:

$$К\,и = \left(\mathbf{1} - \left(\frac{И\ тек.}{И\ max}\right)\right) * \mathbf{100\%} \qquad (5.5)$$

где:

Ки – коэффициент результативности по идентификации инцидентов ИБ;

И***тек*** – идентифицированное количество инцидентов ИБ;

И***max*** – максимально возможное количество инцидентов ИБ за предыдущий период.

С учетом положений (5.4) и (5.5), общий показатель результативности ИСМ рассчитывается следующим образом:

$$К\,смиб = (К\,с * \boldsymbol{\alpha} + К\,и * \boldsymbol{\beta}) \qquad (5.6)$$

где:

К смиб – общий показатель результативности СМИБ,

Кс – коэффициент результативности по идентификации событий ИБ,

Ки – коэффициент результативности по идентификации инцидентов ИБ,

α – весовой коэффициент для определения важности идентификации Кс,

β – весовой коэффициент для определения важности идентификации Ки.

Формула (5.6) обладает рядом особенностей:

1. При С***тек*** = 0 и И***тек*** = 0 получаем абсолютный 100% уровень ИБ, несмотря на ведущийся «лог» многочисленных «сырых» событий. Если «оператор» не выделил события ИБ (нет возможных нарушений ИБ) и не определил инциденты ИБ (нет ущерба ИБ или компрометации бизнес-процессов).
2. Весовые коэффициенты α и β нормируются к единице (α + β = 1) и определяют для конкретного объекта (процесса СМИБ) значимость событий и инцидентов ИБ. В простейшем случае α = β = 0,5.
3. Возможна раздельная предварительная проверка Кс и Ки на установленное «пороговое» значение, например, 10%. Если «пороговое» значение не превышено, переходим к расчету по формуле (5.6). Если «пороговое» значение по формулам (5.4) и (5.5) превышено, необходимо уточнить правила идентификации событий ИБ и/или инцидентов ИБ из «сырого» множества всех событий «оператором».

5.5.9 Примеры кейсов для расчета результативности ИСМ

Рассмотрим несколько практических примеров расчета результативности СМИБ по формуле (5.6) для случая зрелой СМИБ. Предположим также, что ЛПР поставил задачу обеспечить повышение результативности СМИБ на 10% за определенный период.

Кейс 1.

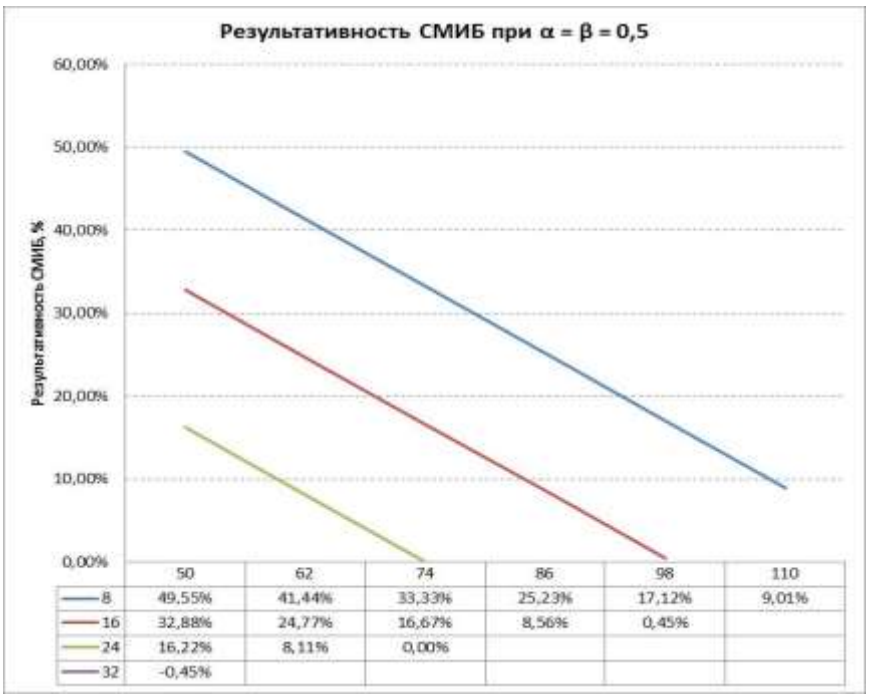
Для С***тек*** = 54, С ***max*** = 60, И***тек*** = 18 и И***max*** = 21, α = β = 0,5 получаем:

Проверка: Кс = 10,0 % ≥ 10 % - пороговое значение выполняется;

Ки = 14,28 % ≥ 10 % - пороговое значение выполняется;

$$\text{К смиб} = \left(\left(\mathbf{1} - \left(\frac{\mathbf{54}}{\mathbf{60}}\right) * \mathbf{100\%}\right) * \mathbf{0,5} + \left(\mathbf{1} - \left(\frac{\mathbf{18}}{\mathbf{21}}\right) * \mathbf{100\%}\right) * \mathbf{0,5}\right) = \mathbf{12,14\%}$$

На рисунке 5.13 показан пример расчета результативности СМИБ по формуле (5.6) для кейса 1.



	50	62	74	86	98	110
8	49,55%	41,44%	33,33%	25,23%	17,12%	9,01%
16	32,88%	24,77%	16,67%	8,56%	0,45%	
24	16,22%	8,11%	0,00%			
32	-0,45%					

Рисунок 5.13 – Расчет результативности СМИБ по формуле (5.6), Кейс 1.

Обратим внимание, что раздельное определение результативности для инцидентов ИБ и событий ИБ позволяет достаточно просто решать поставленную высшим руководством организации задачу перед службой ИБ. Например, если поставлена задача обеспечить К **смиб** ≥ 10 %, то возможно несколько допустимых решений, например, обеспечить менее 24 инцидентов ИБ при 50 событиях ИБ, или менее 16 инцидентов ИБ при 62 событиях ИБ и пр.

Кейс 2.

Для С***тек*** = 70, С ***max*** = 60, И ***тех***. = 18 и И ***max*** = 23, α = 0,3 β = 0,7 получаем:

Проверка: Кс = - 16,66 % ≤ 10 % - пороговое значение не выполняется;

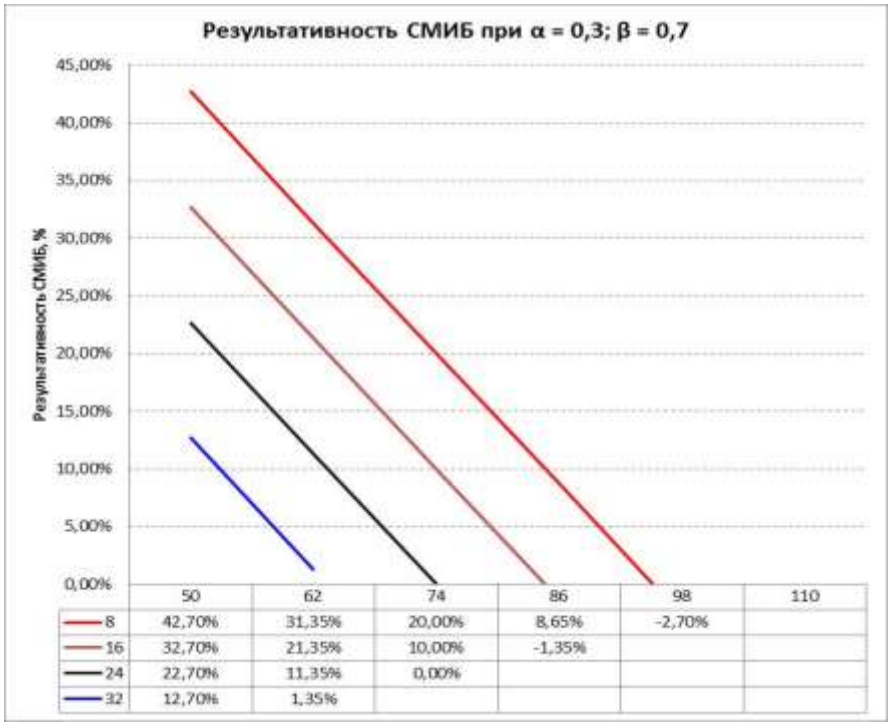
Ки = 21,73 % ≥ 10 % - пороговое значение выполняется;

$$\text{К смиб} = \left(\left(\mathbf{1} - \left(\frac{\mathbf{70}}{\mathbf{60}}\right) * \mathbf{100\%}\right) * \mathbf{0,3} + \left(\mathbf{1} - \left(\frac{\mathbf{18}}{\mathbf{23}}\right) * \mathbf{100\%}\right) * \mathbf{0,7}\right) = \mathbf{-5 + 15,21 = 10,21\ \%}$$

На рисунке 5.14 показан пример расчета результативности СМИБ по формуле (5.6) для кейса 2.

Обратим внимание, что раздельное определение результативности для инцидентов ИБ и событий ИБ, а также изменение весовых коэффициентов α = 0,3 и β = 0,7 существенно меняет общий расчет результативности СМИБ. Явное «внимание» высшего руководства к событиям ИБ приводит к резкому

«подъему» кривых оценки результативности в графике, тем самым «отрезая» приемлемые варианты (при той же поставленной задаче обеспечить К **смиб** ≥ 10 %) в области свыше 86 зарегистрированных событий ИБ.



	50	62	74	86	98	110
8	42,70%	31,35%	20,00%	8,65%	-2,70%	
16	32,70%	21,35%	10,00%	-1,35%		
24	22,70%	11,35%	0,00%			
32	12,70%	1,35%				

Рисунок 5.14 – Расчет результативности СМИБ по формуле (5.6), Кейс 2.

В то же время при малом количестве событий ИБ (например, 50) возможно получить значения результативности СМИБ, слабо зависящие от количества зарегистрированных инцидентов ИБ. Применение весовых коэффициентов в предложенной формуле (5.6) позволяет обеспечить выполнение цели по повышению результативности СМИБ (например, 10%) даже при отрицательной результативности одной из компонент, отражая реальную важность для высшего руководства – конкретное снижение количества инцидентов ИБ.

5.5.10 Дополнительные метрики ИБ для оценки результативности СМИБ

С целью снижения издержек (это одна из приоритетных задач любого бизнеса и наиболее «презентабельная» форма оценки результативности деятельности службы ИБ), могут быть применены метрики, показывающие степень достижения возможного максимума (плана продаж, выполнения в срок проектов и пр.) [98]. Соответственно, могут быть предложены различные типы метрик (более подробно см. Главу 3):

— Простые метрики (например, количество выявленных инцидентов и событий ИБ, количество предотвращенных утечек ПДн, количество проведенных по плану аудита ИБ);

— Сложные метрики (например, отношение стоимости мер защиты к стоимости защищаемых активов);

— Комплексные метрики (например, число произошедших инцидентов ИБ, приведших к ущербу (вынужденному простою) в ИС, определенных как критичные для бизнеса).

В качестве практических метрик ИБ дополнительно рекомендуются к применению:

— Кс = (1 – С тек * 100% / С макс) – для оценки динамики событий ИБ,

— Кр = (1 – Кс (повторных) * 100% / Кс) – для оценки динамики повторных событий ИБ (рецидив),

— Кд = (С макс – С тек) / (К макс – К тек) – для оценки динамики приращений событий ИБ и инцидентов ИБ.

5.6 Выводы к Главе 5

1. Предложен **новый** метод многошаговой оптимизации процесса аудита ИБ в ИСМ для СлПО, который позволяет обеспечить систему координации, распределения ресурсов и оперативного доведения результатов аудита ИБ в ИСМ для ЛПР. Предложенный метод заключается в научно обоснованном и целенаправленном функционировании подсистемы ИБ в составе ИСМ, **отличающийся** от существующих методов непрерывной оценкой результативности на основе оптимальной системы численных показателей (метрик) ИБ.
2. При аудите СМИБ (ИСМ) в соответствии с множеством требований (отраслевых, национальных и международных стандартов), необходимо учитывать и уникальные отраслевые особенности – например, с помощью весовых коэффициентов в аддитивных критериях. В этом случае, как было показано в кейсах, существует сложность выделения по значимости какой-либо сущности, группы активов или набора ТС, влияющих на результаты аудита ИБ и совокупную оценку результативности СМИБ (ИСМ).
3. Для оценки результативности СМИБ (ИСМ) необходимо обеспечить ЛПР в процессе реализации программы аудита ИБ достоверными и удобными для анализа численными метриками ИБ. Оценки результативности СМИБ явным образом влияют на изменение статуса службы ИБ и соответствующего оснащения (бюджета). Предоставление «слабых» оценок ИБ по итогам программы аудита может быть расценено как несоответствие роли службы ИБ для обеспечения успешного достижения бизнес-целей организации.
4. При обеспечении постоянного повышения результативности СМИБ необходимо формировать сопоставимые метрики ИБ, которые позволят оценить сделанные предварительно предположения. Система удобных, сопоставимых и воспроизводимых метрик ИБ позволит сформировать обоснованные цели СМИБ (ИСМ), направленные на обеспечение стабильного развития бизнеса организации.

6 Глава. Имитационное моделирование ИСМ СлПО на примере АК

6.1 Общие положения

Представленные выше теоретические и научно-практические положения нуждаются в оценке адекватности практического применения с целью подтверждения корректности сделанных предположений, установленных допущений и возможности использования моделей и методов аудита ИСМ для СлПО и последующего анализа результатов апробации. В зарубежной литературе приводятся различные подходы к практической оценке математических методов и моделей для описания поведения объектов самой различной природы и уровня сложности ([352], [353], [368], [301], [277]).

В качестве инструмента практической апробации представленных положений результатов предлагается метод имитационного моделирования на модели СлПО – международных АК. Выбор именно данного объекта моделирования обусловлен:

— длительным периодом наблюдения за данным типом объекта – 4 года (с 2012 по 2015 гг. включительно);
— независимым моделированием для увеличения объективности одновременно для двух похожих объектов исследования – АК в Алматы (код ИКАО ALA) и АК в Астане (код ИКАО TSE);
— строгим соблюдением политики конфиденциальности при проведении любого аудита. Дополнительно при моделировании сформированы полностью независимые группы для проведения аудита ИСМ;
— публичным обсуждением результатов моделирования после завершения полностью принятого 3-х летнего цикла аудита и получения раздельных объективных свидетельств [105].

Отметим, что при расследовании авиационных происшествий МАК[263] публикует официальный протокол. В частности, по итогам расследования катастрофы в аэропорту Внуково самолета «Фалкон» с главой компании

---

263 http://www.mak-iac.org/rassledovaniya/falcon-50ex-f-glsa-20-10-2014#115676

«Тоталь» на борту, было определено следующее: «*Подключение второго входа монитора подсистемы обзора и контроля летного поля А3000 на рабочем месте РПА для отображения метеоинформации, что не предусмотрено руководством по эксплуатации подсистемы. При выборе на автоматизированном рабочем месте отображения метеоинформации, радиолокационная информация и световые сигналы тревоги (в процессе аварийного взлета сигнал тревоги был сформирован системой),* ***становятся недоступны*** *для специалиста, находящегося на рабочем месте РПА»;*

Отметим еще один факт, отражающий печальные итоги формального соответствия требованиям в авиационной отрасли. По результатам банкротства компании «ВИМ-Авиа» обнаружилось, она формально соответствовала разработанным в 2008 г. и принятым в 2009 г. новым Федеральным авиационным правилам. Реакция Президента РФ В.В. Путина была соответствующей: «*Если вы выработали такие критерии, то чего они стоят, если ничего не видно за ними? Критериям соответствует, а работать не может. Десятки тысяч людей оказались в очень сложной ситуации*»[264]. Далее будут представлены дополнительно общие данные по известным средствам автоматизации оценки соответствия (не только аудита СМ и/или ИСМ) класса GRC (Governance, Risk, Compliance), доступных на коммерческом рынке и позиционируемых как лидеров рынка средств оценки рисков, управления аудитом и соблюдения соответствия в области ИБ ([293], [373], [384], [375]).

6.2 Известные подходы к оперативной оценке уровня ИБ

На конференциях «Информационная безопасность АСУ ТП КВО» (2015 – 2018 гг.) в докладах экспертов заявлены различные подходы к сбору, анализу и оценке данных для КВО. В частности, отметим доклад «Интеллектуальная система сбора и анализа данных для прогнозирования нештатных ситуаций АСУ ТП КВО» (Гордейчук, ПВЭиФ), доклад «Вопросы динамического моделирования процессов смены исходных состояний системы» (Кульба В.В.) и доклад «Исчисление рисков не мерой вероятности, а мерой опасности»

[264] https://www.kommersant.ru/doc/3422944

(Малинецкий Г.Г.). На V Форуме АЗИ «Актуальные вопросы информационной безопасности» были представлены доклады, посвященные вопросам оперативного анализа текущего уровня безопасности. Например, в докладе «Аспекты безопасности АСУ ТП в отдельных отраслях промышленности» (Даренский, «Информзащита») показаны оценки и статистика инцидентов АСУТП[265]. Актуальные вопросы аудита были подняты в докладе «Рациональный дизайн архитектуры системы защиты АСУ ТП» (Стефанов, «Элвис-Плюс»). Отмечается, что необходимо понимать как способы и инструменты аудита, так и представление результатов (визуализация)[266]. В докладе «Автоматизация процессов ИБ на базе RSA Archer» (Вакациенко, RSA) представлен подход по управлению инцидентами ИБ с позиции представителя разработчика[267]. На конференции «Рускрипто-2016»[268] в докладе С.Агеева и И.Саенко отмечено использование функции риска и ряда метрик, в том числе:

- FAR (вероятность ложной тревоги, *False Acceptance Rate),*
- FRR (вероятность пропуска цели, *False Rejection Rate*).

Следует отметить доклад А.Чечулина, М.Коломеец и И.Котенко «Применение новых методов визуализации для отображения метрик безопасности компьютерной сети». На различных форумах эксперты представляют современный методологический аппарат (основанный на стандартах ISO, NIST, ISAGO, IGA и пр.) и готовы предоставить средства визуализации и быстрого моделирования СМИБ (ИСМ) для ЛПР. Безусловно, наличие «электронной инструментальной панели» («*dashboard»*) повышает осведомленность высшего руководства и помогает ЛПР принимать оперативные решения, а также снижает, в определенной степени, уровень рисков ИБ (пример того, как нужно обеспечивать осведомленность, представлен в обзоре RSA[269]). Однако, с учетом актуальных проблем обеспечения ИБ представляется более важным предоставить ЛПР инструмент не только «следящий», но и

---

265 http://forum-azi.ru/files/files/2016/05%20darensky.pdf
266 http://forum-azi.ru/files/files/2016/06%20stefanov.pdf
267 http://forum-azi.ru/files/files/2016/08%20vakacienko.pdf
268 http://www.ruscrypto.ru/accotiation/archive/rc2016/
269 http://blogs.rsa.com/what-your-business-can-learn-from-wannacry/

«предупреждающий», позволяющий моделировать особенности реализации СрЗИ, перечень функций ИБ, частные параметры СМИБ (ИСМ) и – как вершина системы – гарантировать требуемый уровень ИБ в организации. В качестве комментария рассмотрим статистику 2017 г. компании PwC[270]. По данным статистики более 9 тыс. глав IT-служб из 122 стран (в том числе 248 компаний из РФ), в 40% респондентов из России признали отсутствие в компаниях общей стратегии ИБ (во всем мире — 44%).

6.3 Системы класса GRC

6.3.1 Модели оценки соответствия в автоматизированных системах

Для оценки соответствия могут применяться различные АС, позволяющие ускорить как процесс управления общей программой аудита, так и способствовать (в определенной мере) повышению качества принимаемых решений ЛПР. В качестве примера рассмотрим решения, реализующие некоторые полезные функции, в частности – оценку соответствия (*“compliance”* в терминах стандартов [317], [315]).

6.3.2 Платформы для создания GRC-решений

В настоящее время известно несколько специализированных зарубежных платформ для создания систем уровня GRC: RSA Archer GRC, MetricStream GRC Platform, Rsam GRC Platform, Nasdaq OMX BWise и др. Также известны и ряд отечественных проектов, в частности: Eplat4m (разработка компания КИТ) и Security GRC[271] (разработка компании RVision) [373], [366]. Некоторое функциональное описание представлено на следующих площадках[272]. Тем не менее, в некоторых работах отмечается весьма скромная роль средств автоматизации, в частности, «*человек выполняет именно те операции, которые не поддаются формализации*» ([151], стр. 12), что в целом позволяет оставить задачи «пересчета» для средств автоматизации, а принятие решений, выполнение экспертных оценок на основе сравнения различных альтернатив оставить человеку. Также следует стремиться к снижению количества

---

270 https://www.kommersant.ru/doc/3461367

271 http://forum-azi.ru/files/files/2016/10%20smetanev.pdf

272 https://vimeo.com/160718681

альтернатив для сравнения, а также к снижению общей «вариативности» для вынесения ЛПР суждения в рамках управления СлПО. В частности, можно привести пример работы академика Федорова Е.С. ([151], стр. 23), где отмечено существование только 230 разных типов кристаллических решеток, хотя известна способность самых разных веществ в природе кристаллизоваться при определенных внешних условиях.

Описание платформы RSA Archer eGRC

Решение RSA Archer eGRC версии 5.5 предназначено для стратегического управления, управления рисками и соответствия требованиям регуляторов, которые поддерживают работу ИТ-отделов, финансовых, операционных и юридических служб ([373]). Программная архитектура RSA Archer eGRC построена по трехуровневой модели:

— клиентский уровень;

— сервер приложений;

— СУБД.

Оценка применимости платформы RSA Archer eGRC

Одним из ключевых факторов, который разработчики систем класса GRC приводят в поддержку своих систем, является возможность управлять значительным количеством изменений. Действительно, для выполнения аудита вообще, а для аудита ИБ тем более, это обстоятельство выглядит крайне интересно. По данным Михаэля Расмуссена (GRC) в 2008 г. было внесено более 8700 ключевых изменений в банковской отрасли, а в 2012 г. свыше 17000[273]. На сайте RSA приводятся факты возможной реализации соответствия и для стандартов серии ISO 27001[274]. На основании указанных выше источников ([373], [384], [375]), а также отчета «The Total Economic Impact Of RSA Archer IT GRC»[275], проведем краткий анализ примера проекта экономической рентабельности систем класса GRC за 3-х летний период, представленный

273 http://www.emc.com/collateral/solution-overview/h12373-2013-archer-grc-summit-key-findings.pdf
274 http://www.emc.com/collateral/data-sheet/isms-data-sheet.pdf
275 https://emcinformation.com/78203/REG/.ashx?reg_src=videolp

Forrester Research[276]. В данном отчете обследовано свыше 100 компаний энергетики, свыше 500 сервисных финансовых компаний. Указаны следующие статьи обязательных затрат, например:

- обязательное начальное обследование due diligence;
- закупка лицензий – 450 тыс. долл. за годовую лицензию;
- обязательное обучение по 40 часов – 36 тыс. долл.;
- обязательное сервисное сопровождение – 135 тыс. долл.;

Всего общие затраты за год составили 1,437 млн. долл., причем отмечается, что эти затраты только для блока ИТ и риск-менеджмента. Далее приводятся данные, что решение GRC при внедрении только для блока ИТ «*за счет более высокой ИБ эффективности*» обеспечивает экономию до 10 млн. долл. за 3 года. И сверх этого – за счет «*снижения последствий рисков*» – до 24 тыс. долл. и за счет «*снижения использования ПО третьих поставщиков*» – до 300 тыс. долл. за 3 года. Соответственно, при вложениях в проект 721 тыс. долл. показан доход 22 млн. долл., ROI составляет 763 %, а срок окупаемости до 12 мес.

6.3.3 Решение Oracle GRC Platform

В решении Oracle GRC Platform декларируется реализация следующих ключевых преимуществ [293]:

- Предотвращение утечек значимых материальных активов;
- Качественный и надежный способ формирования отчетов в Oracle;
- Гибкая система смены владельцев ИТ активов и управления доступом;
- Ускоренная и усиленная система контроля безопасности доступа;
- Усиленный внутренний аудит для снижения рисков соответствия (compliance);

Отмечается, что решение Oracle GRC Platform обеспечивает существенное снижение стоимости проведения аудита, в т.ч. аудита безопасности и формальных проверок, в частности, на соответствие требований SOX и формального соответствия (*compliance*) [293].

---

[276] http://securityresponse.symantec.com/content/en/us/enterprise/articles/b-forrester_it_gov_risk_compliance_57691_q42011.en-us.pdf

6.3.4 Решение SAP BusinessObjects GRC

В решении SAP BusinessObjects GRC декларируется реализация высокоуровневых функций управления и контроля доступа к корпоративной SAP системе. Отдельные аспекты управления рисками представлены на рисунке 6.1.

Рисунок 6.1 – Определение рисков и мониторинг целостности данных

Также указано, что предоставляется поддержка областей внутреннего контроля, внутреннего и внешнего аудита и управления технологическими процессами и рисками.

6.3.5 Решение Accelus GRC Enterprise Solutions

В решении Accelus GRC Enterprise Solutions декларируется реализация ряда возможностей функций внутреннего аудита [293]:

— Обеспечение визуализации и прозрачности управления процесса GRC;

— Мониторинг и отслеживание правил регулярных изменений;

— Смягчение риска в отношениях между клиентами;

— Идентификация и снижение законодательных и деловых рисков;

— Управление эффективностью политик безопасности и управления;

— Управление аудитом, рисками и процессами внутреннего контроля.

6.3.6 Решение OpenPages

В решении OpenPages декларируется реализация следующих функций при управлении операционными рисками и аудитом [293]:

— Идентификация, управление, мониторинг;

— Предоставление высокоуровневых отчетов;

— Оценка рисков и самооценка (внутренний аудит);

— Анализ сценариев и управления по KPI;

— Оценка специфических и критических ИТ рисков;

— Управление планированием внутренних аудитов для бизнес-линий;

— Автоматизация рабочей среды и предоставления отчетности.

6.3.7 Решение eplat4m GRC

Решение eplat4m GRC (разработка КИТ) представляет собой программный комплекс, обеспечивающий автоматизацию процессов ИБ и их интеграцию в СУ (в определенном смысле, можно говорить о ИСМ)[277]. Назначение eplat4m GRC состоит, в частности, в предоставлении информации в графическом, табличном и ином удобном виде[278].

Решение eplat4m GRC состоит из модулей:

— управление ИТ-активами в части ИБ;

— управление рисками ИБ;

— управление инцидентами ИБ;

— работа с персоналом и третьими сторонами по вопросам ИБ;

— управление соответствием требованиям ИБ;

— управление непрерывностью ИТ;

— отображение геоинформации.

6.3.8 Решение Security GRC RVision

Российская разработка RVision[279] относится к классу Security GRC и позволяет выполнять проверки на соответствие различных нормативных документов (см. таблицу 6.1). Решение Security GRC позволяет решать задачи по контролю активов, управлению рисками, обеспечения соответствия требованиям законодательства, управлению инцидентами ИБ[280]. R-Vision GRC имеет

---

277 http://www.ussc.ru/catalog/id/76

278 http://www.ussc.ru/user_files/tiny_doc/f0043cac3d7249910ec6bc7c9d661e3e.pdf

279 https://rvision.pro/product/

280 http://forum-azi.ru/files/files/2016/10%20smetanev.pdf

модульную структуру и обеспечивает реализацию определенного процесса ИБ[281]. Дополнительно отметим, что проведена экспертиза функциональных требований к центру мониторинга ГосСОПКА[282] и возможностей продукта RVision, по результатам которой сделан вывод, что данное решение, в целом, позволяет обеспечить выполнение 48% рекомендаций (функций ГосСОПКА)[283].

В системе RVision возможно выполнение «инструментального» аудита, который позволяет получать оценки и сопоставления степени выполнения требований для различных физических устройств (см. рисунок 6.2).

№-п/пп	Критерий	Сетевые устройства					
		Cisco 3945	Cisco ASA Intranet	Cisco ASA Internet	Cisco ASA MRSK	Outside Router	Voice router
	Подключение к сети Интернет	Нет	Нет	Да	Да	Да	Нет
	Remote Access VPN	Нет	Нет	Нет	Да	Да	Нет
1	Устаревшая версия ОС	15.1(4)M4 28 Марта 2011	8.2(3) 06 Августа 2010	8.2(3) 06 августа 2010	8.4(7) 30 Августа 2012	12.4(25f) 10 Августа 2011	15.3(4)M3 07 Ноября 2012
2	Графическое управление без шифрования	Да	Нет	Нет	Нет	Да	Да
3	Командное управление без шифрования	Да	Да	Нет	Нет	Нет	Нет
4	Разрыв сессии	Да (60 мин.)	Да (60 мин.)	Да (60 мин.)	Да (60 мин.)	Нет	Нет
5	Блокировка учетных записей при подборе паролей	Нет	Неприменимо	Неприменимо	Неприменимо	Нет	Нет
6	Отказоустойчивость	Нет	Да (горячий резерв)	Нет	Нет	Нет	Нет
7	Дублирование линий связи	Нет	Нет	Нет	Нет	Нет	Нет
8	Ограничение на подключение для управления по IP-адресам	Нет (подключение возможно с любого адреса)	Да, но слишком большие сети	Да	Да	Да	Да
9	Централизованная аутентификация	Нет	Нет	Нет	Нет	Нет	Нет
10	Небезопасные публично-открытые порты	Неприменимо	Неприменимо	Неприменимо	Нет	Нет	Неприменимо
11	Небезопасные порты, открытые из внутренней сети в сеть Интернет	Неприменимо	Неприменимо	Открыт доступ ко всем DNS-серверам в сети Интернет	Нет	Нет	Неприменимо
12	Парольная политика для подключения к сетевому устройству	Нет	Нет	Нет	Нет	Нет	Нет
13	Синхронизация времени	Нет	Да	Да	Нет	Да	Нет

Рисунок 6.2 – Оценка выполнения требований для сетевых устройств

Для рассматриваемой проблемы интерес представляет возможность визуализации для ЛПР аналитических данных по ИБ, в том числе, проект создания системы управления инцидентами ИБ (см. рисунок 6.3).

281 https://rvision.pro/blog/
282 https://www.kommersant.ru/doc/3472959?from=four_tech
283 https://rvision.pro/blog-posts/kak-razvernut-tsentr-monitoringa-gossopka-na-baze-resheniya-r-vision/

Таблица 6.1 – Проверки на соответствие PCI DSS в системе RVision (фрагмент)

Требования PCI DSS	Пояснения	Процедуры проведения тестирования
7.1 Доступом к вычислительным ресурсам и конфиденциальным данным должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.	Чем больше людей имеют доступ к конфиденциальным данным, тем выше риск использования злоумышленниками пользовательских учетных записей. Предоставление доступа лишь тем сотрудникам, которым он необходим для выполнения должностных обязанностей, позволит организации предотвратить ненадлежащее обращение с конфиденциальными данными, связанное с отсутствием опыта или злым умыслом.	7.1 Изучить задокументированную политику контроля доступа и убедиться, что она отражает требования следующим образом: • определение прав доступа и назначение привилегий для каждой должности; • доступ пользователям предоставлен только к тем данным, которые необходимы им для выполнения своих должностных обязанностей; • назначение прав доступа пользователям должно быть основано на классификации должностей и их должностных обязанностях; • документированное утверждение всех прав доступа полномочными сторонами (в письменной или электронной форме) с описанием конкретных утвержденных привилегий.
7.1.2 Предоставить пользователям с учетными записями с широкими полномочиями доступ только к тем полномочиям, которые необходимы им для выполнения своих должностных обязанностей.	При назначении учетных записей с широкими полномочиями важно предоставлять лицам доступ только к тем полномочиям, которые необходимы для выполнения должностных обязанностей ("минимально необходимые полномочия"). Например, администратор баз данных или администратор резервного копирования не должны иметь те же полномочия, что и системный администратор	7.1.2.Опросить сотрудников, ответственных за назначение прав доступа, для подтверждения того, что доступ к учетным записям с широкими полномочиями: • предоставлен только сотрудникам, которым он необходим; • включает только те полномочия, которые необходимы сотрудникам для выполнения своих должностных обязанностей.

Рисунок 6.3 – Основная панель (*Dashboard*) системы RVision

6.4 Объективные проблемы и риски применения систем GRC

Представленные выше решения должны быть рассмотрены с различных позиций, в частности, помимо известных «кейсов» успешных внедрений для крупных компаний, необходимо рассмотреть риски собственно для самой организации, в которой предполагается внедрение. В частности, как отмечалось на сайте RSA Archer GRC, требуется команда более чем 50 ИТ-специалистов и экспертов по управлению рисками [384], [375]. Также предполагается, что будет привлекаться команда около 200 чел. для проведения корпоративного аудита [384], [307]. Тем не менее, существуют определенные риски, которые должны быть учтены, изучены и должным образом оценены перед выбором и применением на конкретном объекте[284]:

— сложность формирования команды специалистов нужного уровня для поддержки и развития платформы;
— большие инвестиции до начала внедрений;
— сложность тестирования без возможности «обкатки» у заказчиков;
— необходимость дальнейшей поддержки ПО (исправление дефектов, адаптация ПО под новые версии ОС и т.п.).

284 https://rvision.pro/blog/

6.5 Методы имитационного моделирования ИСМ

Известно, что с помощью имитационного моделирования возможно эффективное решение ряда задач самой широкой проблематики, в том числе, СМИБ (ИСМ) и прогнозирования поведения СлПО. По некоторым источникам[285], первая работа по постановке и планированию экспериментов в промышленности опубликована еще в 1957 г., Дж. Бокс [280]. Современные средства имитационного моделирования позволяют автоматизировать процесс создания и быстрой адаптации модели за счет использования различных прикладных модулей (в частности, графического интерфейса). Известны примеры создания моделей с применением специализированных языков моделирования (например, GPSS, AnyLogic), проведение имитационных экспериментов при помощи специализированного ПО (например, Arena, AnyLogic, GPSS World, Palisade@Risk, Oracle Crystall Ball, Primavera) и применение программных средств имитационного моделирования в составе математических пакетов (например, Simulink).

Как правило, имитационная среда обеспечивает возможность визуализации процесса имитации, позволяет производить сценарный анализ и поиск оптимальных решений для СлПО. Под имитационным моделированием, в общем случае, понимают создание компьютерной модели реальной или предполагаемой системы (физической, технологической) с целью проведения экспериментов и анализа полученных результатов и/или предсказания будущих различных вариантов развития. В некоторых ситуациях эксперименты на реальных СлПО могут быть весьма дорогостоящими и крайне опасными – например, для непрерывно действующих КИИ (ТЭК или АК). Что же касается выполнения программы аудита ИБ в ИСМ для СлПО, то возможность «прогнать» полный цикл аудита для различных конфигураций СлПО, отличающихся составом мер (средств) обеспечения ИБ, практически нереализуема. В этой ситуации имитационное моделирование является одним из немногих эффективных инструментов, доступных ЛПР.

---

[285] «Стандарты и качество», 2018 г., вып. 3 (969)

Однако нужно принять во внимание и разумные ограничения моделирования и как процесса и как средства достижения цели. Например, некоторые современные войны снова подтвердили известное правило, что лучше подготовленные одержат победу: «*чрезмерное увлечение имитаторами и моделированием боевых действий не доведет до добра*»[286]. Имевшие место в течение предыдущих лет «проигрывания» на компьютерах военных столкновений давних соперников неизменно заканчивались полным разгромом одной из сторон. Как показано в указанной выше статье из журнала «Независимое военное обозрение», реально получилось почти наоборот.

6.6 Разработка метода моделирования ИСМ для СлПО в АК

6.6.1 Обоснование

Для СлПО достаточно актуальной является проблема обеспечения комплексной безопасности и получения оценок уровня безопасности (текущих и/или прогнозов). Особенно актуально эта проблема проявляется при оценке безопасности функционирования современных АК. Особенностями АК являются, помимо учета требований большого числа служб, приоритет требований АБ, в том числе, требований безопасности (как показал ряд авиационных происшествий в 2014 г. в аэропорту «Кольцово» и «Внуково», в 2015 г. – в аэропорту Ростова и Казани, в 2016 г. в аэропорту Брюсселя и Киева, в 2017 г. в аэропорту Хитроу).

Для обеспечения функционирования АК применяются современные СУ, в состав которых входят СМ, соответствующие международным стандартам (в т.ч. ISAGO, ISO) [105]. Например, на соответствие требованиям ISO серии 9001 сертифицированы: «Международный аэропорт Шереметьево», «Международный аэропорт Алматы», «Международный аэропорт Астана», «ВВСС» (аэропорт «Пулково»). Соответственно, управление и оптимизация деятельности АК может быть выполнена на основе полученных оценок (метрик) в единой ИСМ (как показано в Главе 1). Для этих целей необходимо, во-первых, проектировать ИСМ на базе современных риск-ориентированных стандартов,

---

286 http://nvo.ng.ru/forces/2017-07-14/1_956_dembel.html

во-вторых, сформировать требования к процессам АК в четких измеримых метриках, в-третьих, обеспечить комплексный аудит в АК [66], [52]. В порядке дополнения требований аудита, отметим, что в АК применимы требования к аудитам всех типов (в нотации [23], [20]).

6.6.2 Постановка задачи получения численной оценки

Для решения проблемы обеспечения комплексной безопасности АК и получения оценок уровня обеспечения безопасности (текущих и/или прогнозов) необходимо, предпочтительно, оперировать численными оценками (метриками) ИБ. Уровень обеспечения безопасности АК прежде всего зависит от общей производительности, например, нагрузка (число взлётно-посадочных операций, ВПО) в крупнейших АК России планируется на 55 (60) в час[287], а рекорд в 2017 г. установлен в международном аэропорту Мумбаи: 24 ноября в аэропорту выполнили 969 ВПО[288]. Также для обеспечения комплексной безопасности АК должны быть приняты во внимание и смежные системы управления. Например, грузовой оператор аэропорта Шереметьево, обслуживающий рейсы «Аэрофлота», с 28.01.2018 перевел все направления международных воздушных линий на новый грузовой терминал «Москва Карго»[289]. В связи с ростом грузопотока произошел технический сбой в АСУ хранения и комплектации грузов, что еще усугубилось плохими погодными условиями.

Одно из направлений решения данной проблемы может быть реализовано при применении в составе ИСМ «целевого» стандарта СМИБ, точнее стандарта по измерениям ISO/IEC 27004:2009 [318]. В указанном стандарте предложены определения терминов: «мера» (*measure*) и «измерение» (*measurement*), соответственно, п. 3.9 и 3.10 ([318]). Приведем примеры объектов измерений в различных СМ:

— результативность реализованных мер и средств контроля;

— состояние активов, защищенных мерами и средствами контроля;

---

287 www.rbc.ru/society/27/11/2017/5a1b97049a794713b71b6856?from=main

288 https://timesofindia.indiatimes.com/city/mumbai/in-24-hours-mumbai-airport-handles-969-flights-sets-new-world-record/articleshow/61801575.cms

289 https://www.kommersant.ru/doc/3548142

— результативность процессов, реализованных в СМ;

— деятельность служб в организации, ответственных за безопасность;

— степень удовлетворения заинтересованных сторон.

Для оценки результативности мер и средств контроля ИБ рассмотрим один весьма характерный пример. В настоящее время проблема уничтожения хранящихся на военных ноутбуках данных решается радикальным способом. По требованию Министерства обороны РФ в комплект к аппаратам должна входить кувалда[290]. В случае возникновения угрозы захвата противником ноутбука с секретными данными, оператор устройства должен уничтожить информацию физическим образом. Для целей обеспечения комплексной безопасности АК могут использоваться различные источники данных, например, [66], [154], [373].

В качестве примера процедуры организации, касающейся безопасности, рассмотрим пример организации воздушного движения (ОрВД) московской воздушной зоны, в которой выполняется до 19 тыс. полетов в сутки. Сейчас основной системой ОрВД над Москвой является шведская «Теркас»[291], запущенная в 1981 г., но ее ресурс, как отмечается, был исчерпан в 1996 г. На этой системе в 2015–2016 гг. было 4 полных отказа, и нагрузка ложилась на резервную систему, установленную в 2008 г. Уже в 2017 г. в работе новой системы ОрВД «Синтез-АР4» дважды был зафиксирован сбой: 19 октября произошел отказ в работе комплекса средств автоматизации управления воздушным движением (КСА УВД), а 24 октября произошло нарушение работоспособности в части автоматической обработки сообщений плановой информации[292]. Сбои подтвердил разработчик системы концерн «Алмаз-Антей». Уточняется, что в первом случае сбой был «*парирован средствами встроенного и автономного резервирования*» и перерыва в информационном обеспечении не было. При втором сбое пришлось перезапустить некоторые серверы и потребовалось почти два часа[293]. Всего за время работы новой системы были

290 http://www.securitylab.ru/news/489331.php
291 https://www.kommersant.ru/doc/3371849
292 http://www.rbc.ru/technology_and_media/08/11/2017/5a02c0be9a7947c7b2dc7b33?from=main
293 https://www.kommersant.ru/doc/3460820

выявлены неисправности 9 мониторов диспетчеров, 5 из них удалось починить. К системе было предъявлено 16 замечаний, из которых 13 устранено[294].

Аналогичные проблемы возникают периодически и в системе управления перелетами Европейской организации по безопасности воздушной навигации (Евроконтроля)[295]. В частности, 3 апреля 2018 г. в европейском воздушном пространстве было запланировано 29 тыс. авиарейсов. Более 15 тыс. рейсов были задержаны в связи с масштабным сбоем в системе управления Евроконтроля. Как сообщается [296] в уведомлении Евроконтроля, за двадцать лет работы система управления давала сбой лишь дважды – в 2001 и 2018 г.

Таким образом, может быть сформулирована постановка задачи как получение оценок уровня обеспечения безопасности (текущих и/или прогнозов). Численная оценка результативности по модели ИСМ соответствует численной оценке уровня обеспечения безопасности.

6.6.3 Модель для проведения аудита ИСМ в АК

Рассмотренные в Главе 2 требования (базовые и расширенные) относятся к АК, которые в полной мере могут считаться промышленными объектами (СлПО) и, во-первых, требуют строгого выполнения комплекса нормативных требований (например, по результатам террористической атаки в аэропорту Брюсселя в 2016 г.), во-вторых, требуют периодического контроля – как именно выполняются в конкретном АК установленные требования (например, аэропорт «Внуково») [66], [52], [110], [325] – [327]. Обратим внимание, что в аэропорту «Внуково» существуют определенные проблемы именно с периодическим контролем. В декабре 2017 г. сотрудники ФСБ провели обыски в Центре ОрВД в аэропорту «Внуково», т.к. один из системных администраторов создал ферму для майнинга криптовалюты, которая была подключена к сети аэропорта[297].

В аспекте требований аудита в ИСМ актуален практический вопрос о преимуществе какого-либо критерия (стандарта, требования, регламента и пр.)

---

294 http://novostnoy.com/v-rabote-novoi-sistemy-upravleniia-poletami-nad-moskvoi-proizoshli-sboi/
295 https://www.securitylab.ru/news/492450.php
296 https://www.eurocontrol.int/press-releases/enhanced-tactical-flow-management-system-etfms-outage-official-statement
297 http://safe.cnews.ru/news/top/2017-12-15_sisadmin_aeroporta_vnukovo_majnil_kriptovalyutu

над иными. В условиях многокритериальных задач, к которым можно отнести и задачу проведения комплексных аудитов ИСМ для АК, необходимо применять математически обоснованный и достоверный метод. Известно, что МАИ (предложен Т. Саати) среди методов многокритериальной теории полезности по ориентировочным оценкам уже более 20 лет удерживает ведущие позиции в применении к решению слабоструктурированных многокритериальных задач [141], [54], [113].

Соответственно, поставленную задачу целесообразно решать на основе базовой модели аудита ИСМ (см. Главу 1, рисунок 1.7), дополненной специальным блоком оптимизации (см. Главу 2, рисунок 2.12) – для целей получения оценки уровня безопасности. С учетом указанных выше особенностей проведения комплексного аудита в АК, центральное внимание должно быть уделено блоку оптимизации модели ИСМ в АК. Это требование особенно важно в целях выполнения имитационного моделирования и предоставления оценок ЛПР в режиме, близком к РРВ.

Как отмечалось выше в (см. Главу 1 и Главу 2), блок оптимизации учитывает («на входе») степень результативности бизнес-процессов АК и отрабатывает необходимые изменения в модели ИСМ («на выходе»). Этот подход позволяет вносить управляющие воздействия в цикле PDCA по каналам обратной связи на основе оценки результативности (степени достижения численных метрик ИБ), через необходимую оптимизацию и периодический анализ ИСМ со стороны ЛПР (см. Главу 5). Поставленная задача решается через численную оценку результативности (оценку уровня обеспечения безопасности) как для отдельных функциональных подсистем ИСМ (соответствующие формулы представлены в Главе 5).

6.6.4 Формирование перечня атрибутов для аудита ИСМ

Для выполнения результативного аудита в ИСМ представляется рациональным формировать перечень атрибутов (т.е. в стандартных терминах – список требований, которые могут быть проверены и измерены на соответствие критериям – стандартов ISO, ГОСТ и пр.), причем количество этих критериев

может составлять несколько сотен [66], [52]. В качестве базы для создания перечня, может быть взято Приложение Б [46]. Представляется полезным сопоставить указанное выше приложение для национальных стандартов ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО 9001. Данные представлены в таблице 6.2.

Таблица 6.2 – Пример перечня атрибутов аудита ИСМ (фрагмент)

п.п.	Примеры положений ГОСТ Р 51901.1-2002 (Приложение Б)	ГОСТ Р ИСО 9001	ГОСТ Р ИСО 27001
1	Определяют и документируют классификационную категорию ЗО. Устанавливают: - факторы латентности и угрожающих ОЗ факторов; - характер, стоимость (или значимость без стоимостной оценки), латентные свойства и концентрация защищаемых ценностей; - факторы, определяющие экономическую и неэкономическую ответственности ЗО	6.3 6.4 7.1	4.1 4.2 4.3
2.	Проверяют виды служб безопасности ЗО, оценивается наличие на ЗО собственной технической службы.	7.5.1	5.3 7.2
4.	Осматривают и оценивают контрольные зоны на ЗО с размещением технических средств подсистем.	8.2.2	9.1 9.2
9.	Проверяют паспортизацию ЗО (наличие, виды, содержание, условия хранения, каллиграфия, актуализация паспортов).	8.2.2 4.2	7.5 9.2
11.	Проверяют наличие на ЗО технических документов (планов, схем, маршрутов, методик тренировок) по эвакуации людей в ЧС.	5.5.3 4.2	7.3 7.5
14	Экспертно оценивают организацию технического обслуживания (ТО) на ЗО. Проверяют: наличие планов работ; принятые виды и периодичность ТО; квалификацию и техническую оснащенность персонала; ведение документации по ТО.	6.2 6.3 6.4 4.2	6.1 7.1 7.2 7.5

6.6.5 Формирование перечня атрибутов для аудита ИСМ в АК

В документе РУБП (Doc 9859 ИКАО) отражены дополнительные атрибуты, по которым необходимо проводить аудит СМ (и ИСМ) для АК. Прежде всего, это следующие атрибуты:

1. Физическая безопасность (п. 11.2.4.1);

2. Уязвимые места (п. 11.2.4.9);
3. Система контроля "замок – ключ" (п. 11.2.4.11);
4. Метрология (ДОБ 1-28, Руководство по авиационной безопасности);
5. Выделение ресурсов (Doc 9082, Doc 9184, Doc 9562);
6. Меры контроля качества (ДОБ 8-13).

Анализ исходных данных аудита ИСМ в АК

В течение 2012-2015 гг. автор принимал участие в проведении аудита ИСМ в нескольких АК (г. Алматы и г. Астана, Республика Казахстан). По всем аудитам группой экспертов были надлежащим образом оформлены свидетельства аудита, анализ которых позволил выявить закономерности, практическое применение которых позволяет обоснованно подойти к вопросу определения текущей оценки уровня обеспечения ИБ в СлПО – АК. Основное внимание предлагается уделить количеству несоответствий по «профильным» службам АК, обеспечивающих безопасность в АК (см. таблицу 6.3).

Таблица 6.3 – Несоответствия при внешнем аудите ИСМ (фрагмент)

Служба	ISO 9001	ISO 14001	OHSAS 18001	Всего
АС	5	8	8	21
ГСМ	6	3	2	11
САБ	2	3	13	18
СПАСОП	3	9	8	20
ССТ	6	7	5	18
ТТиСТО	2	1	11	14
ЭСТОП	3	5	8	16
Общий итог	101	65	153	319

Группа внешних аудиторов также проверила позже состояние планирования и фактических результатов разработки (актуализации) одного из ключевых процессов (подробно рассмотренных в Главе 5) – документирования информации ИСМ в АК (см. таблицу 6.4). На основе полученных данных экспертом Танатаровой А.Т., внешние аудиторы зафиксировали объективное улучшение ситуации с разработкой внутренних нормативных документов (ВНД) по плану (81,2% против 5,8% годом ранее) и общим снижением вновь разрабатываемых ВНД (149 против 465).

Таблица 6.4 – Разработка ВНД (фрагмент)

Категория ВНД	2012 г.			2013 г.		
	Всего разработано	По плану	Сверх плана	Всего разработано	По плану	Сверх плана
Методические инструкции	21	14	7	15	10	5
Рабочие инструкции	14	5	9	49	30	19
Должностные инструкции	164		164	77	77	
Инструкции САБ	247		247	2	2	
…	…	…	…	…	…	…
Всего	**465**	**27**	**438**	**149**	**121**	**25**
Доля %	100 %	5,8 %	99,94 %	100 %	81,20%	18,79 %

Отметим резкий «сброс» количества разработанных новых инструкций САБ против общего количества инструкций иных категорий, что отражает метрику результативности степени документирования конкретной функциональной подсистемы АК. В продолжение обоснования модели «мгновенных аудитов» ИСМ (см. Главу 3), получаем еще одно подтверждение, что «быстрый» цикл аудита ИБ позволяет в одном замкнутом цикле PDCA снизить количество корректирующих мер (документации) на 2 порядка, что значительно снижает общие издержки как на подсистему аудита (на (k+1)-м цикле), так и на обеспечение функциональной безопасности СлПО.

Достаточно интересный пример управления издержками на практике представлен предприятием «Северсталь» на конференции «Цифровой инфофорум» в 2017 г. В докладе «Безопасная цифровизация процессов – цель, суть и содержание»[298] представлена «Система интеллектуальной поддержки контрольных функций» (проект «Скиф»), которая обеспечивает решение задачи контроля над издержками и снижением потерь во всех бизнес-процессах за счет автоматизированного выявления нарушений.

Сопоставление данных, полученных внутренними и внешними аудиторами, всегда представляют определенный интерес для ЛПР, т.к. при том же объекте

[298] https://infoforum.ru/conference/conference/view/id/39

исследования и единых методах получаются расхождения, объективный и беспристрастный анализ которых может улучшить методы аудита, применяемые в конкретной ИСМ [152], [21], [20], [318]. В докладе эксперта М.Макух (DQS) в 2015 г. представлена оценка ожидаемых несоответствий СМК по разделам стандарта [126]. Сопоставление данных внутренних и внешних аудитов (применительно только к СМК по ISO 9001 версии 2008 г.), а также оценок DQS, представлено в таблице 6.5.

Таблица 6.5 – Сопоставление данных аудита (фрагмент)

Раздел стандарта ИСО 9001:2008	**Данные DQS, %**	**Данные внутреннего аудита, %**	**Данные внешнего аудита, %**
4.	26	57	45
5.	9	11	11
6.	19	8	17
7.	17	8	21
8.	29	16	6
Всего, %	**100**	**100**	**100**

6.7 Пример расчета модели ИСМ для оценки уровня обеспечения безопасности АК

На основании постановки задачи, расширенной системы критериев (ISO, ISAGO и ГОСТ, см. Главу 2), а также предложенной модели ИСМ для аудита АК (см. Главу 2), представляется возможным выполнить моделирование СлПО и определить весовые коэффициенты (**α** и **β,** соответственно, для функциональных подсистем и атрибутов). Дополнительно при формировании иерархической структуры атрибутов в модели ИСМ для аудита АК учитываются данные: внешних и внутренних аудитов, состав документации, внешние требования регуляторов (IATA, ISAGO, ISO) и иные объективные свидетельства.

В некоторых публикациях (например, «Страшнее хакеров только регуляторы»[299]) отмечается, что главную опасность инвесторы видят в киберугрозах, а главы компаний более склонны ждать неприятностей от государства, в частности, в виде чрезмерного регулирования. По данным этого обзора все респонденты считают необходимость демонстрировать результаты в

[299] https://www.kommersant.ru/doc/3560649?from=four_economic

более жестких временных рамках. Рост недоверия в отношениях компаний с правительствами фиксируют 48% инвесторов и 24% руководителей.

В работе М. Месаровича, Д. Мако и И. Такахара [127] дается крайне важный пример учёта «вмешательства» вышележащего уровня управления на нижележащие. С учетом рассмотренных выше функций качества («*полезности*»), это позволяет динамически переоценивать значения числовых параметров в **новых** формулах оценки результативности СМИБ (ИСМ). В принципе, предлагаются различные схемы («*кормчий*», «*координатор*» и пр.), что предусматривает, в любом случае, получение «обратной связи» для обеспечения качества управления ([127], стр.55). Вообще важно не просто предусмотреть, но численно оценить любое вмешательство на каждом уровне управления СлПО. Более точно, функция аудита СМИБ (ИСМ) дает возможность перейти к более простой модели, также обеспечивающей решение поставленной выше задачи для ЛПР (см. Главу 5). В частности, предлагаются к рассмотрению многоэшелонные системы ([127], стр. 69), для которых по характеру иерархического взаимодействия разделяются несколько категорий принятия решений:

- одноуровневые одноцелевые,
- одноуровневые многоцелевые,
- многоуровневые многоцелевые.

Кроме того, отметим, что именно 3-я категория характеризуется необходимостью включения «арбитра» (в терминах [127]) для обеспечения достижения целей ЛПР. Предыдущие две категории не предусматривают наличие конфликтов, либо допускается «коалиция» (в терминах [127]). Для данного примера важно обеспечить заданный уровень ИБ, определяемый ЛПР (который может быть выделен как «арбитр»), что подразумевает необходимость согласования многих мнений, дискуссий о выделении ресурсов и шагов по реализации программы аудита ИБ ради достижения поставленной цели. В данной ситуации программа аудита ИБ может иметь важнейшее стратегическое значение, поскольку утверждается ЛПР, должна охватывать все бизнес-

процессы СлПО, но, вероятно, с разной степенью «быстродействия» на различных уровнях иерархии. В частности, ранее представленный подход «мгновенных аудитов» ИБ может иметь прямое прикладное значение для каждого уровня иерархии СлПО, что обеспечит, в том числе, и «арбитраж» с необходимой частотностью вмешательства со стороны ЛПР (см. Главу 5).

6.7.1 Требования к модели для оценки уровня обеспечения безопасности АК

В документе РУБП (ICAO Doc 9859[300]) определены подходы для расследования, которые затрагивают последовательно достижение следующих целей (п. 2.9.2):

1. Забыть об утратах и убытках.
2. Восстановить доверие и уверенность в системе.
3. Возобновить нормальную деятельность.
4. Выполнить политические задачи.

Помимо этого, декларируется приверженность высшего руководства (ЛПР) к принципам управления безопасностью. В модели оценки также крайне важно учесть не только степень приверженности ЛПР (*commitment*), но и длительность реализации всех запланированных мероприятий на должном уровне. Например, в Государственном космическом научно-производственном центре им. Хруничева (ГКНПЦ) было ликвидировано контрольно-ревизионное управление (КРУ)[301]. Оно приняло непосредственное участие в возбуждении десятков уголовных дел, в общей сложности, на миллиарды руб. КРУ сразу же было наделено крайне широкими полномочиями по проверке деятельности не только ГКНПЦ, но и всех дочерних предприятий. Таким образом, КРУ проверяло и подписываемые контракты, и документацию за десятилетний срок.

В разделе 7 РУБП отмечается целесообразность интеграции СУБП и СУК (СМК), т.е. каждая система управления по отдельности не может обеспечить главного преимущества – единого управления факторами риска для

300 http://www.icao.int/safety/SafetyManagement/Documents/Doc.9859.3rd%20Edition.alltext.en.pdf
301 https://www.kommersant.ru/doc/3456177

безопасности полетов, связанными с последствиями факторов, с которыми АК должна сталкиваться в процессе предоставления услуг. Отметим, что в РУБП определено, как авиационные предприятия именуются «*системами систем*» (п. 7.8.1), среди которых и СУБП, и СУК (СМК), САБ и пр. Однако, там же приводится важная оговорка, что пути интеграции всех систем весьма различны и, более того, требования к такой интеграции систем управления (СМ) в единую ИСМ выходят за рамки документов ИКАО и РУБП (п. 7.8.3).

6.7.2 Программная среда моделирования MPriority

Для выполнения имитационного моделирования применяется программная среда MPriority версии 1.0 (авторы: Абакаров А.Ш., Сушков Ю.А.[302]). MPriority предназначена для поддержки принятия решений в различных сферах деятельности. Данная система содержит диалоговые средства, позволяющие получать наиболее полную информацию о проведенных попарных сравнениях и устранять возможные несогласованности в МПС[303]. Практическое применение МАИ для различных современных приложений (транспорт, энергетика, логистика, управление персоналом и пр.) описано в публикациях ([335], [364], [231], [264]).

6.7.3 Исходные данные для моделирования в среде MPriority

Для выполнения имитационного моделирования в среде MPriority приняты следующие исходные данные:

1. Объект: модель аудита ИБ в ИСМ для СлПО – АК (см. Главу 2).
2. Количество уровней модели (всего – 5):
   - — уровень цели,
   - — уровень функциональных подсистем (всего – 4),
   - — уровень типов аудита ИСМ (всего – 3),
   - — уровень ключевых процессов ИБ (всего – 6),
   - — уровень альтернатив (всего – 5).
3. Формулы расчета результативности ИСМ (5.1, 5.2 см. Главу 5).

---

302 http://tomakechoice.com/mpriority.html

303 http://tomakechoice.com/paper/mpriority.pdf

Требуется определить результативность СМИБ по представленной модели (см. Главу 2, принимая во внимание текущие параметры):

4. Цель определена как: оценка результативности ИСМ.

Общая структура модели ИСМ для СлПО АК показана на рисунке 6.5. Показан уровень функциональных подсистем; всего в представленной модели 4 уровня иерархии и 5 возможных альтернатив – стандартов ISO и ISAGO (IATA).

5. Выполнены все типы аудита:

— Аудит 1-й стороной (в объеме 100%),

— Аудит 2-й стороной (в объеме 30%),

— Аудит 3-й стороной (в объеме 100%).

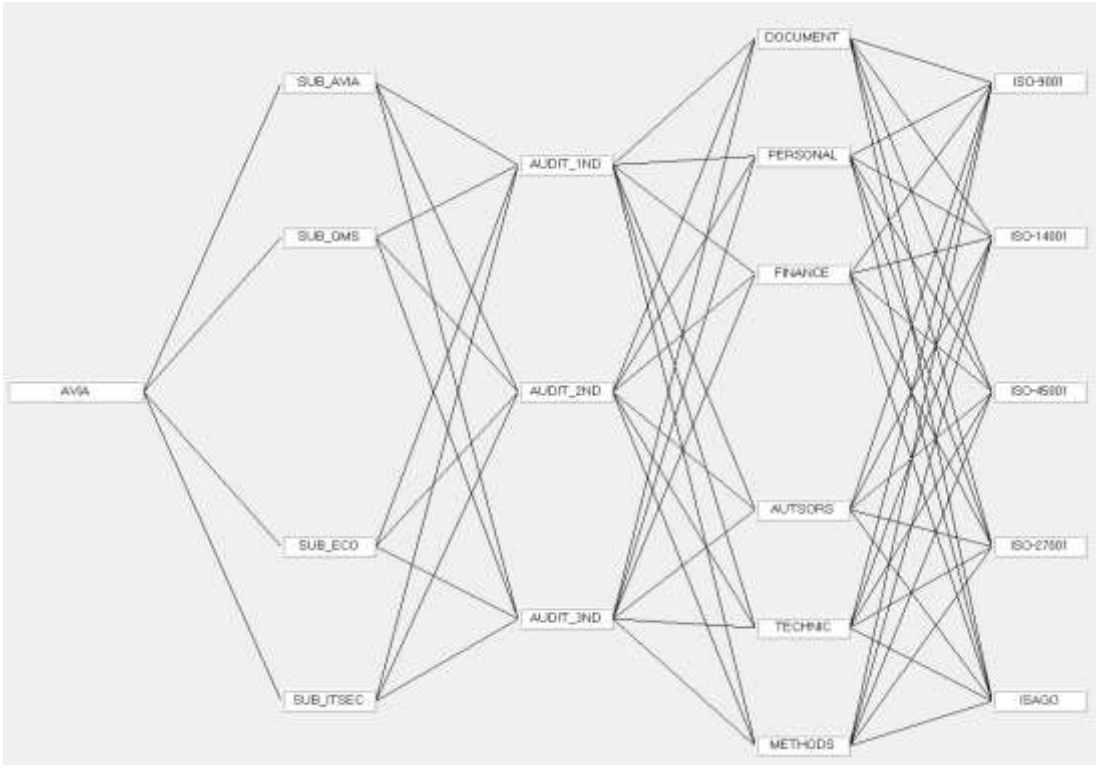


Рисунок 6.4 – Общая структура модели ИСМ для СлПО АК

Результативность по каждому типу аудита составляет, соответственно: 0,9; 0,8 и 1 (как аргументы формулы (5.2). Весовые коэффициенты (**β**) для данного уровня иерархии определяются по методу МАИ в системе MPriority. На рисунке 6.5 представлен расчет коэффициентов **β** (аудита ИСМ) для одной из функциональной подсистем: ***Sub_Avia***, (нормированных к 1 – 0,62; 0,27 и 0,11 соответственно).

6. Выявлены несоответствия по функциональным подсистемам:

— По ***Sub_Avia*** *(все типы аудита);*

— По ***Sub_QMS*** *(аудит 1-й и 3-й стороной);*

— По ***Sub_ECO*** *(аудит 1-й и 3-й стороной);*

— По ***Sub_ITSec*** *(аудит 1-й и 3-й стороной)*

7. Атрибуты выявленных несоответствий для каждого типа аудита по каждой из функциональных подсистем соответственно:

— По $A_{1\text{-}ND}$ соответственно 0,8; 0,8; 0,75 и 0,7.

— По $A_{2\text{-}ND}$ соответственно 0,7; 1; 1; и 1.

— По $A_{3\text{-}ND}$ соответственно 0,8; 0,6; 0,7 и 0,7.

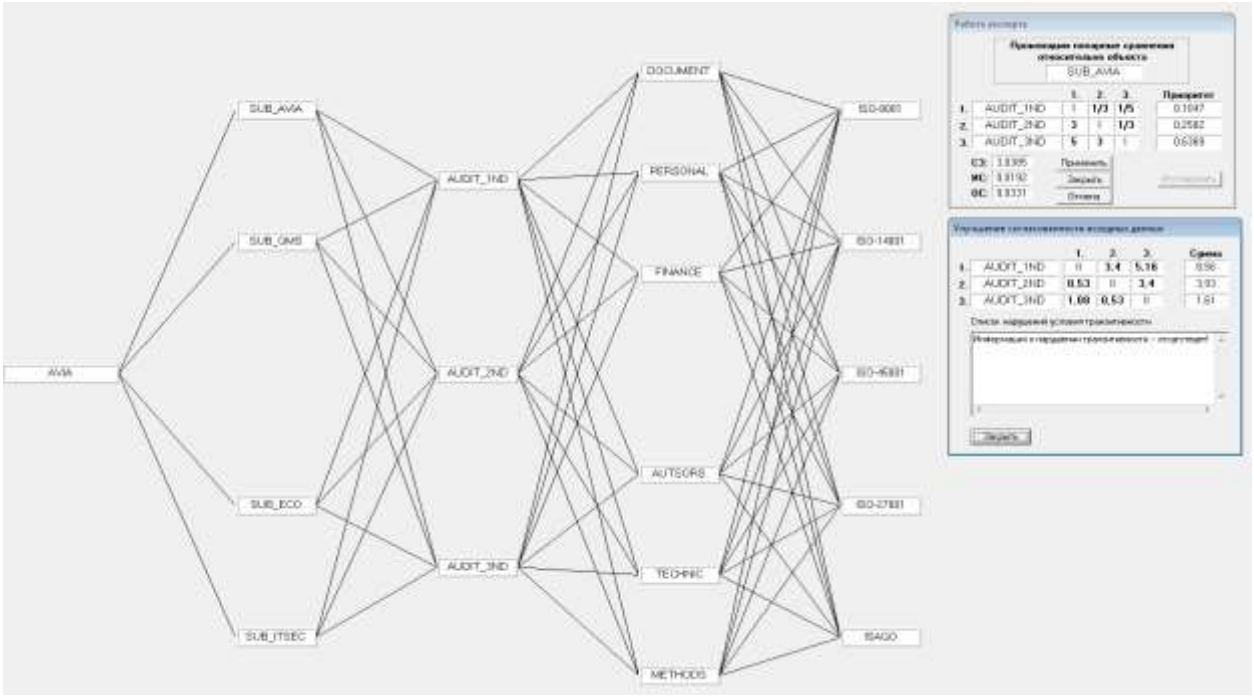


Рисунок 6.5 – Расчет коэффициентов **β** для подсистемы Sub_Avia

На рисунке 6.6 представлен расчет коэффициентов **α** для всех функциональных подсистем модели аудита ИСМ для АК. Предположим, ***μ*** = 0,9 по формуле (5.2). С учетом полученных коэффициентов (**α** и **β**) выполним расчет по формулам (5.1) и (5.2) модели аудита ИСМ для АК. В модели учтены все 4 подсистемы (***Sub_Avia, Sub_QMS, Sub_ECO, Sub_ITSec***) и 3 атрибута (метрики), агрегированные по различным видам аудита (***1-ND, 2_ND, 3_ND***, соответственно, 1-й, 2-й и 3-й стороной). В силу ограничения объема расчет результативности подсистем по модели ИСМ для АК будет представлен по агрегированным 3-м параметрам:

$$P_{ПС\ Sub\_Avia} = \mu\ (\beta_{11}\ A_{1\text{-}ND} + \beta_{21}\ A_{2\text{-}ND} + \beta_{31}\ A_{3\text{-}ND})$$

$$P_{ПС\ Sub\_QMS} = \mu\ (\beta_{12}\ A_{1\text{-}ND} + \beta_{22}\ A_{2\text{-}ND} + \beta_{32}\ A_{3\text{-}ND})$$

$$P_{ПС\ Sub\_ECO} = \mu\ (\beta_{13}\ A_{1\text{-}ND} + \beta_{23}\ A_{2\text{-}ND} + \beta_{33}\ A_{3\text{-}ND})$$

$$P_{ПС\ Sub\_ITSec} = \mu\ (\beta_{14}\ A_{1\text{-}ND} + \beta_{24}\ A_{2\text{-}ND} + \beta_{34}\ A_{3\text{-}ND})$$

и, соответственно:

$$P_{ИСМ} = \varphi\ (\alpha_{Avia}\ P_{ПС\ Sub\_Avia} + \alpha_{QMS}\ P_{ПС\ Sub\_QMS} + \alpha_{ECO}\ P_{ПС\ Sub\_ECO} + \alpha_{ITSec}\ P_{ПС\ Sub\_ITSec})$$

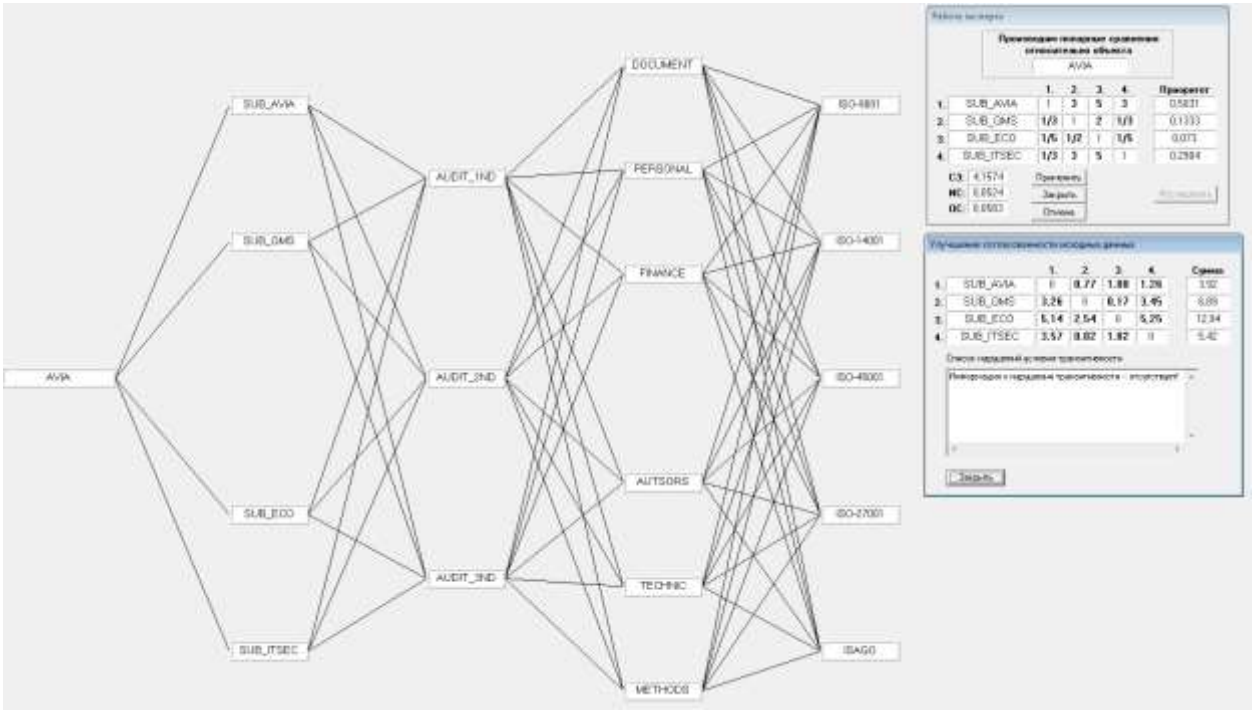


Рисунок 6.6 – Расчет коэффициентов **α** для подсистем модели ИСМ в АК

Получаем по (5.2):

$P_{ПС\ Sub\_Avia} = 0{,}9 * (0{,}11 * 0{,}8 + 0{,}25 * 0{,}7 + 0{,}64 * 0{,}8) = 0{,}9 * 0{,}78 = 0{,}7.$

$P_{ПС\ Sub\_QMS} = 0{,}9 * (0{,}10 * 0{,}8 + 0{,}22 * 1 + 0{,}68 * 0{,}6) = 0{,}9 * 0{,}71 = 0{,}66.$

$P_{ПС\ Sub\_ECO} = 0{,}9 * (0{,}14 * 0{,}75 + 0{,}28 * 1 + 0{,}58 * 0{,}7) = 0{,}9 * 0{,}7 = 0{,}63.$

$P_{ПС\ Sub\_ITSec} = 0{,}9 * (0{,}14 * 0{,}7 + 0{,}22 * 1 + 0{,}64 * 0{,}7) = 0{,}9 * 0{,}77 = 0{,}69.$

Предположим, $\varphi = 0{,}9$ и $\alpha_{Avia} = 0{,}51$; $\alpha_{QMS} = 0{,}13$; $\alpha_{ECO} = 0{,}07$; $\alpha_{ITSec} = 0{,}29$.

Получаем в итоге по (5.1):

$$P_{ИСМ} = 0{,}51*0{,}7 + 0{,}13*0{,}66 + 0{,}07*0{,}63 + 0{,}29*0{,}69 = 0{,}68$$

Заметим, что общая (интегральная) оценка $P_{ИСМ}$ может учитывать произвольное количество оценок функциональных подсистем. В предложенной модели используются шкалы зрелости ИСМ (см. таблицу 6.6):

Таблица 6.6 – Шкалы зрелости ИСМ

Уровень	Зрелость ИСМ	Основные характеристики ИСМ	Значение $Р_{ИСМ}$
0	Отсутствует	· Реализация отдельных требований	$0,1 \geq Р_{ИСМ} > 0$
1	Определенная	· Реализация всех требований СМ · ИСМ документирована	$0,25 \geq Р_{ИСМ} > 0,1$
2	Управляемая	· ИСМ документирована · Поддерживается цикл PDCA	$0,5 \geq Р_{ИСМ} > 0,25$
3	Установленная	· Реализация всех требований в ИСМ · ИСМ сертифицирована	$0,75 \geq Р_{ИСМ} > 0,5$
4	Предсказуемая	· ИСМ сертифицирована · Управление по целям	$0,8 \geq Р_{ИСМ} > 0,75$
5	Оптимизируемая	· ИСМ прошла 1 цикл сертификации · Определены цели улучшения · Управление эффективностью	$Р_{ИСМ} > 0,8$

По таблице 6.6 при $Р_{ИСМ} = 0,68$ уровень зрелости равен 3, степень зрелости ИСМ – «Установленная». Отметим, что не всегда оценки результативности могут быть корректно подготовлены для ЛПР, в частности, на защите одного решения в Университете ИТМО был представлен график даже с отрицательным коэффициентом защищенности (см. рисунок 6.7):

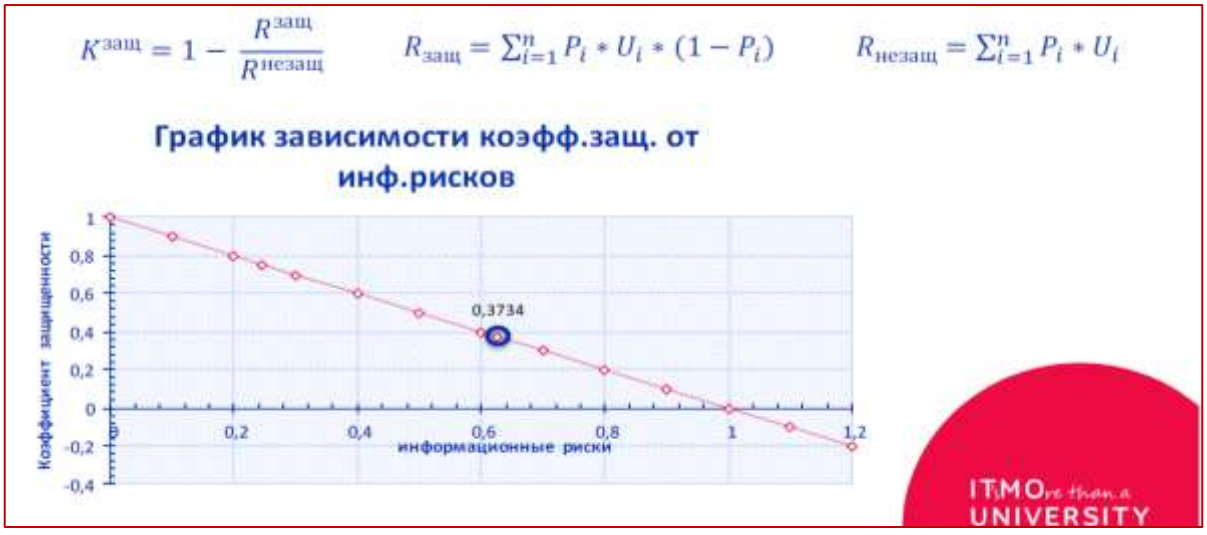


Рисунок 6.7 – Пример отрицательного коэффициента защищенности

В представленном примере с помощью системы моделирования MPriority получена оценка приоритетов существующих стандартов (ISO, ISAGO, ГОСТ) для целей обеспечения безопасности СлПО в АК (см. рисунок 6.8).

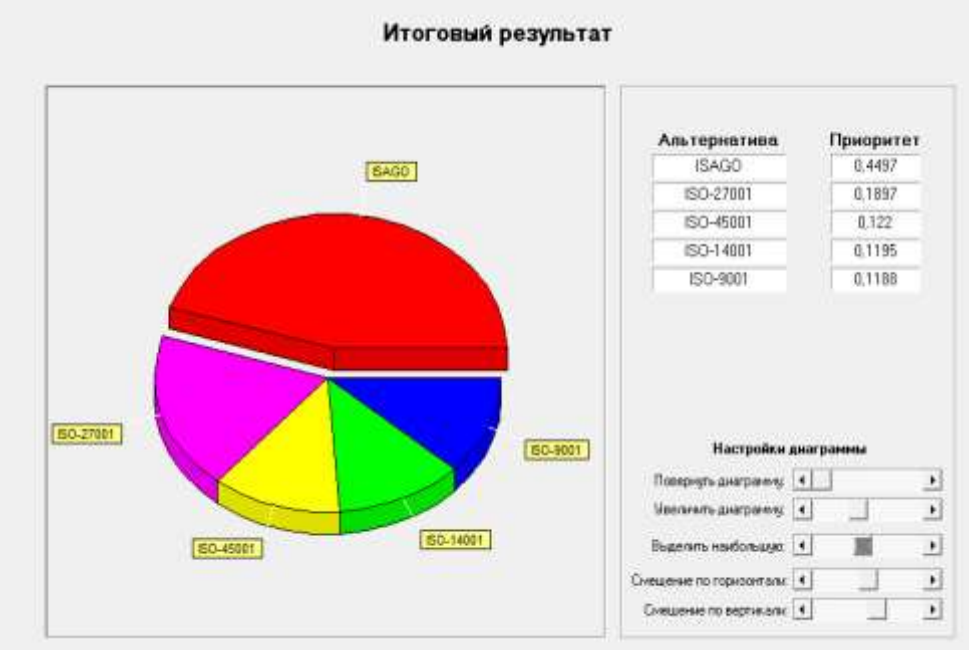


Рисунок 6.8 – Расчет приоритетов стандартов для целей обеспечения безопасности СлПО в АК

6.8 Метод измерения производительности системы моделирования

6.8.1 Необходимость оценки производительности

Известны результаты первого международного исследования Riverbed Global Application Survey 2015, которое было выполнено исследовательской командой Riverbed Technology[304]. Результаты опроса топ-менеджмента показали, что бизнес сталкивается с низкой производительностью работы ИТ-инфраструктуры, и что 96% руководителей согласились с тем, что оптимальная производительность корпоративных приложений критически важна для достижения эффективности функционирования бизнеса организации. При этом 94% опрошенных заявили, что низкая производительность негативно повлияла на их работу. Необходимость оценки производительности любой технической системы важна в том случае, если ЛПР не имеет возможности ждать сколь угодно долго результатов реального аудита ИСМ для СлПО и/или предпочитает выполнить работу с экспертной группой (сессию моделирования) в режиме, близком к РРВ [13], [64], [140]. Например, решение – Industrial Cyber Security Risk Manager, система автоматического мониторинга, оценки и управления

304 http://www.cnews.ru/news/line/2016-02-24_96_organizatsij_po_vsemu_miru_schitayut_proizvoditelnost

рисками возникновения киберугроз предложила компания Honeywell[305]. Указано, что данное решение позволяет выполнять контроль угроз ИБ, анализ уровня их опасности в РРВ и позволяет точно рассчитывать соответствующие риски в соответствии с требованиями нового стандарта ISA 62443, как показано в Главе 2. Однако, указывается, что решение принимает все же человек – диспетчер, более того, этот диспетчер оценивает риски ИБ на промышленных предприятиях, использующих оборудование разных поставщиков в режиме, близком к РРВ. Кроме указанного решения Industrial Cyber Security Risk Manager существуют и иные решения, например[306]:

- Sentryo;
- CyberShield Analysis and Detection for SCADA Networks;
- Indegy;
- PFP Cybersecurity;
- Industrial Defender Automation Systems Manager (ASM);
- NexDefense Sophia.

6.8.2 Характеристики методики Apdex

В качестве методики для оценки производительности системы имитационного моделирования предлагается модифицированная методика Apdex [172]. Базовая методика Apdex обладает свойствами, необходимыми для качественного решения задачи оценки измерения производительности:

- объективность: формируемая оценка не должна зависеть от различных субъективных факторов отдельных экспертов,
- прикладной характер: формируемая оценка должна отражать реальную производительность системы,
- интегральность: формируемая оценка должна учитывать все аспекты работы системы,
- измеримость: формируемая оценка должна быть измеримой (численной) для сравнения различных вариантов.

---

305 http://www.cnews.ru/news/line/honeywell_predstavila_reshenie_dlya_avtomaticheskogo

306 http://bis-expert.ru/blog/8463/52152

Методика Apdex оперирует понятием «ключевой операции», т.е. операции, время успешного исполнения которой является критичной для ЛПР [172]. Кроме того, учитывается и приоритет ключевой операции, также исходя из важности для ЛПР. Дополнительно учитывается целевое время ключевой операции (**T**), это время, за которое всегда должна выполняться ключевая операция. Целевое время ключевой операции, как правило, определяет ЛПР.

6.8.3 Интерпретация полученных оценок производительности Apdex

Методика Apdex позволяет интерпретировать полученные числовые значения в терминах качественных и количественных оценок (см. таблицу 6.7):

Таблица 6.7 – Шкала оценок методики Apdex

Значение		**Оценка**	**Примечание**
Мин.	Макс.		
0,00	0,50	Неприемлемо	Относительно «целевого времени» ЛПР
0,50	0,70	Плохо	
0.70	0,85	Удовлетворительно	
0,85	0,94	Хорошо	
0,94	1.00	Отлично	

6.8.4 Определение оценки производительности по методике Apdex

Алгоритм получения базовой оценки по методике Apdex следующий:

1. Формирование списка ключевых операций.
2. Определение приоритетов для ключевых операций.
3. Определение целевого времени для каждой операции.
4. Определение фактического времени выполнения ключевых операций.
5. Формирование оценки Apdex.

Базовая оценка Apdex вычисляется по формуле:

$$I_{Apdex\ base} = \frac{NS + NT\ /2}{N} \qquad (6.1)$$

где:

$I_{Apdex\ base}$ – *базовая оценка (индекс производительности) Apdex;*
N – *общее количество выполнений данной операции;*
NS – *количество выполнений с временем отклика от 0 до T;*
NT – *количество выполнений с временем отклика от T до 4T;*
T – *целевое время ключевой операции (удовлетворительное);*
$4T$ – *время ключевой операции (неудовлетворительное).*

Рассмотрим недостатки базовой формулы (6.1) [172], в частности:

— для расчета Apdex собирается множество статистических данных о времени выполнения типовых операций в системе;

— у базовой формулы есть объективное условие, что количество одноименных операций за период должно быть более 10, иначе значение Apdex будет занижено;

— как правило, все примеры, демонстрирующие результаты методики Apdex содержат не более 5 операций [172], [128].

— никак не учитываются так называемые «разочарованные» пользователи, которые не дождались ответа ни к целевому времени **T** («*довольные*»), ни ко времени **4T** («*удовлетворены*»).

Для применения базовой методики Apdex для целей оценки производительности системы имитационного моделирования СлПО на примере АК внесем в базовую формулу следующие изменения:

$$I_{Apdex\ New} = \frac{f(Nt) * NT + f(Nq) * NQ}{N} \qquad (6.2)$$

где:

$I_{Apdex\ New}$ – *новая оценка (индекс производительности) Apdex;*
$f(Nt)$ – вероятность получения ЛПР ответа к целевому времени T и 4T
$f(Nq)$ – вероятность получения ЛПР ответа свыше времени 4T.
NT – *кол-во выполнений операций с временем отклика от 0 до 4T;*
NQ – *кол-во выполнений операций с временем отклика свыше 4T;*
N – *общее количество выполнений данной операции.*

На основании **новой** формулы (6.2) рассмотрим состав операций для оценки производительности системы имитационного моделирования СлПО на примере АК (объекты: АК международные аэропорты Алматы и Астаны). Общие исходные данные показаны в таблице 6.8. Перечень операций в таблице 6.8 завершается проверкой согласованности МПР и финальным расчетом в системе MPriority. Время на представление результатов имитационного моделирования ЛПР, время обсуждения результатов с группой экспертов и внесения новых исходных данных не учитывается. Отметим, что в формуле (6.2) ***f (Nt) + f (Nq) = 1***, при этом ***f (Nt)*** = 0,9973, а ***f (Nq)*** = 0,0027 (в соответствии с правилом **3σ** (где **σ**

– среднее квадратическое отклонение при допущении нормального закона распределения Гаусса ([11], [67]). Действительно, маловероятно, что кол-во выполнений операций со временем отклика свыше 4T будет существенным, но, тем не менее, такая вероятность учитывается и в новой оценке индекса производительности Apdex, и, соответственно, в примере расчета (см. таблицу 6.8).

Результаты полного цикла имитационного моделирования по модели ИСМ для СлПО в АК на основании **новой** предложенной формулы оценки производительности Apdex New (6.2) представлены на рисунке 6.9

Рисунок 6.9 – Результаты полного цикла имитационного моделирования

Состав операций, представленный в таблице 6.8, точно соответствует одному полному циклу (аналитической сессии) работы экспертов СлПО, любые изменения, уточнения или исключения приводят к запуску нового цикла имитационного моделирования по уточненной модели СлПО для АК. Кроме того, имитационное моделирование настоятельно рекомендуется применять совместно как в процессе планирования приемлемого для ЛПР «времени отклика» при реализации предложенного метода «мгновенных аудитов», так и при формировании набора мер и средств контроля ИБ в методу формирования «элитного множества», представленных в Главе 3.

Таблица 6.8 – Оценка производительности СлПО для АК

Операция	**T, сек.**	**N**	**Nt**	**V_{Nt}**	**Nq**	**V_{Nq}**	**Apdex base**	**Оценка (база)**	**Apdex new**	**Оценка (новая)**
Формирование цели ЛПР	30	20	18	0,997	2	0,003	0,95	Отлично	0,90	Хорошо
Формирование функциональных подсистем	120	47	38	0,997	9	0,003	0,90	Хорошо	0,81	Удовл.
Формирование ключевых процессов ИБ	300	48	28	0,997	20	0,003	0,79	Удовл.	0,58	Неприемлемо
Формирование мер и средств контроля ИБ	600	94	65	0,997	29	0,003	0,85	Хорошо	0,69	Неприемлемо
Формирование альтернатив	120	20	18	0,997	2	0,003	0,95	Отлично	0,90	Хорошо
Расчет по системе MPriority	10	100	94	0,997	6	0,003	0,97	Отлично	0,94	Хорошо
Проверка согласованности МПС, ошибок транзитивности	600	90	49	0,997	41	0,003	0,77	Удовл.	0,54	Неприемлемо
Представление результатов ЛПР	120	20	17	0,997	3	0,003	0,93	Хорошо	0,85	Хорошо

Рассмотрим пример возможной применимости на практике метода «мгновенных аудитов» для формирования приемлемого «времени отклика» СлПО в АК. В мае 2015 г. самолет производства Airbus Group разбился в Испании во время испытаний[307]. После взлета три из четырех двигателей перестали работать, четверо членов экипажа погибли. Оказалось, необходимые для работы двигателей данные были случайно стерты, когда сотрудники Airbus Group устанавливали ПО. Расследование инцидента в Минобороны Испании завершилось в 2017 г. и было подтверждено, что данные были удалены. Согласно отчету, в октябре 2014 г. производитель двигателей Europrop International предупредил Airbus Group и European Aviation Safety Agency о том, что ошибки при инсталляции ПО могут привести к потере данных, необходимых для работы двигателей. Как показало расследование, техперсонал не знал о проблеме до крушения A400M, а пилоты не имели инструкций на случай подобного сценария.

Применение широкого перечня критериев аудита хорошо укладывается в иерархическую модель ИСМ для реализации в МАИ (например, как альтернативы, существующие или «*проектируемые*», в нотации Т.Саати), а также позволяет определять весовые коэффициенты, необходимые при расчете численных метрик для оценки уровня обеспечения безопасности (текущего или прогнозного).

6.9 Реализация полученных научных результатов на практике

По результатам накопления и анализа данных (на примере сертификации СМИБ) и знаний (на примере результатов аудита ИБ в СлПО), с учетом динамики происходящих изменений (собственно, СлПо также постоянно изменяются), предлагаются **новые** методы оптимизации процесса управления ИБ в функции ЖЦ и, дополнительно, обоснование бюджета для подсистемы обеспечения ИБ.

Примеры реализации полученных научных результатов в практической деятельности для СлПО различной отраслевой принадлежности наглядно демонстрируют достижение цели исследования и возможность их применения

---

307 https://www.securitylab.ru/news/489596.php

для повышения уровня «зрелости» СМИБ (ИСМ) в интересах повышения стабильности функционирования СлПО (см. таблицу 6.9).

Таблица 6.9 – Результаты, подтверждающие достижения цели исследования

Предприятие	**Акт внедрения**	**Параметр**	**Значение**
Международный аэропорт Алматы (Казахстан)	**Да**	Затраты на систему внутренних аудитов ИБ	Снижены на 5%
Международный аэропорт Астаны (Казахстан)	**Да**	Затраты на систему вн аудитов	Снижены на 4%
ИТСК (РФ)	**Да**	Затраты на систему внутренних аудитов ИБ	Снижены на 2%
АКБ «Рускобанк» (РФ)	**Да**	Уровень соответствия ИБ требованиям СТО БР ИББС	Достигнут уровень 4
AQS (Азербайджан)	**Да**	Результативность обучения аудиторов	Повышена на 15%
ГУП «Водоканал Санкт-Петербурга» (РФ)	**Да**	Результативность обучения аудиторов	Значительно
«Газинформсервис» (РФ)	**Да**	Длительность выполнения аудитов СОИБ	Снижена на 4 месяца

6.10 Выводы к Главе 6

1. Оценка уровня обеспечения безопасности для СлПО – АК формируется по **новой** модели аудита ИБ для ИСМ в АК как оценка результативности по множеству критериев МАИ, оцениваемых в процессе комплексного аудита всех типов. Мерой оценки результативности в предложенной модели аудита ИБ в ИСМ служат численные метрики, предложенные экспертами, утвержденные высшим менеджментом АК и прошедшие апробацию в аналитических сессиях.
2. Входными данными, имеющими наибольшую ценность при проведении комплексного аудита ИБ в ИСМ на реальном объекте – АК, являются данные о структуре документированной информации ИСМ и результатах проведения комплексного аудита всех типов,
3. Выходные данные, полученные на основе модели аудита ИСМ, являются численными, сформированными на основе достоверного математического аппарата (МАИ). Согласованные мнения экспертов прошли строгие математические проверки в МАИ на оценку однородности и нарушение транзитивности в каждой аналитической сессии в среде моделирования MPriority.
4. Подтверждено, что применение **новой** модели ИСМ для проведения аудита ИБ способствует получению численных оценок, применимых для формирования ЛПР обоснованного управленческого решения, направленного на повышение уровня безопасности, устойчивого функционирования и общей экономической эффективности АК. Представленный пример расчета положительно характеризует адекватность работы экспертов в аналитических сессиях по представленной модели ИСМ для аудита ИБ применительно к АК.

Заключение

В диссертационной работе **решена** крупная важная научно-техническая проблема, заключающаяся в создании теоретических основ для снижения длительности и стоимости аудита ИБ, формирования количественной оценки уровня обеспечения ИБ в СлПО, применения наилучшего множества мер (средств) обеспечения ИБ для парирования выявленных рисков в СлПО. Решение данной проблемы имеет научную и практическую ценность для обеспечения безопасности СлПО, в том числе получены следующие научные результаты, составляющие **итоги** диссертационного исследования:

1. Проведено исследование системных требований, предъявляемых к процессам обеспечения ИБ в СлПО и определены закономерности между системными изменениями требований регуляторов, применимыми стандартами (международными, национальными, отраслевыми) и объективными потребностями создания ИСМ для различных отраслей промышленности;

2. Проведено исследование системных требований, предъявляемых при создании современных ИСМ, предназначенных для защиты ценных активов СлПО, в частности, нематериальных активов (*goodwill*), с учетом риск-ориентированного подхода при обеспечении ИБ для СлПО;

3. Проведено исследование и анализ с целью создания иерархической структуры численных показателей (метрик) ИБ в процессах обеспечения ИБ, предназначенных для формирования требований к ИСМ для СлПО;

4. Разработаны обобщенная модель ИСМ для обеспечения безопасности ИСМ, базовая модель аудита ИСМ и система численных показателей (метрик) ИБ для выполнения аудита ИСМ. Раскрыта специфика процесса планирования, выполнения и анализа результатов аудита ИБ в ИСМ, заключающаяся в широком применении системы численных показателей (метрик) ИБ для оценки результативности ИСМ согласно применимым требованиям.

5. Разработан метод проведения аудита ИСМ для СлПО, который, в отличие от известных методов аудита, позволяет учесть расширенный перечень критериев аудита (например, требований регуляторов и/или отраслевой

специфики) и отличается применением численных показателей (метрик) ИБ с учетом специфики обеспечения безопасности различных видов СлПО. Предложенный метод реализует новый принцип управления аудитом ИБ по частоте и предоставляет ЛПР оценку роста уровня обеспечения ИБ в СлПО как показатель результативности (*effectiveness*) СМИБ (ИСМ) и соответствия применимым требованиям.

6. Разработан метод исследования динамики сертификации по международным стандартам ISO для СлПО, основанный на публичных статистических данных ISO, устанавливающий оценку влияния «лидеров» разного ранга и учитывающий приоритеты отраслей в соответствии с международными кодами экономической деятельности ЕАС. Новый метод позволяет оценить «входные» динамические изменения потребностей бизнеса, выраженные в изменении предпочтений ЛПР по составу внедряемых СМ, прошедших внешний (независимый) аудит в составе ИСМ и формировать прогнозные оценки.

7. Разработан метод многошаговой оптимизации процесса аудита ИБ в ИСМ для СлПО, который, в отличие от известных стандартов ISO, обеспечивает координацию, распределение ресурсов и оперативное информирование ЛПР по оценке результативности аудита ИСМ. Предложенный метод обеспечивает научно обоснованное и целенаправленное функционирование СМИБ как самостоятельной СМ или в составе ИСМ, и отличается от существующих методов циклической непрерывной оценкой ИБ на основе оптимальной системы численных показателей (метрик) ИБ.

8. Выполнено исследование практической применимости предложенных моделей и методов обеспечения ИБ в составе ИСМ для СлПО для различных отраслей.

Сформулированы **рекомендации** по применению результатов работы с учетом новых законодательных инициатив (например, ФЗ-187) для обеспечения безопасности объектов критической инфраструктуры РФ. Научные положения, представленные в диссертации, обеспечивают методическое сопровождение

процессов автоматизации формирования численных показателей (метрик) ИБ для выполнения аудита ИСМ, сокращения длительности процессов планирования, выполнения и анализа результатов аудита ИБ в ИСМ для СлПО. Эти показатели применяются при оптимизации процесса аудита ИБ в ИСМ, в том числе, позволяют учесть известные ресурсные ограничения. Также полученные в диссертации результаты создают перспективы для обеспечения оперативного информирования ЛПР по оценке результативности аудита ИСМ и создания системы циклической непрерывной оценкой ИБ на основе оптимальной системы численных показателей (метрик) ИБ.

В качестве **перспектив дальнейшей разработки тематики** могут быть предложены:

1. Разработка модели перехода от фиксированного перечня УБИ к модели комплексного оценивания рисков в процессе реализации аудита ИБ. В прогнозируемой перспективе это позволит обеспечить «единое управленческое поле» в ИСМ для обеспечения безопасности всех процессов в современных и перспективных СлПО.

2. Представление метода имитационного моделирования в режиме, близком к РРВ, с целью создания более эффективной системы комплексной защиты СлПО на основании расширенной теории «элитных групп» с учетом известных и планируемых бюджетных ограничений.

3. Разработка модели реализации комплексного аудита ИБ, которые позволяли бы предоставлять оценки всех процессов в современных системах управления СлПО в едином численном пространстве, а не по отдельности в ИСМ (управление персоналом, управление инцидентами, управление рисками и пр.), что значительно повысило бы шансы на успех в информационном противоборстве с потенциальными злоумышленниками.

Соответствие диссертации паспорту научной специальности. Положения, выносимые на защиту, соответствуют паспорту научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» в части области исследований по п. 1 (теория и

методология обеспечения информационной безопасности и защиты информации); п. 7 (анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения); п. 9 (модели и методы оценки защищенности информации и информационной безопасности объекта), п. 14 (модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности) и п. 15 (модели и методы управления информационной безопасностью).

Перечень сокращений

АИС	–	авиационная инженерная служба
АРМ	–	автоматизированное рабочее место
БД	–	база данных
ГОСТ	–	Государственный стандарт
ИБ	–	информационная безопасность
ИББС	–	информационная безопасность банковской системы
ИС	–	информационная система
ИСМ	–	интегрированная система менеджмента
ИСПДн	–	информационная система персональных данных
ИУС	–	информационно-управляющая система
ЖЦ	–	жизненный цикл
КВО	–	критически важный объект
КИИ	–	критическая информационная инфраструктура
КЗ	–	контролируемая зона
КиПД	–	корректирующие и предупреждающие действия
КС	–	канал связи
ЛВС	–	локальная вычислительная сеть
ЛПР	–	лицо, принимающее решение
МПС	–	Матрица попарных сравнений
МПлС	–	Международная платежная система
МЧС	–	Министерство по чрезвычайным ситуациям
МЭ	–	межсетевой экран
НДВ	–	недокументированные (недекларированные) возможности
НСД	–	несанкционированный доступ
НМА	–	нематериальные активы
НПЗ	–	нефтеперерабатывающий завод
ОВД	–	служба управления воздушного движения
ОЗ	–	объект защиты
ОИ	–	объект информатизации
ОС	–	операционная система
ПДн	–	персональные данные
ПО	–	программное обеспечение
ПС	–	прикладная система
РРВ	–	режим реального времени
САБ	–	служба авиационной безопасности
СВА	–	система внутреннего аудита
СИБ	–	служба информационной безопасности
СКЗИ	–	средство криптографической защиты информации
СлПО	–	сложный промышленный объект
СМИБ	–	система менеджмента информационной безопасности
СМИС	–	структурированная система мониторинга и управления инженерными системами зданий и сооружений
СМК	–	система менеджмента качества

СМНБ	–	система менеджмента непрерывности бизнеса
СОИБ	–	система обеспечения информационной безопасности
СрЗИ	–	средство защиты информации
СТО	–	стандарт организации
СУБД	–	система управления базами данных
СУУ	–	система управления ИТ-услугами
СЭнМ	–	система энергоменеджмента
ТС	–	техническое средство
УБПД	–	угроза безопасности персональных данных
ФСБ	–	Федеральная служба безопасности
ФСТЭК	–	Федеральная служба технического и экспортного контроля
ЭСТОП	–	электро- и светотехническая служба обеспечения полетов
ACL	–	Access Control List (Список контроля доступа)
ATP	–	Advanced Persistent Threat (Целенаправленные атаки)
CA	–	Certification Audit (сертификационный аудит)
Cobit	–	Control Objectives for Information and Related Technologies (Задачи управления для информационных и смежных технологий)
DLP	–	Data Leak Prevention (Система защиты данных от утечки)
IATA	–	International Air Transport Association (Международная ассоциация воздушного транспорта)
IEC	–	International Electrotechnical Commission, (Международная электротехническая комиссия)
IPS	–	Intrusion Prevention System (Система предупреждения вторжений
ISA	–	Internal Security Audit (Внутренний аудит по безопасности)
ISAGO	–	IATA Safety Audit for Ground Operations (Аудит IATA по безопасности наземного обслуживания)
ISO	–	International Standard Organization (ИСО, Международная организация по стандартизации)
MTPD	–	Maximum tolerable period of disruption, (Максимально возможный период прерывания деятельности)
NERC	–	North American Electric Reliability Corporation, (СевероАмериканская электрическая корпорация)
NIST	–	The National Institute of Standards and Technology, (Национальный институт стандартов и технологий)
PCI DSS	–	Payment Card Industry Data Security Standard (стандарт безопасности данных индустрии платёжных карт)
PDCA	–	“Plan – Do – Check - Act” (Планируй – Делай – Проверяй – Действуй, «Цикл Деминга»)
RA	–	Recertification Audit (Ресертификационный аудит)
RTO	–	Recovery time for Objectives (Допустимое время восстановления)
RPO	–	Recovery point for Objectives

		(Допустимая точка восстановления)
SA	–	Surveilance Audit (Надзорный аудит)
SLA	–	Service Level Agreement (Соглашение об уровне сервиса)
SAQ	–	Self-Assessment Questionnaire (Лист самооценки)
SSL	–	Secure Sockets Layer (Уровень защищённых сокетов)
TLS	–	Transport Layer Security (Безопасность транспортного уровня).
QSA	–	Qualified Security Assessor (Аудитор, сертифицированный для проведения внешних проверок безопасности)

Перечень терминов и определений

Автоматизированная система	–	система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
Атака	–	целенаправленные действия нарушителя с использованием технических и / или программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.
Доступ к информации	–	возможность получения информации и ее использования.
Доступность информации	–	состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечить беспрепятственный доступ к информации субъектов, имеющих на это полномочия.
Защита информации от несанкционированного доступа или воздействия	–	деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).
Информационная система персональных данных	–	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Информация	–	сведения (сообщения, данные) независимо от формы их представления.
Ключевая система информационной инфраструктуры	–	Информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан и в результате деструктивных информационных воздействий, на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.
Контролируемая зона	–	пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей

		организации, а также транспортных, технических и иных материальных средств.
Конфиденциальная информация	–	информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.
Локальная вычислительная сеть	–	совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с другими информационными системами, через определенные точки входа/выхода информации, которые являются границей локальной вычислительной сети.
Межсетевой экран	–	локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и / или выходящей из автоматизированной системы.
Недекларированные возможности	–	функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности информации.
Несанкционированный доступ	–	доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.
Объект информатизации	–	совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов, в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.
Персональные данные	–	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Средства вычислительной техники	–	совокупность программных и технических элементов систем обработки данных, способных

		функционировать самостоятельно или в составе других систем.
Субъект доступа	–	лицо или процесс, действия которого регламентируются правилами разграничения доступа.
Удаленный доступ	–	доступ к информационным активам, обрабатываемым в информационной системе, осуществляемый из-за пределов контролируемой зоны, в которой располагаются данные активы посредством использования информационных технологий
Уязвимость объекта защиты	–	слабость одного или нескольких объектов защиты, которая может быть использована одной или несколькими угрозами.
Характеристика безопасности объекта	–	требование к объекту или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.
Целостность информации	–	состояние защищённости информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки и хранения

Список литературы

[1] Абрамов М.В., Азаров А.А., Тулупьев А.Л., Фильченков А.А. Модели распространения информации в социальных медиа. В книге: СОЦИАЛЬНЫЙ КОМПЬЮТИНГ: ОСНОВЫ, ТЕХНОЛОГИИ РАЗВИТИЯ, СОЦИАЛЬНО-ГУМАНИТАРНЫЕ ЭФФЕКТЫ (ISC-14) материалы Третьей Международной научно-практической конференции. – 2014. – С. 112-115.

[2] Авсентьев О.С. Организационно-техническое и правовое обеспечение безопасности инфокоммуникационных систем объектов «критической инфраструктуры» в Российской Федерации / А.Н. Бабкин, С.А. Бабкин // Доклады ТУСУРа. – 2014. – № 2 (32). – С. 27 – 32.

[3] Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Прототип комплекса программ для анализа защищенности персонала информационных систем, построенный на основе фрагмента профиля уязвимостей пользователя // Труды СПИИРАН. – 2012. – Вып. 2(21). – С. 21 - 40

[4] Акимов В.А. и др. Надежность технических систем и техногенный риск: Учебное пособие. Под общей редакцией М.И. Фалеева. – М.: «Деловой Экспресс». 2002. – 368 с.

[5] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (утверждена Заместителем директора ФСТЭК России 15 февраля 2008).

[6] Бир С. Мозг фирмы. – М.:УРСС, 2005. – 416 с.

[7] Бычкова С.М. Доказательства в аудите. // М.: Финансы и статистика, 1998. – 176 с.

[8] Васильков Ю.В., Гущина Л.С. Система менеджмента рисков как инструмент управления экономикой предприятия // Методы менеджмента качества. 2012. № 2. С. 10-15.

[9] Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л., Азаров А.А. Количественные измерения поведенческих проявлений уязвимостей пользователя, ассоциированных с социоинженерными атаками // Труды СПИИРАН. – 2011. – Вып. 4(19). – С. 34 – 47.

[10] Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л. Классификация психологических особенностей, составляющих основу уязвимостей пользователя при угрозе социоинженерных атак // Тр. СПИИРАН. – 2011. – Вып. 2(17). – С. 70–99.

[11] Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М.: Наука. – 1991. – 384 с.

[12] Взрыв газопровода в Сибири в 1982 году [Электронный ресурс]. Режим доступа: http://dic.academic.ru/dic.nsf/ruwiki/625340, свободный. − Загл. с экрана

[13] Винер Н. Кибернетика, или управление и связь в животном и машине. – 2-е издание. – М.: Наука; Главная редакция изданий для зарубежных стран, 1983. – 344 с.

[14] Винер Н. Кибернетика и общество. М.: Издательство иностранной литературы, 1958.

[15] Воронина Л.И. Основы современного бухгалтерского учета и аудита: Учебное пособие: В 2 частях. Ч. 2. Основы аудита. - М.: 1999. - 304 с
[16] Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ, ст. 48.1 [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/popular/gskrf (дата обращения: 12.08.2015).
[17] Гидроэлектростанция Таум Саук [Электронный ресурс]. Режим доступа: http://lifeglobe.net/entry/4987, свободный. − Загл. с экрана
[18] Голощапов А.Н., Рыжов И.В. Общая характеристика и алгоритм проведения внутреннего аудита системы менеджмента качества организации // Экономика и предпринимательство. 2012. № 5 (28). С. 244-248.
[19] ГОСТ Р ИСО 9001-2011 Системы менеджмента качества. Требования // М.: ФАТРиМ, 2013.
[20] ГОСТ Р ИСО 19011-2011 Руководящие указания по проведению аудитов систем // М.: ФАТРиМ, 2011.
[21] ГОСТ Р ИСО/МЭК 17021:2011. Оценка соответствия. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента // М.: ФАТРиМ, 2011.
[22] ГОСТ Р ИСО/ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности // М.: ФАТРиМ.
[23] ГОСТ Р ИСО/МЭК 15408-1 – 2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель // М.: ФАТРиМ, 2012.
[24] ГОСТ Р ИСО/МЭК 15408-2 – 2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности // М.: ФАТРиМ, 2013.
[25] ГОСТ Р ИСО/МЭК 15408-3 – 2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности // М.: ФАТРиМ, 2013.
[26] ГОСТ Р ИСО 15489-1-2007 Система стандартов по информации, библиотечному и издательскому делу. Управление документами, Москва, Стандартинформ, 2007, 34 с.
[27] ГОСТ Р /ISO/TR 15801-2009 Системы электронного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надёжности, Москва, Стандартинформ, 2011, 59 с.
[28] ГОСТ Р ИСО/МЭК 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности, Москва, 2007, 45 с.
[29] ГОСТ Р 18492:2005 Обеспечение долговременной сохранности электронных документов, Москва, Стандартинформ, 2011, 30 с.

[30] ГОСТ Р ИСО/МЭК 20000-1-2013 Информационная технология. Управление услугами. Часть 1. Требования к системе управления услугами // М.: ФАТРиМ, 2014.
[31] ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования // М.: ФАТРиМ, 2014.
[32] ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования // М.: ФАТРиМ, 2008.
[33] ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство // М.: ФАТРиМ, 2010.
[34] ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;
[35] ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функции хеширования;
[36] ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования – для криптографических средств обеспечения режима конфиденциальности информации ограниченного доступа.
[37] ГОСТ Р ИСО 50001-2012 Системы энергетического менеджмента. Требования и руководство по применению // М.: ФАТРиМ, 2012.
[38] ГОСТ Р 50922-2006 Защита информации Основные термины и определения
[39] ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества, Москва, Стандартинформ, 2006, 23 стр.
[40] ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
[41] ГОСТ Р 22.1.12–2005 Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования // М.: ФАТРиМ, 2005.
[42] ГОСТ Р 22.1.13–2013 Безопасность в чрезвычайных ситуациях. Мероприятия по гражданской обороне, мероприятия по предупреждению чрезвычайных ситуаций природного и техногенного характера. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Требования к порядку создания и эксплуатации // М.: ФАТРиМ, 2013.
[43] ГОСТ Р 22.1.14–2013 Безопасность в чрезвычайных ситуациях. Комплексы информационно-вычислительных структурированных систем мониторинга и управления инженерными системами зданий и сооружений. Технические требования. Методы испытаний // М.: ФАТРиМ, 2013.
[44] ГОСТ РО 0043-003-2012 Аттестация объектов информатизации. Общие положения // М.: ФАТРиМ, 2012.

[45] ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения // М.: ФАТРиМ, 2014.
[46] ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем 2006 г. // М.: ФАТРиМ, 2002
[47] ГОСТ Р 52551-2006 Системы охраны и безопасности. Термины и определения // М.: ФАТРиМ, 2006 г.
[48] ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества, Москва, 2006.
[49] ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения // М.: ФАТРиМ, 2008.
[50] ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования // М.: ФАТРиМ, 2010
[51] ГОСТ Р 53893-2010. Руководящие принципы и требования к интегрированным системам менеджмента // М.: ФАТРиМ, 2011.
[52] Гущин А. Система контроля качества аэропортовых услуг как механизм увеличения доли на рынке аэропортового обслуживания и эффективный способ снижения затрат [Электронный ресурс] // МАКС. − 2009. − 2 сентября. − Режим доступа: http://www.aex.ru/docs/2/2009/9/2/801/, свободный. − Загл. с экрана.
[53] Дефлиз Ф.Л., Дженик Г.Р., Рейлли В.М., Хирш М.Б. Аудит Монтгомери // Пер. с англ. под ред. Я.В. Соколова. – М.: Аудит, ЮНИТИ, 1997. – 542 с.
[54] Душа И. Приоткрытый рынок ИБ АСУ ТП // Безопасность Деловой Информации. – 2015. – Вып. 9. – С. 17 – 19.
[55] Ефимов А.Н. Элитные группы, их возникновение и эволюция. // Знание – сила. – 1988, № 1. – С. 56 – 64.
[56] Заварихин Н.М., Потехина Ю.В. Методы аудита [Электронный ресурс] // Аудитор. – 2005. - №7. − Режим доступа: http://www.gaap.ru/articles/metody_audita/, свободный. − Загл. с экрана.
[57] Захаров А.О. Сужение множества Парето на основе замкнутой информации об отношении предпочтения ЛПР // Вестник Санкт-Петербургского Университета. – 2009. – вып. 4. – С. 69 – 82.
[58] Зефиров С.Л., Голованов В.Б. Система менеджмента информационной безопасности организации и измерения. Метрология, метрики, безопасность // Защита информации. Инсайд.– 2008.– № 2 (20). – С. 22-27.
[59] Зикратов И.А., Шаго Ф.Н. Оптимизация мероприятий аудита системы менеджмента информационной безопасности // Информация и космос. – 2014. – № 2. – С. 59-65.
[60] Зикратов И.А., Шаго Ф.Н. Методика оптимизации планирования аудита системы менеджмента информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – № 2 (90). – С. 111-117.

[61] Ильин В. А., Садовничий В. А., Сендов Бл. Х. Глава 3. Теория пределов. Математический анализ / Под ред. А. Н. Тихонова. — 3-е изд., перераб. и доп. // М.: Проспект, 2006. Т. 1. 672 с.

[62] Информационное сообщение по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 25 июля 2014 г. № 240/22/2748 [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.garant.ru/products/ipo/prime/doc/70605558/ (дата обращения: 12.08.2015).

[63] Камышанов П.И. Практическое пособие по аудиту. М.: ИНФРА-М. 1996. – 552. с.

[64] Кини Р.Л., Райфа Х. Принятие решений при многих критериях: Предпочтения и замещения: Пер. с англ./ Под ред. И.Ф. Шехнова. – М.: Радио и Связь. 1981. – 560 с.

[65] Корнеев А.В. Защита инфраструктуры ТЭК от новых средств кибернетического нападения. Опыт борьбы с дистанционным терроризмом // Энергобезопасность и энергосбережение. – 2012. – № 1. – С. 5-10

[66] Корень А.В. Пути повышения эффективности наземного обслуживания в аэропортах России. Стратегический подход и лучшая практика [Электронный ресурс] // 1-я международная конференция «Наземное обслуживание в аэропортах». − 2010. − 7 сентября. − Режим доступа: http://www.aex.ru/docs/2/2010/9/22/1160/, свободный. − Загл. с экрана.

[67] Корн Г., Корн Т. Справочник по математике для научных работников и инженеров // М.: Наука. 1978. 832 с.

[68] Котенко И.В., Саенко И.Б., Юсупов Р.М. Аналитический обзор докладов Международного семинара «Научный анализ и поддержка политик безопасности в кибер-пространстве» (SA&PS4CS 2010) // Труды СПИИРАН. – 2010. – Вып. 2. – С. 226 – 248

[69] Котенко И.В., Юсупов Р.М. Перспективные направления исследований в области компьютерной безопасности // Защита информации. Инсайд. – 2006. – № 2 (8). – С. 46-57.

[70] Краткий отчет о ICCC 2015 [Электронный ресурс] // ICCC. − 2015. − Режим доступа: http://s3r.ru/2015/10/standarty/kratkiy-otchet-o-iccc-2015/, свободный. − Загл. с экрана

[71] Кремков М.В. Особенности внутренних рисков для предприятий топливно-энергетического комплекса // Энергобезопасность и энергосбережение. – 2012. – № 5. – С. 5-8.

[72] Круглов М.Г. Редакционный отчет о VI региональной конференции «Системы менеджмента качества в сфере образования» 3-4 декабря 2014 г.» // Менеджмент качества. – С. 4 – 17.

[73] Кузьмин В.В. Правовое регулирование защиты критически важных для национальной безопасности объектов инфраструктуры населения страны от угроз техногенного и природного характера: дис. канд. юр. наук: 05.26.02 / С.-Петербургский университет государственной противопожарной службы – СПб. – 2009. – 109 л.

[74] Кустов В.Н. Яковлев В.В., Станкевич Т.Л. Эффективное функционирование информационной системы компании при оптимальном уровне ее защищенности // Проблемы информационной безопасности. Компьютерные системы. – 2017. – № 4. – С. 122-127.

[75] Кустов В.Н.. Корниенко А.А., Ададуров С.Е., Глухов А.П., Диасамидзе С.В. Модели управления рисками и ресурсами автоматизированных систем критического применения железнодорожного транспорта с учетом экономического фактора // Известия Петербургского университета путей сообщения. – 2017. – Т. 14. – № 4. – С. 15.

[76] Кустов В.Н. Кирюшкин С.А., Станкевич Т.Л. О подходах к автоматизации процесса аудита операторов сервисов доверия // Известия Петербургского университета путей сообщения. – 2014. – № 3 (40). – С. 169-176.

[77] Лафицкий Алексей. Подход «Лаборатории Касперского» к защите индустриальной сети [Электронный ресурс] // BIS Expert. – 2015. – Режим доступа: http://bis-expert.ru/sites/default/files/archives/2015/bis2015_lafickiy.pdf, свободный. – Загл. с экрана.

[78] Лобанов А.А. и др. Энциклопедия финансового риск-менеджмента. – М.: Альпина Паблишер. – 2003. – 786 с.

[79] Лившиц И.И. Оценка современных условия обеспечения безопасности сложных промышленных объектов / И.И. Лившиц, А.В. Неклюдов, А.Т. Танатарова // Энергобезопасность и энергосбережение. – 2018. – № 2. – С. 5-14. DOI: 10.18635/2071-2219-2018-2-5-14.

[80] Лившиц И.И. Модель интегрированной системы менеджмента для обеспечения безопасности сложных объектов / Лившиц И.И., Фаткиева Р.Р. // Вопросы кибербезопасности. – 2018. – № 1 (25). – С. 64-71. DOI: 10.21681/2311-3456-2018-1-64-71

[81] Лившиц И.И. Менеджмент информационной безопасности // Стандарты и качество. – 2017. – № 9. – С. 48-52.

[82] Лившиц И.И. Гибридная методика оценки безопасности информационных технологий / Лившиц И.И., Неклюдов А.В. // Автоматизация в промышленности. – 2017. – № 7. – С. 36-41.

[83] Лившиц И.И. Анализ существующих ИТ активов для обеспечения информационной безопасности / Лившиц И.И., Неклюдов А.В. // Вопросы защиты информации. – 2017. – № 1 (116). – С. 46-57.

[84] Лившиц И.И. Методика оптимизации программы аудита интегрированных систем менеджмента // Труды СПИИРАН. – 2016. – № 5. – С. 52 – 68. DOI 10.15622/sp.48.3

[85] Лившиц И.И. Нормативное обеспечение эксплуатации средств защиты информации: учебное пособие /А.В. Красов, И.И. Лившиц, Д.В. Юркин, А.В. Малых, Ю.О. Изотова; СПбГУТ. – СПб., 2017. – 68 с.

[86] Лившиц И.И. Управление качеством систем менеджмента информационной безопасности: учебное пособие / А.В. Красов, И.И. Лившиц, Д.В. Юркин, А.В. Малых; СПбГУТ. – СПб., 2016. – 75 с.

[87] Лившиц И.И. Формирование бюджета и оценка результативности системы менеджмента информационной безопасности // Стандарты и качество. – 2016. – № 6. – С. 106-107

[88] Лившиц И.И. Формирование требований к защищенности сложных промышленных объектов // Стандарты и качество. – 2016.– № 2.– С.46-47.

[89] Лившиц И.И. Формирование метрик для измерения результативности систем менеджмента информационной безопасности / И.И. Лившиц, П.А. Лонцих // Вестник Иркутского государственного технического университета. – 2016. – № 5 (112). – С. 65-72.

[90] Лившиц И.И. Оценка методических подходов для формирования систем безопасности сложных промышленных объектов топливно-энергетического комплекса // Вопросы защиты информации. – 2016. – № 1 (112). – С. 56-61.

[91] Лившиц И.И. Практические аспекты аудита информационной безопасности в соответствии с требованиями стандартов СТО БР ИБСС (Точка зрения) // Деньги и кредит. – 2016. – № 2. – С. 54-58

[92] Лившиц И.И. К вопросу оценки соответствия сервисов ДТС требованиям информационной безопасности на основе стандарта ISO 27001 // Оборонный комплекс - научно-техническому прогрессу России. – 2016. – № 1 (129). – С. 7-14.

[93] Лившиц И.И. Оценка защищенности объектов топливно-энергетического комплекса//Энергобезопасность и энергосбережение.–2015.–№ 5.–С.5–10.

[94] Лившиц И.И. Формирование концепции мгновенных аудитов информационной безопасности // Труды СПИИРАН. – 2015. – № 6. – С. 253 – 270.

[95] Лившиц И.И. Определение активов при внедрении и сертификации СМИБ // Стандарты и качество. – 2015. – № 6 (936). – С. 84 – 85.

[96] Лившиц И.И. Методика выполнения комплексных аудитов промышленных объектов для эффективного внедрения энергоменеджмента // Энергобезопасность и энергосбережение. – 2015. – № 3. – С. 10-15.

[97] Лившиц И.И. Анализ современных трендов по сертификации систем менеджмента информационной безопасности по требованиям ISO 27001 / И.И. Лившиц, П.А. Лонцих // Вестник Иркутского государственного технического университета. – 2015. – № 3. – С. 268 – 273.

[98] Лившиц И.И. Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации: ИСО 27001 и СТО Газпром / И.И. Лившиц, А.В. Полещук // Труды СПИИРАН. – 2015. – № 3. – С. 33 – 44.

[99] Лившиц И.И. К вопросу оценки результативности при внедрении систем менеджмента информационной безопасности // Оборонный комплекс – научному прогрессу. – 2015. – № 2. – С. 3 – 9.

[100] Лившиц И.И. Анализ уязвимостей и угроз национальной платежной системы Российской Федерации // Вопросы защиты информации. – 2015. – № 1. – С. 75 – 80.

[101] Лившиц И.И. Методический подход к оценке защищенности информации в телекоммуникационных системах на основе анализа их доступности / И.И. Лившиц, В.В. Маликов // Вестнік Сувязі. – 2015. – № 2. – С. 57-61.

[102] Лившиц И.И. Исследование несанкционированного доступа к системам безналичных электронных платежей / И.И. Лившиц, В.В. Маликов // Вестнік Сувязі. – 2015. – № 5. – С. 52-56

[103] Лившиц И.И. Внутренний аудит в интегрированных системах менеджмента / И.И. Лившиц, А.Т.Танатарова // Стандарты и качество. – 2014. – № 8 (926). – С. 86-88.

[104] Лившиц И.И. Внедрение систем энергоменеджмента в соответствии с требованиями ISO 50001:2011 для промышленных объектов // Энергобезопасность и энергосбережение. – 2014. – № 6. – С. 9 – 12.

[105] Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН.– 2014.– № 6.– С.72 – 94.

[106] Лившиц И.И. Концепция оценки уровня информационной безопасности сервис-провайдеров информационных систем для промышленных объектов // Труды СПИИРАН. – 2014. – № 4 (35). – С. 117 – 135.

[107] Лившиц И.И. Исследование зависимости сертификации по международным стандартам ISO от типов организации для ведущих отраслей промышленности / И.И. Лившиц, А.А. Молдовян, А.Т. Танатарова // Труды СПИИРАН. – 2014. – № 3 (34). – С. 160 –177.

[108] Лившиц И.И. Подходы к оценке уязвимостей и угроз информационной безопасности для объектов критичной инфраструктуры Российской Федерации на примере национальной платежной системы / И.И. Лившиц, М.М. Кучерявый // Информатизация и связь. – 2014. – № 3. – С. 35 – 39.

[109] Лившиц И.И. Стандарты ISO/IEC, ITIL и CobiT в контексте требований к информационной безопасности // Менеджмент качества. – 2013. – № 2. – С. 94 – 106.

[110] Лившиц И.И. Применение модели СМИБ для оценки защищенности интегрированных систем менеджмента // Труды СПИИРАН. – 2013. – № 8 (31). – С. 147 – 162.

[111] Лившиц И.И. Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на

основании требований международных стандартов BSI / ISO // Информатизация и связь. – 2013. – № 6. – С. 62– 67.

[112] Лившиц И.И. Подходы к решению проблемы учета потерь в интегрированных системах менеджмента // Информатизация и связь. – 2013. – № 1. – С. 57 – 62.

[113] Лившиц И.И. Подходы к синтезу модели оценки защищенности персональных данных в соответствии с требованиями стандарта ISO/IEC 27001:2005 // Труды СПИИРАН. – 2012. – № 4 (23). – С. 80 – 92.

[114] Лившиц И.И. Современная практика аудита информационной безопасности // Управление качеством. – 2011. – № 7. – С. 34 – 41.

[115] Лившиц И.И. Информационная безопасность. Интеграция международных стандартов в систему информационной безопасности России / И.И. Лившиц, И.Ф. Козин // Информатизация и связь. – 2010. – № 1. – С. 50 – 55.

[116] Лившиц И.И. Проектирование, создание и внедрение комплексных систем обеспечения информационной безопасности на базе ISO/IEC 27001:2005 // Электросвязь. – 2010. – № 4. – С. 49 – 51

[117] Лившиц И.И Модели обеспечения безопасности сложных промышленных объектов на базе риск-ориентированного подхода. / Лившиц И.И, Подолянец Л.А. // В сборнике: Материалы конференции «Моделирование и Анализ Безопасности и Риска в Сложных Системах (МАБР - 2015)». – Санкт-Петербург. – 2015. – С. 188 – 193.

[118] Лившиц И.И. Актуальные задачи обеспечения информационной безопасности в процессах жизненного цикла информационных систем / Лившиц И.И., Молдовян А.А. // В сборнике: Материалы конференции «Информационные технологии в управлении (ИТУ – 2014)». – Санкт-Петербург. – 2014. С. 623 – 630.

[119] Лившиц И. И. Подходы к решению проблем обеспечения непрерывности бизнеса в интегрированных системах менеджмента посредством аудита информационной безопасности в соответствии с требованиями международных стандартов // В сборнике: Материалы конференции XXVIII научно-практической конференции Комплексная защита информации». – Брест. – 2013. – С. 84-86.

[120] Лившиц И.И. Практика проведения GAP-анализа и аудита SLA при создании современной системы управления услугами // Материалы III-й Всероссийской конференции itSMF. – Москва. – 2012.

[121] Лившиц И. И. Современная практика проведения аудитов ИБ // В сборнике: Материалы XVI научно-практической конференции «Комплексная защита информации». – Гродно. – 2011.

[122] Лим В.Г., Арбузов Ю.А., Химич В.Н., Дзиоев С.К. Моделирование угроз информационной безопасности в АСУ предприятия топливно-энергетического комплекса // Вопросы защиты информации. – 2010. –№ 3. – С. 23-27.

[123] Липатников В.А., Шевченко А.А., Яцкин А.Д., Семенова Е.Г. Управление информационной безопасностью организации интегрированной

структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. – 2017. – № 4(89). – С. 59-67.

[124] Липатников В.А., Шевченко А.А. Модель процесса управления информационной безопасностью распределенной информационной системы на основе выявления и оценки уязвимостей // Информационные системы и технологии. – 2018. – № 1 (105). – С. 114-123.

[125] Липатников В.А., Сахаров Д.В., Кузнецов И.А. Управление АСМК организации интегрированной структуры с прогнозированием состояния информационной безопасности // Электросвязь. – 2016. – № 3. – С. 28-36.

[126] Макух М. Роль аудита в формировании добавленной стоимости при оценке бизнеса // Международная научно-практическая конференция «Многогранность оценки бизнеса: проблемы и перспективы в условиях формирования наукоемкой экономики, КазЭУ им Т. Рыскулова, Алматы, 16.05.2014.

[127] Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. М.: Мир. 1973. — 334 с., ил.

[128] Методика Apdex – стандарт оценки производительности корпоративных приложений [Электронный ресурс] // [Офиц. сайт]. URL: http://www.gilev.ru/apdex-teoriya (дата обращения 19.01.2015).

[129] Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6-432);

[130] Меры защиты информации в государственных информационных системах (Утвержден ФСТЭК России 11 февраля 2014);

[131] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена руководством ФСТЭК России 14.02.2008);

[132] Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий [Офиц. сайт]. URL: http://www.mchs.gov.ru/dop/terms/item/86502 (дата обращения: 12.08.2015).

[133] Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: Лань, 2001. — 224 с., ил.

[134] Молдовян А.А., Молдовян Н.А. Новые алгоритмы и протоколы для аутентификации информации в АСУ, Автоматика и телемеханика, 2008. – № 7. – С. 157–169

[135] Молдовян А.А., Молдовян Н.А., Еремеев, А. А. Защитные преобразования информации в АСУ на основе нового примитива. Автоматика и телемеханика, 2002. – № 12. – С. 147–165

[136] Молдовян А.А., Молдовян Н.А. Метод скоростного преобразования для защиты информации в АСУ. Автоматика и телемеханика, 2000. – № 4. – С. 151–165.

[137] Молдовян А.А., Молдовян Н.А. Гибкие алгоритмы защиты информации в АСУ. Автоматика и телемеханика, 1998. – № 8. – С.166–176.

[138] Надежность и эффективность в технике: Справочник в 10 т./Ред. совет: В.С. Авдуевский, (пред.) и др. – М.: Машиностроение, 1988. – (в пер.) Т. 3. Эффективность технических систем/Под общ. ред. В.Ф. Уткина, Ю.В. Крючкова. – 328 ст.: ил.

[139] Нехорошкин Н.И. Проблемы и возможности информационно-аналитического обеспечения аудита проектов и программ // Вестник АКСОР. 2010. Т. 1. № 12. С. 41-45.

[140] Николис Г., Пригожин И. Познание сложного. Введение. М., Мир, 1990. – 345 с.

[141] Ногин В.Д. Принятие решений при многих критериях // Государственный Университет – Высшая школа экономики, Санкт-Петербург, 2007, 103 стр.

[142] Нормативно-методический документ Федеральной службы по техническому и экспортному контролю России – Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, 2008.

[143] Нормативно-методический документ Федеральной службы по техническому и экспортному контролю России – Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, 2008.

[144] Нормативно-методический документ Федеральной службы по техническому и экспортному контролю России – Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, 2008.

[145] Нормативно-методический документ Федеральной службы по техническому и экспортному контролю России – Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, 2008.

[146] Нургалиев Р. К., Зарипов Р. Н., Флакс Д. Б., Даутова Э. У. Промышленные сети передачи данных // Вестник Казанского Технологического Университета. – 2013. – Том 16. – Вып. – № 11, стр. 252-254

[147] Петухов Алексей. Подход к обеспечению ИБ АСУТП подстанций [Электронный ресурс]. – Режим доступа: http://www.itsecurityforum.ru/itsf-2015/materials/ (дата обращения 23.06.2015)

[148] Петренко С.А. Требования SOX 404 к контролю ИТ // Защита информации. Инсайд. – 2006, № 3 (9). – С. 10-16.

[149] Петров Илья. Комплексный подход к обеспечению защит информации в АСУ ТП [Электронный ресурс]. – Режим доступа: http://www.itsecurityforum.ru/itsf-2015/materials/ (дата обращения 23.06.2015)

[150] Пригожин И., Стенгерс И. Время. Хаос. Квант. К решению парадокса времени. М.: Едиториал УРСС, 2003. – 240 с.

[151] Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ // М.: Высшая школа. 1989. – 360 с.

[152] Положение по аттестации объектов информатизации по требованиям безопасности информации. (Утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.)

[153] Положение о сертификации средств защиты информации по требованиям безопасности информации. (Утв. Приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. N 199).

[154] Попов А.В., Семенюк А.П., Еременко Н.В. Моделирование бизнес-процессов обслуживания пассажиров аэропорта // РАДІОЕЛЕКТРОННІ І КОМП'ЮТЕРНІ СИСТЕМИ, 2011 No 4 (52)

[155] Постановление Правительства РФ от 21.05.2007 N 304 «О классификации чрезвычайных ситуаций природного и техногенного характера» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_law_68490/ (дата обращения: 12.08.2015).

[156] Постановление Правительства РФ от 22.12.2011 N 1107 «О порядке формирования и ведения реестра объектов топливно-энергетического комплекса» (вместе с «Правилами формирования и ведения реестра объектов топливно-энергетического комплекса») [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_124278/ (дата обращения: 12.08.2015).

[157] Постановление Правительства РФ от 05.05.2012 №458 «Об утверждении правил по обеспечению безопасности и антитеррористической защищенности объектов топливно- энергетического комплекса» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_law_179479/ (дата обращения: 12.08.2015).

[158] Постановление Правительства РФ от 05.05.2012 №459 «Об утверждении Положения об исходных данных для проведения категорирования объекта топливно-энергетического комплекса» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://base.consultant.ru/cons/CGI/online.cgi?req=doc;base=LAW;n=129654 (дата обращения: 12.08.2015).

[159] Постановление Правительства РФ от 05.05.2012 №460 «Об утверждении Правил актуализации паспорта безопасности объекта топливно-энергетического комплекса» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://base.consultant.ru/cons/CGI/online.cgi?req=doc;base=LAW;n=129654 (дата обращения: 12.08.2015).

[160] Постановление Правительства Российской Федерации от 01.11.2012 №1119 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных/ [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт].

URL: http://www.consultant.ru/document/cons_doc_law_137356/ (дата обращения: 12.08.2015).

[161] Постановление Правительства от 2 октября 2013 года №861 «Об утверждении Правил информирования субъектами топливно-энергетического комплекса об угрозах совершения или совершении актов незаконного вмешательства на объектах топливно-энергетического комплекса» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_152677/ (дата обращения: 12.08.2015).

[162] Постановление Правительства РФ от 22.09.2009 № 754 (ред. от 06.04.2013) Положение о системе МЭДО [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_91827/ (дата обращения: 15.11.2016).

[163] Постановление Правительства РФ от 06.09.2012 № 890 (ред. от 21.07.2014) О мерах по совершенствованию электронного документооборота в ОГВ [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_135055/ (дата обращения: 15.11.2016).

[164] Постановление Правительства РФ от 25.12.2014 № 1494 Правила обмена документами в электронном виде при организации информационного взаимодействия [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_172990/ (дата обращения: 15.11.2016).

[165] Постановление Государственного комитета Российской Федерации по статистике от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;

[166] Приказ Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. N 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;

[167] Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 12.08.2015).

[168] Приказ Минэнерго России от 10.02.2012 N 48 «Об утверждении методических рекомендаций по включению объектов топливно-энергетического комплекса в перечень объектов, подлежащих

категорированию» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=137344 (дата обращения: 12.08.2015).

[169] Приказ ФСТЭК России от 18.02.2013 № 21 Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

[170] Приказ Минкомсвязи России № 186, ФСО России № 258 от 27.05.2015 Требования к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде (Зарегистрировано в Минюсте России 22.09.2015 N 38956) [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_186762/ (дата обращения: 15.11.2016).

[171] Письмо Госстроя от 06.06.2013 N 5061-ДБ/12/ГС «О разъяснении нормативно-правовых и нормативно-технических документов в области проектирования особо опасных производственных объектов» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/law/ hotdocs/26392.html (дата обращения: 12.08.2015).

[172] Оценка производительности системы по методике Apdex [Электронный ресурс] // [Офиц. сайт]. URL: http://tavalik.ru/metodika-apdex (дата обращения 19.01.2015)

[173] Официальный сайт Infosecurity Russia [Электронный ресурс]. – Режим доступа:www.infosecurityrussia.ru/2015/program/23.09.2015/?lang=ru#s22083 свободный (дата обращения 18.04.2016).

[174] Официальный сайт IT Security Forum 2015. [Электронный ресурс]. – Режим доступа: http://www.itsecurityforum.ru/itsf-2015/materials/ свободный (дата обращения 23.06.2015).

[175] Официальный сайт Центрального Банка РФ URL: www.cbr.ru (дата обращения 07.07.2015).

[176] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012 N 803) [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_150730/ (дата обращения: 23.05.2016).

[177] Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. – М.: Наука, 2006. – 410 с.

[178] Распоряжение Правительства РФ от 27.08.2005 N 1314-р «Об одобрении Концепции федеральной системы мониторинга критически важных объектов инфраструктуры Российской Федерации и опасных грузов» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_55325/ (дата обращения: 12.08.2015).

[179] Распоряжение Правительства РФ от 02.10.2009 № 1403-р Технические требования к организации взаимодействия системы МЭДО ФОИВ [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_92231/ (дата обращения: 15.11.2016).

[180] Распоряжение Правительства РФ от 02.04.2015 № 583-р Перечень видов документов, передаваемых при взаимодействии ФОИВ, ОИВ субъектов РФ, ГВФ в электронном виде [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_177621/ (дата обращения: 15.11.2016).

[181] Рудакова С.А. Концепция выбора метрик информационной безопасности // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. – 2013. – № 3 (22). – С. 162-166.

[182] Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства. ОБСЕ. – 2013. – 96 стр.

[183] Сайт Федерального государственного унитарного предприятия «Предприятие по поставкам продукции Управления делами Президента Российской Федерации» [Электронный ресурс]. – М.: ФГУП «ППП», 2015. – Режим доступа: http://www.certifsecurity.ru, свободный. – Загл. с экрана.

[184] Сайт Издательского дома «Connect» [Электронный ресурс]. – М.:, 2015. – Режим доступа: http://www.connect.ru/article.asp?id=10607, свободный. – Загл. с экрана.

[185] Сайт Корпоративного журнала «Jet Info» [Электронный ресурс]. – 2011. – Режим доступа: http://www.jetinfo.ru/stati/asu-tp-voprosy-bezopasnosti, свободный. – Загл. с экрана.

[186] Сайт портала «Security Lab» [Электронный ресурс]. – 2015. – Режим доступа: http://www.securitylab.ru/blog/personal/Business_without_danger/130461.php, свободный. – Загл. с экрана.

[187] Сайт «ЦентрПроектЗащита» [Электронный ресурс]. – 2014. – Режим доступа: http://17.mchs.gov.ru/upload/site64/iblock/fdc/fdc9dd18dcb05a1c4ee457f3d9834d97.pdf, свободный. – Загл. с экрана.

[188] Сайт портала Scribd [Электронный ресурс]. – 2007. – Режим доступа: http://ru.scribd.com/doc/212339737/ANSI-ISA-99-00-01-2007-pdf, свободный. – Загл. с экрана.

[189] Сайт портала ITSec Pro [Электронный ресурс]. – 2012. – Режим доступа: http://www.itsec.pro/2013/05/0043-003-2012.html, свободный. – Загл. с экрана.

[190] Сайт Федеральной службы по техническому и экспортному контролю России [Электронный ресурс]. – 2013. – Режим доступа: http://fstec.ru/component/attachments/download/574, свободный. – Загл. с экрана.

[191] Сайт портала ISO27000.ru [Электронный ресурс]. – 2013. – Режим доступа: http://www.iso27000.ru/blogi/aleksandr-astahov/kogda-i-dlya-kogo-attestaciya-obekta-informatizacii-yavlyaetsya-obyazatelnoi, свободный. – Загл. с экрана.

[192] Сайт портала IT Law Wiki [Электронный ресурс]. – 2009. – Режим доступа: http://itlaw.wikia.com/wiki/ANSI/ISA-62443-2-1_(99.02.01)-2009, свободный. – Загл. с экрана.

[193] Сайт портала ISA [Электронный ресурс]. – 2009. – Режим доступа: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731, свободный. – Загл. с экрана.

[194] Сайт портала ICS Cert [Электронный ресурс]. – 2009. – Режим доступа: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf, свободный. – Загл. с экрана.

[195] Сайт компании «Normdocs» [Электронный ресурс]. – 2014. – Режим доступа: http://normdocs.ru/isa, свободный. – Загл. с экрана.

[196] Сайт Department of Homeland Security [Электронный ресурс]. – 2007. – Режим доступа: http://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf, свободный. – Загл. с экрана.

[197] Сайт American Petroleum Institute [Электронный ресурс]. – 2015. – Режим доступа: http://www.api.org/, свободный. – Загл. с экрана.

[198] Сайт American Gas Association [Электронный ресурс]. – 2015. – Режим доступа: https://www.aga.org/, свободный. – Загл. с экрана.

[199] Сайт International Electrotechnical Commission [Электронный ресурс]. – 2015. – Режим доступа: https://webstore.iec.ch/publication/6591&preview=1, свободный. – Загл. с экрана.

[200] Сайт International Electrotechnical Commission [Электронный ресурс]. – 2015. – Режим доступа: https://webstore.iec.ch/publication/6591&preview=1, свободный. – Загл. с экрана.

[201] Сайт International Electrotechnical Commission [Электронный ресурс]. – 2015. – Режим доступа: https://webstore.iec.ch/publication/5879, свободный. – Загл. с экрана.

[202] Сайт International Electrotechnical Commission [Электронный ресурс]. – 2015. – Режим доступа: https://webstore.iec.ch/publication/7033, свободный. – Загл. с экрана.

[203] Сайт International Electrotechnical Commission [Электронный ресурс]. – 2015. – Режим доступа: https://webstore.iec.ch/publication/6903, свободный. – Загл. с экрана.
[204] Сайт АКОРБ [Электронный ресурс]. – 2015. – Режим доступа: http://npk.akforb.ru/upload/doc/2015/Туруев.pdf, свободный. – Загл. с экрана.
[205] Сайт АКОРБ [Электронный ресурс]. – 2015. – Режим доступа: http://npk.akforb.ru/upload/doc/2015/Поморина.pdf, свободный. – Загл. с экрана.
[206] Сайт АКОРБ [Электронный ресурс]. – 2015. – Режим доступа: http://npk.akforb.ru/2015/, свободный. – Загл. с экрана.
[207] Сайт Hirshmann [Электронный ресурс]. – 2015. – Режим доступа: http://www.hirschmann.ru/industrial/catalog/iec61850/mach1000.series, свободный. – Загл. с экрана.
[208] Сайт Hirshmann [Электронный ресурс]. – 2015. – Режим доступа: http://www.hirschmann.ru/industrial/catalog/eagle/, свободный. – Загл. с экрана.
[209] Скрыль С.В., Белокуров С.В., Зыбин Д.Г., Громов Ю.Ю., Кондратов О.А. Показатели эффективности информационных процессов в интегрированных системах безопасности в условиях угроз искажения и блокирования информации // Приборы и системы. Управление, контроль, диагностика. – 2014, № 4. – С. 23-27.
[210] Смирнов Михаил. Практика противодействия сложным нацеленным атакам [Электронный ресурс]. – Режим доступа: http://www.itsecurityforum.ru/itsf-2015/materials/ (дата обращения 23.06.2015)
[211] Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), (приложение к приказу Гостехкомиссии России от 03.08.2002 № 282).
[212] Соколов Б.В., Юсупов Р.М. Комплексное моделирование функционирования автоматизированной системы управления навигационными космическими аппаратами // Проблемы управления и информатики. – 2002. – № 5. – С. 103-117.
[213] Соколов Б.В., Юсупов Р.М. Концептуальные основы оценивания и анализа качества моделей и полимодельных комплексов // Теория и системы управления. – 2004. – № 6. – С. 5-16.
[214] Соколов Б.В., Юсупов Р.М. Неокибернетика в современной структуре системных знаний // Робототехника и техническая кибернетика, 2014, вып. 3, стр. 3 – 11.
[215] Соколов Б.В., Юсупов Р.М. Концептуальная и теоретико-множественная модель управления структурной динамикой космических средств // Мехатроника, автоматизация, управление. 2003. № 5.С. 17-25.
[216] Соколов Я.В. Очерки по истории бухгалтерского учета. М.: Финансы и статистика, 1991. – 400 с
[217] Соловьев С.М. Публичные чтения о Петре Великом. М.: Наука, 1984.

[218] Стандарт Банка России СТО БР ИББС-1.0-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения // М.: Банк России, 2014.
[219] Стандарт Банка России СТО БР ИББС-1.1-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности // М.: Банк России, 2014.
[220] Стандарт Банка России СТО БР ИББС-1.2-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 // М.: Банк России, 2014.
[221] СТО Газпром 4.2-0-004-2009 Система обеспечения информационной безопасности ОАО «Газпром». Базовая модель угроз информационной безопасности корпоративным информационно-управляющим системам, 2009.
[222] СТО Газпром 4.2-1-001-2009 Система обеспечения информационной безопасности ОАО «Газпром». Основные термины и определения, 2009
[223] СТО Газпром 4.2-2-001-2010 Система обеспечения информационной безопасности ОАО «Газпром». Система обеспечения информационной безопасности ОАО «Газпром». Требования к информационно-управляющим системам предприятия, 2010.
[224] СТО Газпром 4.2-2-002-2009 Система обеспечения информационной безопасности ОАО «Газпром». Требования к автоматизированным системам управления технологическими процессами, 2009.
[225] СТО Газпром 4.2-3-002-2009 Система обеспечения информационной безопасности ОАО «Газпром». Требования по технической защите информации при использовании информационных технологий, 2009.
[226] СТО Газпром 4.2-3-003-2009 Система обеспечения информационной безопасности ОАО «Газпром». Анализ и оценка рисков, 2009.
[227] СТО Газпром 4.2-3-004-2009 Система обеспечения информационной безопасности ОАО «Газпром». Правила классификации объектов защиты, 2009
[228] СТО Газпром 4.2-3-004-2009 Система обеспечения информационной безопасности ОАО «Газпром». Классификация объектов защиты, 2009.
[229] СТО Газпром 4.2-3-005-2013 Система обеспечения информационной безопасности ОАО «Газпром». Управление инцидентами информационной безопасности, 2013
[230] Суворова А.В., Мусина В.Ф., Тулупьева Т.В., Тулупьев А.Л., Красносельских Т.В., Фильченков А.А., Азаров А.А., Абдала Н. Автоматизированный инструментарий для опроса респондентов об эпизодах рискованного поведения: первичный анализ результатов применения // Труды СПИИРАН. 2013. Вып. 3(26). 175 – 193
[231] Терелянский П.В., Кременов С.И. Реализация метода анализа иерархий для оценки конкурентоспособности компьютерных фирм // Вестник

Волгоградского государственного университета. Серия 3: Экономика. Экология. 2008. № 2. С. 35-43.

[232] Тулупьев А.Л., Пащенко А.Е., Азаров А.А. Информационные модели компонент комплекса «Информационная система – персонал», находящегося под угрозой социоинженерных атак // Труды СПИИРАН. 2010. Вып. 3(14). С. 50–57.

[233] Тулупьев А.Л., Пащенко А.Е., Азаров А.А. Информационная модель пользователя, находящегося под угрозой социоинженерной атаки // Труды СПИИРАН. 2010. Вып. 2(13). С. 143–155.

[234] Тулупьева Т.В., Тулупьев А.Л., Азаров А.А. Психологические аспекты оценки безопасности в контексте социоинженерных атак // Медико-биологические и социально-психологические проблемы безопасности в чрезвычайных ситуациях. 2013. № 1. С. 77-83.

[235] Федеральный закон от 30.11.1994 № 51-ФЗ «Гражданский кодекс Российской Федерации (часть первая)» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_5142 (дата обращения: 12.08.2015).

[236] Федеральный закон от 06.04.20111 № 63-ФЗ «Об электронной подписи» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 21.05.2016)

[237] Федеральный закон от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/Cons_doc_LAW_5295/ (дата обращения: 21.05.2016)

[238] Федеральный закон от 21.07.1997 N 116-ФЗ «О промышленной безопасности опасных производственных объектов», ст. 2 п. 1 [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_15234/ (дата обращения: 12.08.2015).

[239] Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=133341 (дата обращения: 12.08.2015).

[240] Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://base.consultant.ru/cons/CGI/online.cgi?req=doc;base=LAW;n=166051;frame=434 (дата обращения: 12.08.2015).

[241] Федеральный закон Российской Федерации от 27.06.2011 № 161-ФЗ «О национальной платежной системе» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 12.08.2015).

[242] Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_34447/ (дата обращения: 12.08.2015).

[243] Федеральный закон от 27.12.2002 N 184-ФЗ (ред. от 28.11.2015) «О техническом регулировании» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_40241/ (дата обращения: 12.12.2015).

[244] Федеральный закон от 11 июля 2011 г. N 190-ФЗ «Об обращении с радиоактивными отходами и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_law_116552/ (дата обращения: 12.08.2015).

[245] Федеральный закон от 30.12.2001 № 197-ФЗ «Трудовой кодекс Российской Федерации» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_law_34683/ (дата обращения: 12.08.2015).

[246] Федеральный закон от 27.07.2010 № 225-ФЗ «Об обязательном страховании гражданской ответственности владельца опасного объекта за причинение вреда в результате аварии на опасном объекте» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156785 (дата обращения: 12.08.2015).

[247] Федеральный закон от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_117196/ (дата обращения: 12.08.2015).

[248] Федеральный закон от 03.12.2011 № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_122558/ (дата обращения: 12.08.2015).

[249] Федеральный закон от 29 ноября 2010 г. N 314-ФЗ «О внесении изменения в статью 48.1 Градостроительного кодекса Российской Федерации» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL:

http://www.consultant.ru/document/cons_doc_LAW_107278/ (дата обращения: 12.08.2015).

[250] Федеральный закон от 28 ноября 2011 г. N 337-ФЗ «О внесении изменений в Градостроительный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_122221/ (дата обращения: 12.08.2015).

[251] Федеральный закон от 4 декабря 2007 г. N 324-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (с изменениями и дополнениями) [Электронный ресурс] // Компания «КонсультантПлюс» [Офиц. сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_73033/ (дата обращения: 12.08.2015).

[252] Шахраманьян М. А., Ларионов В. И., Нигметов Г. М. и др. Комплексная оценка риска от чрезвычайных ситуаций природного и техногенного характера // Безопасность жизнедеятельности. 2001. № 12. – С. 8—14.

[253] Шишкин В. М. Степенное распределение и управление рисками критических систем // Проблемы управления рисками и безопасностью: Труды Института системного анализа Российской академии наук: Т.31. М.: КомКнига, 2007. – С. 39–59.

[254] Шишкин В. М. Концептуальная модель оценивания защищенности объектов информатизации, опыт использования в учебном процессе // Информатика – исследования и инновации». Сб.научных трудов. ЛГОУ им. А.С. Пушкина. – СПб: 2000. – С. 114-116.

[255] Шишкин В.М., Юсупов Р.М. Доктрина информационной безопасности Российской Федерации — опыт количественного моделирования // Труды СПИИРАН. Вып. 1, т. 1. - СПб: СПИИРАН, 2002.

[256] Шмельова Т.Ф., Сікірда Ю.В., Ассаул О.Ю. Вплив факторів середовища менеджменту авіапіприемства на безпеку авіаційної діяльності // Технологический аудит и резервы производства. 2015. Т. 2. № 3 (22). С. 17-24.

[257] Щеглов А.Ю. Вопросы защиты информации. Без комментариев. [Электронный ресурс] /

[258] Щербина В. Новые подходы к стандартам по безопасности сложных технических систем // Межотраслевой тематический каталог «Системы безопасности 2015». С. 63 – 65.

[259] Юсупов Р. М, Шишкин В. М. О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. Вып. 6. — СПб.: Наука, 2008. С. 39–59.

[260] Юсупов Р.М., Заболотский В.П. Показатели оценивания состояния и результатов развития информационного общества // Труды СПИИРАН. 2010, Вып. 4, стр. 75 – 84.

[261] Юсупов Р.М., Соколов Б.В. Проблемы развития кибернетики и информатики на современном этапе // Сб. «Кибернетика и информатика». – СПб.: Изд-во СПбГПУ, 2006. – С. 6-21.
[262] Юсупов Р.М. Наука и национальная безопасность. СПб.: Наука, 2006.
[263] Юсупов Р. М., Шульц В.Л. Национальная безопасность и наука // Труды СПИИРАН. 2009. Вып. 10. с. 11 -32
[264] Abdullah L., Jaafar S., Taib I. Ranking of Human Capital Indicators Using Analytic Hierarchy Process. Procedia - Social and Behavioral Sciences. 2013. V. 107. P. 22-28.
[265] Abdullah K., Lee C., et al. IDS Rainstorm: Visualizing ids alarms. IEEE Workshops on Visualization for Computer Security, 2005.
[266] Acquisti A. and H.R. Varian, Conditioning Prices on Purchase History, Marketing Science, vol. 24, no 3, 2005, pp. 1–15.
[267] Acquisti A. Personalized Pricing, Privacy Technologies, and Consumer Acceptance, CHI Workshop on Personalization and Privacy, 2006; www.isr.uci.edu/pep06/papers/Proceedings_PEP06.pdf.
[268] Acquisti A. Privacy and Security of Personal Information: Economic Incentives and Technological Solutions, The Economics of Information Security, J. Camp and S. Lewis, eds., Kluwer, 2004.
[269] Andrew Jaquith. Security Metrics: Replacing Fear, Uncertainty, and Doubt 1st Edition. Addison-Wwsley, 2007, ISBN 0785342349986
[270] An Introduction to ISO 27001, ISO 27002 … ISO 27008, The ISO 27000 Directory, 2009;
[271] Apdex Is Not Just For Application Performance [Электронный ресурс] // [Офиц. сайт]. URL: http://www.apdex.org/index.php/2014/05/apdex-is-not-just-for-application-performance/ (дата обращения 19.01.2015)
[272] Amazon, The Software Company, Economist, 18 Dec. 2001; www.economist.com/displayStory.cfm?Story_ID=393096.
[273] Arvanitis A., Gregory J. Credit: The complete guide to pricing, hedging and risk management. — L.: Risk Books, 2001.
[274] Balepin, I., Maltsev, S., Rowe, J., Levitt, K. Using specification-based intrusion detection for automated response. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, pp. 135-154 (2003)
[275] Banking in the Cloud, TEMENOS, 2011;
[276] Basak Manders, Henk J. de Vries. Does ISO 9001 pay? - Analysis of 42 studies. (http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1665, дата обращения 15.03.2016)
[277] Bertini E., Hertzog P., Lalanne D. SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms. IEEE Symposium on Visual Analytics Science and Technology (VAST) 2007
[278] Belcsak H. P. Country risk assessment/In: Clark B. W. Handbook of international credit management. 3rd ed. — L.: Gower Publishing Co.,
[279] Bohme R. and S. Koble, “On the Viability of Privacy-Enhancing Technologies in a Self-regulated Business to Consumer Market: Will Privacy Remain a

Luxury Good?," Proc. Workshop on Economics of Information Security (WEIS 07), 2007.
[280] Box G.E.P. Evolutionary Operation: A Method of Increasing Industrial Productivity // Applied Statistics. – 1957. – Vol. 6 – Pp. 81-101.
[281] Brands S. Rethinking Public Key Infrastructure and Digital Certificates - Building in Privacy, MIT Press, 2000.
[282] Cannon D., Certified Information Systems Auditor Study Guide, 3rd ed., Wiley, 2011.
[283] Calzolari G. and A. Pavan, "On the Optimality of Privacy in Sequential Contracting," J. Economic Theory, vol. 130, no. 1,2006.
[284] Center for strategic and International Studies [Электронный ресурс]. – Режим доступа: www.csis.org свободный (дата обращения 18.04.2016).
[285] Cisco Report 2016 [Электронный ресурс] // [Офиц. сайт]. URL: http://www.cisco.com/c/dam/m/ru_ru/offers/assets/pdfs/cisco_2016_asr_011116_ru.pdf (дата обращения 10.05.2016).
[286] CipherCloud Enables Healthcare Pioneer to Deliver a Medical Audit Solution, CipherCloud, 16 May 2012;
[287] CloudAudit: Automated Audit, Assertion, Assessment, and Assurance, CloudAudit, 12 Feb. 2010;
[288] Chaum D. "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. ACM, vol. 28, no. 10, 1985, pp. 1030–1044.
[289] Chaum D. "Blind Signatures for Untraceable Payments," Advances in Cryptology (CRYPTO 82), Plenum Press, 1983, pp. 199–203.
[290] Chowdhury P. Das, B. Christianson, and J. Malcolm, "Privacy Systems with Incentives, Proc. First Int'l Workshop Information Systems, 2006.
[291] Danezis G. and D. Martin, eds., 2006, pp. 259–272; www.petworkshop. org/2005/workshop/call.html.
[292] Das Chowdhury P., Anonymity and Trust in the Electronic World, PhD thesis, computer science dept., Univ. of Hertfordshire, 2005.
[293] Deloitte. Governance, Risk and Compliance [Электронный ресурс] // [Офиц. сайт]. URL: http://www.lopdf.net/d/Deloitte-SAP-GRC-services.pdf (дата обращения 19.01.2015).
[294] DEMACHI Kouji, AKABANE Kuniharu, NAKAJIMA Takeshi, YOKOI Toyoaki Vnet/IP REAL-TIME PLANT NETWORK SYSTEM [Электронный ресурс] // [Офиц. сайт]. URL: http://cdn2.us.yokogawa.com/rd-tr-r00039-005.pdf (дата обращения 19.01.2015).
[295] Derek L. Nazaretha, Jae Choib // A system dynamics model for information security management // Information & Management Volume 52, Issue 1, January 2015, Pages 123–134
[296] Dr. Gary Hinson // Seven Myths about information Security metrics // ISSA Journal, July 2006
[297] FedRAMP: Ensuring Secure Cloud Computing for the Federal Government, US General Services Administration, 20 Nov. 2012;

[298] Federal Information Security Management Act (FISMA) [Электронный ресурс]. – Режим доступа: www.csrc.nist.gov свободный (дата обращения 18.04.2016).
[299] Gentry C., “A Fully Homomorphic Encryption Scheme,” PhD dissertation, Dept. Computer Science, Stanford Univ., Sept. 2009;
[300] Hansen M. et al., “Privacy-Enhancing Identity Management,” Information Security Tech. Report, vol. 11, no.3, 2006, 119–128.
[301] Harrison, L., Spahn, R., Iannacone, M., Downing, E., Goodall, J.R.: NV: Nessus Vulnerability Visualisation for the Web. Proc. of the VizSec’12, October 15 2012, Seattle, WA, USA (2012)
[302] Heitzmann A., Palazzi B., Papamanthou C., Tamassia R. Effective Visualisation of File System Access-Control. 5th international workshop on Visualisation for Computer Security (VizSec'08), LNCS, Vol.5210, Springer-Verlag, Berlin, Heidelberg, 2008.
[303] Hermalin B. and M. Katz, “Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy,” Quantitative Marketing and Economics, vol. 4, no. 3, 2006, pp. 209–239.
[304] Hubert K. Rampersad. Total Quality Management: An Executive Guide to Continuous Improvement Hardcover – March 1, 2001
[305] ICCC International Common Criteria Conference 2015 [Электронный ресурс] // ICCC. − 2015. − Режим доступа: https://www.iccc15.org.uk/Speakers.aspx, свободный. − Загл. с экрана
[306] Information Supplement: PCI DSS Cloud Computing Guidelines,” Cloud Special Interest Group PCI Security Standards Council 2013;
[307] ISO 27001 – Compliance and Audit Solutions [Электронный ресурс] // [Офиц. сайт]. URL: http://governify.com/wp-content/uploads/2011/12/ISMS_DataSheet.pdf (дата обращения 19.01.2015).
[308] ISO [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/annual_report_2014_en_-_lr.pdf свободный (дата обращения 18.04.2016).
[309] ISO [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/iso-survey свободный (дата обращения 18.04.2016).
[310] ISO [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO%209001&countrycode=AF свободный (дата обращения 15.03.2016).
[311] ISO/IEC 20000-1:2011 «Information technology - Service management - Part 1: Service management system requirements»
[312] ISO/IEC 20000-2:2012 «Information technology - Service management - Part 2: Guidance on the application of service management systems»
[313] ISO/IEC 20000-3:2012 «Information technology - Service management - Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1»
[314] The Business Model for Information Security, ISBN 978-1-60420-154-3, 2010 г.

[315] ISO 22301:2012 «Societal security. Business continuity management systems. Requirements», International Organization for Standardization, 2011. – 24 pages;
[316] ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Organization for Standardization, 2014. – 31 pages;
[317] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013. – 23 pages.
[318] ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement, International Organization for Standardization, 2009. – 55 pages;
[319] ISO/IEC 27005-2011 Information technology — Security techniques — Information security risk management, International Organization for Standardization, 2011. – 68 pages;
[320] ISO/IEC 27013:2015 Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1, International Organization for Standardization, 2015. – 39 pages;
[321] ISO 50001:2011 Energy management systems – Requirements with guidance for use, International Organization for Standardization, 2011. – 22 pages;
[322] ISO 55000:2014 Asset management – Overview, principles and terminology // International Organization for Standardization, 2014. – 19 pages.
[323] ISO 55001:2014 Asset management – Management systems – Requirements // International Organization for Standardization, 2014. – 14 pages.
[324] ISO 55002:2014 Asset management – Management systems – Guidelines for the application of ISO 55001 // International Organization for Standardization, 2014. – 32 pages.
[325] ISAGO Standards Manual Effective, January 2014 3rd Edition;
[326] IATA Reference Manual for Audit Programs, November 2012 3rd Edition;
[327] ISAGO & IGOM & GDDB Integrated solution for improved Ground Safety, Joseph Suidan Head of Ground Operations, ULD Care, May 2013;
[328] Jahnke, M., Thul, C., Martini, P. Graph based metrics for intrusion response measures in computer networks. LCN 2007: Proceedings of the 32nd IEEE Conference on Local Computer Networks, Washington, DC, USA, pp. 1035-1042. IEEE Computer Society, Los Alamitos (2007)
[329] Jansen W. and Grance T., “Guidelines on Security and Privacy in Public Cloud Computing,” Nat’l Inst. Standards and Technology, Dec. 2011;
[330] Krag Brotby // Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement Hardcover // 211 pages, March 30, 2009, ISBN 9781420052855
[331] Komiya Hiroyoshi, et al., FCS Compact Control Station in CENTUM CS R3, Yokogawa Technical Report, No. 38, 2004, pp. 5-8
[332] Koble S. and R. Bohme, “Economics of Identity Management: A Supply-side Perspective,” Privacy Enhancing Technologies Workshop (PET 05),

[333] Kurka T. Application of the analytic hierarchy process to evaluate the regional sustainability of bioenergy developments // Energy. 2013. V. 62. P. 393-402.
[334] Laurence Frank Business models for airports in a competitive environment. One sky, different stories, Research in Transportation Business & Management, Volume 1, Issue 1, August 2011, Pages 25–35
[335] Lawrence Gordon, Martin Loeb // Managing Cybersecurity Resources: A Cost-Benefit Analysis // The Mcgraw-Hill Homeland Security Series, 1st Edition // 2005, 224 pages, ISBN-13: 9780071452854
[336] Lee Preston, James Post's // Private Management and Public Policy: The Principle of Public Responsibility // 2012, 192 pages, ISBN 9780804783866
[337] Li B., Chang X. Application of Analytic Hierarchy Process in the Planning of Energy Supply Network for Electric Vehicles // Energy Procedia. 2011. Vol.12. P. 1083-1089.
[338] Livshitz I., Neklyudov A., Lontsikh P. Evaluation of IT security – genesis and its state-of-art. IOP Conf. Series: Journal of Physics: Conf. Series 1015 (2018) 042029 **DOI**: 10.1088/1742-6596/1015/4/042029.
[339] Livshitz I.I., Lontsikh, P.A., Lontsikh, N.P., Kunakov, E.P., Drolova, E.Y. Implementation and auditing of risk management for the oil and gas company. Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. DOI: 10.1109/ITMQIS.2017.8085881
[340] Livshitz, I.I., Ezrahovich, A.Y., Vladimirtsev, A.V., Karasev, S.N., Drolova, E.Y. Assessment of the impact of the modern risk-oriented standards on the security of the complex industrial facilities. Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. DOI: 10.1109/ITMQIS.2017.8085873
[341] Livshitz, I.I., Ezrahovich, A.Y., Vladimirtsev, A.V., Lontsikh, P.A., Karaseva, V.A. Risk-based thinking of ISO 9001:2015 - The new methods, approaches and tools of risk management. Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017 DOI: 10.1109/ITMQIS.2017.8085872
[342] Livshitz, I.I., Nikiforova, K.A., Lontsikh, P.A., Karasev, S.N. The new aspects for the instantaneous information security audit. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS. DOI: 10.1109/ITMQIS.2016.7751920
[343] Livshitz, I.I., Nikiforova, K.A., Lontsikh, P.A., Karaseva, V.A. The evaluation of the electronic services with accordance to IT-security requirements based on ISO/IEC 27001. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. DOI: 10.1109/ITMQIS.2016.7751921
[344] Livshitz, I.I., Lontsikh, P.A., Karaseva, V.A., Kunakov, E.P., Nikiforova, K.A. Implementation of information security and data processing center protection standards. 2016 IEEE Conference on Quality Management, Transport and

Information Security, Information Technologies, IT and MQ and IS 2016. DOI: 10.1109/ITMQIS.2016.7751923

[345] Livshitz, I.I., Nikiforova, K.A., Lontsikh, P.A., Drolova, E.Y., Lontsikh, N.P. The optimization of the integrated management system audit program. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS. DOI: 10.1109/ITMQIS.2016.7751919

[346] Livshitz, I.I., Yurkin, D.V., Minyaev, A.A. Formation of the Instantaneous Information Security Audit Concept. Distributed Computer and Communication Networks, 2016. https://doi.org/10.1007/978-3-319-51917-3_28.

[347] Livshitz I., Lontsikh P., Eliseev S. The Method of Implementation of the Numerical IT-Security Metrics in Management Systems. Proceedings of the FRUCT'20 (3-7 April 2017) pp. 242 – 248. ISSN 2305-7254. DOI: 10.23919/FRUCT.2017.8071318

[348] Livshitz I., Lontsikh P., Eliseev S. The Optimization Method of the Integrated Management System Security Audit. Proceedings of the FRUCT'20 (3-7 April 2017) pp. 248 – 254. ISSN 2305-7254. DOI: 10.23919/FRUCT.2017.8071319

[349] Livshitz Ilya, Podolyanets Lada. Models of Complex Industrial Facilities Assessment Based on Risk Approach. International Review of Management and Marketing, 2016, N.6 (S5) pp. 125-135. ISSN: 2146-4405

[350] Low S., N.F. Maxemchuk, and S. Paul, "Anonymous Credit Cards," Proc. 2nd ACM Conf. Computer and Communications Security, ACM Press, 1994, pp. 108–117.

[351] Luca S. Public engagement in strategic transportation planning: An analytic hierarchy process based approach // Transport Policy.2014.Vol.33.pp. 110-124.

[352] Marouf S., Shehab M. SEGrapher: Visualization-based SELinux PolicyAnalysis. 4th Symposium on Configuration Analytics and Automation (SAFECONFIG), 2011.

[353] Mansmann F., Göbel T., Cheswick W. Visual Analysis of Complex Firewall Configurations. VizSec'12, October 15, 2012, Seattle, WA, USA, 2012.

[354] Mario Linkies, Horst Karin SAP Security and Risk Management // Galileo Press. – 2010. – 742 P.

[355] Mell P. and Grance T., "The NIST Definition of Cloud Computing," NIST special publication 800-145, 2011; http://csrc.nist.gov/publications/nistpubs/800-145 /SP800-145.pdf.

[356] Morvay Z., Gvozdenac D. Applied Industrial Energy and Environmental Management // John Wiley & Sons, Chichester, UK, 2008.

[357] Number of U.S. government 'cyber incidents' jumps in 2015 Reuters [Электронный ресурс]. – Режим доступа: http://www.reuters.com/article/us-usa-cyber-idUSKCN0WN263 свободный (дата обращения 10.08.2015).

[358] Odlyzko A., "Privacy, Economics, and Price Discrimination on the Internet," Proc. 5th Int'l Conf. Electronic Commerce, ACM Press, 2003, pp. 355–366.

[359] Odlyzko A., "The Evolution of Price Discrimination in Transportation and its Implications for the Internet," Rev. Network Economics, vol. 3, no. 3, 2004, pp. 323–346.

[360] Pauley W.A., “Cloud Provider Transparency: An Empirical Evaluation,” IEEE Security & Privacy, vol. 8, no. 6, 2010, pp. 32–39.
[361] Paul R. Carlile, Davide Nicolini, Ann Langley, and Haridimos Tsoukas // How Matter Matters. Objects, Artifacts, and Materiality in Organization Studies //2013, 316 pages // ISBN 9780199671533
[362] PAS-99:2012 «Specification of common management system requirements as a framework for integration»
[363] QlikView Reference Manual [Электронный ресурс] – URL: http://semanticommunity.info/@api/deki/files/24990/QlikView_Reference_Manual.pdf – Режим доступа: свободный (дата обращения: 8.05.2015).
[364] Randall P., Brown L., Deschaine L., Dimarzio J., Kaiser G., Vierow J. Application of the analytic hierarchy process to compare alternatives for the long-term management of surplus mercury // Journal of Environmental Management. 2004. Vol. 71. Iss. 1. P. 35-43.
[365] RAROC and risk management: Quantifying the risks of business. Bankers Trust New York Corporation, 1995.
[366] Resetting the Definition of IT-GRC at Gartner [Электронный ресурс]. – 2016. – Режим доступа: http://blogs.gartner.com/paul-proctor/2013/05/15/resetting-the-definition-of-it-grc-at-gartner/, свободный. – Загл. с экрана.
[367] Reeder R. W., Bauer L., Cranor L. F., et al. Expandable grids for visualizing and authoring computer security policies. SIGCHI Conference on Human Factors in Computing Systems (CHI '08). ACM, New York, NY, USA, 2008.
[368] Reporting on Controls at Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)—AICPA Guide. January 2012, American Institute of CPAs, 2012.
[369] Recommended Security Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Revision 4, Nat’l Inst. Standards and Technology, 2009
[370] Security Self-Assessment Guide for Information Technology Systems. NIST Special Publication SP 800-26, Nat’l Inst. Standards and Technology, 2009
[371] Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30, Nat’l Inst. Standards and Technology, 2009
[372] Recommended Security Controls for Federal Information Systems. NIST Special Publication SP 800-53, Nat’l Inst. Standards and Technology, 2009;
[373] Robert Cook, Transforming Airport Business Models, http://www.forbes.com/sites/wheelsup/2010/09/02/transforming-airport-business-models/(дата обращения 15.03.2016).
[374] RSA Archer GRC Summit 2013 [Электронный ресурс] // [Офиц. сайт]. URL: http://www.emc.com/collateral/solution-overview/h12373-2013-archer-grc-summit-key-findings.pdf (дата обращения 19.01.2015)
[375] RSA Archer ISMS Foundation [Электронный ресурс] // [Офиц. сайт]. URL: http://www.emc.com/collateral/data-sheet/isms-data-sheet.pdf (дата обращения 19.01.2015).
[376] RSWB v.1.2.1. Часть 2. Системы безопасности / Yokogawa ProSafe-RS. – Москва. – 2006. – с. 10 – 19.

[377] Safe Harbor 2.0 framework begins to capsize as January deadline nears [Электронный ресурс]. – 2015. – Режим доступа: http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/, свободный. – Загл. с экрана.

[378] Security and Privacy Controls for Federal Information Systems and Organizations (Rev.4) [Электронный ресурс] // NIST. − 2013. − Режим доступа: http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf, свободный. − Загл. с экрана

[379] Security Report [Электронный ресурс]. – Режим доступа:https://www.trustwave.com/Resources/Library/Documents/Security-on-the-Shelf---An-Osterman-Research-Survey-Report/ свободный (дата обращения 18.04.2016).

[380] SOC Reports, American Institute of CPAs, 2013.

[381] Smith, Gordon E. (1992, ASQC) Massey University, Palmerston North, New Zealand, Auditing Statistical Methods for ISO 9001. Annual Quality Congress, Nashville TN Vol. 46 No. 0, QICID: 9905 May 1992 pp. 849-854

[382] Spiekermann S., “Individual Price Discrimination: An Impossibility?” CHI Workshop on Personalization and Privacy, 2006; www.isr.uci.edu/pep06/papers/Proceedings_PEP06.pdf.

[383] Steve Doe // Security and Emergency Management for Water Systems // ISBN: 9781934493069

[384] Streamline, Automate, Operationalize ISO 27001 & 27002 initiative [Электронный ресурс] // [Офиц. сайт]. URL: http://www.emc.com/security/rsa-archer-governance-risk-compliance/rsa-archer-isms-foundation.htm (дата обращения 19.01.2015)

[385] Taylor C.R., “Consumer Privacy and the Market for Customer Information,”RAND J. Economics, vol. 35, no. 4, 2004, pp. 631–651.

[386] Tran T., Al-Shaer E., Boutaba R. PolicyVis: Firewall Security Policy Visualisation and Inspection. 21st Conference on Large Installation System Administration Conference (LISA’07), USENIX Association, Berkeley, CA, USA, 2007.

[387] The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid [Электронный ресурс]. – 2015. – Режим доступа: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf, свободный. – Загл. с экрана.

[388] The Global State of Information Security Survey 2016 [Электронный ресурс]. – Режим доступа: www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml/ свободный (дата обращения 18.04.2016)

[389] The Global State of Information Security Survey 2015. – [Электронный ресурс]: – Режим доступа: http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml, свободный (дата обращения 24.03.2015)

[390] The Wall Street Journal, [Электронный ресурс]. – 2015. – Режим доступа: http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407/, свободный. – Загл. с экрана.

[391] Toth, T., Krugel, C. Evaluating the impact of automated intrusion response mechanisms. ACSAC 2002: Proceedings of the 18th Annual Computer Security Applications Conference, Washington, DC, USA, p. 301. IEEE Computer Society, Los Alamitos (2002).

[392] Varian H., Economic Aspects of Personal Privacy, in Privacy and Self-Regulation in the Information Age, NTIA report, 1996; www.sims.berkeley.edu/hal/people/hal/papers.html.

[393] Varian H.R., “Price Discrimination and Social Welfare,” Am. Economic Rev., vol. 75, no. 4, 1985, pp. 870–875.

[394] White Paper «Dealing with Data Breaches and Data Loss Prevention» [Электронный ресурс]. – Режим доступа: https://www.proofpoint.com/de/id/PPWEB-WP-Osterman-Data-Breaches-and-DLP-Q115 свободный (дата обращения 18.04.2016).

[395] Wall Street Journal, 9/18/14 “Chinese Hacked U.S. Military Contractors, Senate Panel Say”, [Электронный ресурс] - http://www.slideshare.net/SelectedPresentations/08-smorodinsky, – Режим доступа: свободный (дата обращения 23.03.2015).

Приложение А Акты, подтверждающие реализацию результатов работы

Приложение А.1 Акт о внедрении АО «Международный Аэропорт Алматы»

УТВЕРЖДАЮ
Вице - президент по экономике и развитию
АО «Международный аэропорт Алматы»
Мамеков Даулет Абирбекович
«26» 09 2014г.

АКТ

об использовании результатов диссертационной работы на соискание ученой степени «доктор технических наук» Лившица Ильи Иосифовича

Акционерное общество «Международный аэропорт Алматы» («Алматы халықаралық әуежайы» АҚ) подтверждает, что результаты диссертационной работы на соискание ученой степени доктора технических наук Лившица И.И. внедрены и используются в процессах развития основных направлений деятельности основных служб. Научные и практические результаты, полученные Лившицем И.И. и опубликованные в работе «Ценность внутренних аудитов интегрированной системы менеджмента для проведения результативного анализа со стороны руководства / Стандарты и Качество. 2014 г., применяются в АО «Международный аэропорт Алматы» («Алматы халықаралық әуежайы» АҚ) при обеспечении безопасности процессов основной деятельности, связанных с исследованием:

- требований, предъявляемых при создании современной ИСМ, основанной на управлении рисками промышленных объектов;
- практической применимости предложенных методов обеспечения безопасности в ИСМ.

Сформированные Лившицем И.И подходы, способствующие снижению издержек в процессе разработки и внедрения ИСМ и минимизацию потерь при возникновении ситуаций риска, присущих промышленным объектам, нашли свое применение в процессах совершенствования сложных организационно-технических систем деятельности аэропорта.

Использование результатов исследования Лившица И.И. позволило повысить результативность процессов разработки и внедрения современных систем менеджмента для обеспечения безопасности объектов критических инфраструктур АО «Международный аэропорт Алматы» («Алматы халықаралық әуежайы» АҚ). Полученный экономический эффект от внедрения и использования ИСМ с учетом предложенных научных и практических результатов Лившица И.И. привел, по предварительным оценкам, к оптимизации на 5% затрат на систему проведения внутренних аудитов.

Председатель комиссии:
Руководитель отдела менеджмента качества — **Валуева Татьяна Тарасовна**

Члены комиссии:
Начальник службы теплотехнического и санитарно-технического обеспечения — **Усов Вячеслав Петрович**

Начальник службы АвиаГСМ — **Тумышев Куаныш Мажитович**

Начальник службы электро-светотехнического обеспечения полетов — **Вальтер Юрий Иванович**

Начальник службы безопасности и охраны труда — **Аманов Насип Аманович**

Приложение А.2 Акт о внедрении АО «Международный Аэропорт Астаны»

"АСТАНА ХАЛЫҚАРАЛЫҚ ӘУЕЖАЙЫ"
Акционерлік қоғамы
Құжаттың шығыс № _____
_____ _____ 20__ ж.

УТВЕРЖДАЮ

Заместитель председателя Правления
АО «Международный аэропорт Астана»

Р. Адимолда
«15» сентября 2014г.

АКТ

об использовании результатов диссертационной работы на соискание ученой степени «доктор технических наук» Лившица Ильи Иосифовича

Акционерное общество «Международный аэропорт Астаны» («Астана халықаралық әуежайы» АҚ) подтверждает, что результаты диссертационной работы на соискание ученой степени доктора технических наук Лившица И.И. внедрены и используются в процессах развития основных направлений деятельности основных служб. В частности, научные результаты, полученные Лившицем И.И. и опубликованные в работах: «Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов ISO», Информатизация и Связь, 2013 и «Ценность внутренних аудитов ИСМ для проведения результативного анализа со стороны руководства, Стандарты и Качество, 2014 г., применяют в АО «Международный аэропорт Астаны» («Астана халықаралық әуежайы» АҚ) в процессах, связанных с исследованием и формированием основных принципов:

- научных основ создания и интеграции современных систем менеджмента (ИСМ);
- формирования критериев обеспечения безопасности объектов критических инфраструктур;
- применения моделей и методов исследований в сложных (интегрированных) системах.

Сформированная Лившицем И.И. система требований, предъявляемых к процессам обеспечения безопасности промышленных объектов, нашла свое применение в процессах анализа сложных организационно-технических систем деятельности аэропорта. Использование результатов диссертационного исследования Лившица И.И. позволило повысить результативность процессов разработки и внедрения современных систем менеджмента для обеспечения безопасности объектов критических инфраструктур АО «Международный аэропорт Астаны» («Астана халықаралық әуежайы» АҚ). Полученный экономический эффект от внедрения ИСМ с учетом предложенных научных результатов Лившица И.И. привел, по предварительным оценкам, к оптимизации на 4 % затрат на систему проведения внутренних аудитов.

Председатель комиссии:
Управляющий директор по производству — **Кишшакбаев Сейл Бахитжанович**

Члены комиссии:
Начальник отдела управления СМК — **Аубакирова Айдана Бейбитовна**

Начальник службы электросветотехнического обеспечения полетов — **Шамбергер Иван Францевич**

Начальник службы досмотра — **Ахметов Жоламан Нурмадиевич**

Начальник службы поисково-аварийно-спасательного обслуживания полетов — **Островский Леонид Медортович**

Приложение А.3 Акт о внедрении ООО «ИТСК»

УТВЕРЖДАЮ
Директор департамента инфраструктуры
Дирекции по инфраструктуре и связи
ООО «Информационно – технологическая
сервисная компания»
_____ Тарасанов И. В.
«01» октября 2013 г.

АКТ

об использовании результатов диссертационной работы на соискание ученой степени «доктор технических наук» Лившица Ильи Иосифовича

ООО «Информационно – технологическая сервисная компания» (ИТСК) подтверждает, что результаты диссертационной работы на соискание ученой степени доктора технических наук Лившица И.И. внедрены и используются в процессах развития компетенций по планированию, организации и выполнению аудитов интегрированной системы менеджмента (ИСМ) в составе системы менеджмента качества (ISO 9001) и системы управления ИТ-услугами (ISO 20000).

В частности, научные результаты, полученные Лившицем И.И. и опубликованные в работах: «Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов ISO», Информатизация и Связь (2013 г.) и «Применение моделей СМИБ для оценки защищённости интегрированных систем менеджмента // Труды СПИИРАН. (2013 г.) применяются в ИТСК в процессах, связанных с исследованием и формированием основных принципов:

- научных основ создания и интеграции современных систем менеджмента (ИСМ);
- применения моделей и методов исследований в сложных (интегрированных) системах;
- практической применимости предложенных методов обеспечения безопасности в ИСМ.

Сформированная Лившицем И.И. система требований, предъявляемых к обеспечению аудитов критичных объектов, нашла свое применение в процессах анализа сложных организационно-технических систем ИТСК, как одной из крупнейших ИТ компаний России. Использование результатов диссертационного исследования Лившица И.И. позволило повысить результативность процессов поддержания и совершенствования систем менеджмента в составе ИСМ для обеспечения безопасности инфраструктуры Московского нефтеперерабатывающего завода в структуре ОАО «Газпром нефть». Полученный экономический эффект от внедрения ИСМ с учетом предложенных научных результатов Лившица И.И. привел, по предварительным оценкам, к оптимизации на 2 % затрат на систему проведения внутренних аудитов в 2012-2013 гг.

Председатель комиссии:
Директор департамента инфраструктуры
Дирекции по инфраструктуре и связи _____ Тарасанов И. В.

Члены комиссии:
Помощник директора Дирекции по инфраструктуре и связи _____ / Колесова Е. А.

_____ / Лившиц И.И.

_____ / Коскинен Л.В.

_____

_____

Приложение А.4 Акт о внедрении «AQS Group of Companies»

ADVANCED
QUALITY
SOLUTIONS

bsi. ASSOCIATE CONSULTANT PROGRAMME

УТВЕРЖДАЮ
AQS Group Of Companies
J. Jabbarli str. 44, Caspian Plaza 1, 6th floor, AZ 1065, Baku, Azerbaijan
T: +994 12 4970328 |
F: +994 12 4970329 |
azer.taghiyev@aqs.az
www.aqs.az

/ Azer Taghiyev

«11» January 2016 г.

АКТ

об использовании результатов диссертационной работы на соискание ученой степени доктора технических наук Лившица Ильи Иосифовича (Специальность: 05.13.19 – «Методы и системы защиты информации, информационная безопасность»)

AQS Group Of Companies подтверждает, что результаты диссертационной работы на соискание ученой степени доктора технических наук Лившица И.И. используются в процессах обучения по курсам аудитов систем менеджмента информационной безопасности (СМИБ), интегрированных систем менеджмента (ИСМ), в том числе для сложных промышленных объектов (СлПО) в соответствии с требованиями PAS 99 и международных стандартов BS и ISO/IEC.

Следующие научные результаты (методика исследования динамики сертификации по международным стандартам ISO для СлПО, метод многошаговой оптимизации процесса аудитов ИСМ для СлПО), полученные лично Лившицем И.И и опубликованные в работах: «Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI / ISO» (Информатизация и Связь, 2013 г., вып. 6), «Информационная безопасность и интеграция международных стандартов в систему информационной безопасности России» (Информатизация и Связь, 2010 г., вып. 1) применялись в AQS Group Of Companies в период 2012 – 2014 гг.

Предложенный Лившицем И.И. метод многошаговой оптимизации процесса аудитов ИСМ для СлПО нашел свое применение в процессах обучения аудиторов / ведущих аудиторов, проводимых AQS Group Of Companies на соответствие требованиям PAS 99 и стандартов ISO/IEC серии 27001, 31000, 50001 и 9001. Использование результатов диссертационного исследования Лившица И.И. позволило повысить общую удовлетворенность слушателей в процессе обучения в AQS Group Of Companies на 15% в среднем по данным итоговых аттестаций.

Председатель комиссии:
Executive Director / Azer Taghiyev

Члены комиссии:

Training Manager "AQS Group of Companies" / S. Salimzade

Business Development Manager
"AQS Group of Companies" / F. Vakilov

Приложение А.5 Акт о внедрении АО «Рускобанк»

УТВЕРЖДАЮ
Директор
АО «Рускобанк», 188640,
Ленинградская обл., г. Всеволожск,
Всеволожский пр., д. 29.

_____ / Ю.М. Тавдидишвили
«___» _____ 2015 г.

АКТ

об использовании результатов диссертационной работы на соискание ученой степени доктора технических наук Лившица Ильи Иосифовича (Специальность: 05.13.19 – «Методы и системы защиты информации, информационная безопасность»)

АО «Рускобанк» подтверждает, что результаты диссертационной работы на соискание ученой степени доктора технических наук Лившица И.И. внедрены и используются в процессах выполнения аудитов информационной безопасности, оценки и самооценки защищенности сложных информационных объектов в соответствии с требованиями СТО БР ИББС версии 2014 г. и ISO/IEC 27001 версии 2013 г.

Следующие научные результаты (модель оптимизации проведения аудитов кредитных организаций, модель управления приоритетными изменениями показателей информационной безопасности, совместное решение задач максимизации показателей информационной безопасности и минимизации затрат и времени на внедрение реализацию мер и средств обеспечения информационной безопасности) полученные лично Лившицем И.И и опубликованные в работах: «Определения активов при внедрении и сертификации СМИБ» (Стандарты и Качество, 2015, вып. 6), «Методическое обеспечение процесса оценки банковских продуктов в соответствии с требованиями современных стандартов ISO» (Деньги и кредит, 2014 г., вып. 6) и «Practical aspects of Information Security audits in accordance with the requirements of Bank Standards» (Proceeding ISPIT, 2015) и применяются в АО «Рускобанк» в следующих процессах:

- оценки соответствия обеспечения информационной безопасности требованиям СТО БР ИББС
- управления инцидентами информационной безопасности в автоматизированной банковской системе.
- внутреннего аудита системы обеспечения информационной безопасности.

Предложенная Лившицем И.И. модель оптимизации проведения аудитов в системе обеспечения информационной безопасности кредитных организаций, нашла свое применение в процессах годового цикла аудитов информационной безопасности АО «Рускобанк» на соответствие требованиям СТО БР ИББС-1.0-2014, а также при формировании рекомендаций по повышению уровня обеспечения информационной безопасности.

Использование результатов диссертационного исследования Лившица И.И. позволило повысить результативность процессов обеспечения ИБ кредитной организации – АО «Рускобанк». Полученный результат от внедрения рекомендаций по повышению уровня обеспечения информационной безопасности с учетом

предложенных научных результатов Лившица И.И. обеспечил итоговое повышение уровня соответствия информационной безопасности до рекомендованного 4 уровня, согласно СТО БР ИББС-1.2-2014.

Председатель комиссии:
Заместитель директора _____ / Голосов А.И.

Члены комиссии:

Заместитель начальника Управления безопасности _____ / Гиркин В.С.

Начальник Управления информационных технологий _____ / Музелин О.Ю.

Начальник Отдела информационной безопасности Управления безопасности _____ / Нестерук Ф.Г., к.т.н., доцент

Приложение А.6 Акт о внедрении ООО «Газинформсервис»

GiS
Общество с ограниченной ответственностью
«ГАЗИНФОРМСЕРВИС»
198096, г. С-Петербург, ул. Кронштадтская, д.10, литера А
Почтовый адрес: 198096, г. Санкт-Петербург, а/я 59
тел.: (812) 305-20-50, факс: (812) 305-20-51
E-mail: resp@gaz-is.ru, www.gaz-is.ru

р/с 40702810000050000251 в Санкт-Петербургском
филиале ОАО «ФОНДСЕРВИСБАНК»
БИК 044030717, к/с 30101810200000000717,
ОКПО 72410666, ОГРН 1047833006099,
ИНН/КПП 7838017968 / 780501001

04.04.2016 № 1239
На № _____

Председателю диссертационного совета
Д 002.199.01 при
Федеральном государственном
бюджетном учреждении науки
Санкт-Петербургского института
информатики и автоматизации РАН
(СПИИРАН)
член-корреспонденту РАН,
д.т.н., профессору
Р.М. ЮСУПОВУ

В.О., 14-я линия, д. 39,
Санкт-Петербург, 199178
Тел.: (812) 232-97-04
Факс: (812) 232-23-07

АКТ

об использовании результатов диссертационной работы на соискание ученой степени доктора технических наук Лившица Ильи Иосифовича (Специальность: 05.13.19 – «Методы и системы защиты информации, информационная безопасность»)

Научно-техническая комиссия ООО «Газинформсервис» в составе: председателя: генерального директора, с.н.с., к.ф.-м.н. Пустарнакова В.Ф., членов комиссии: советника генерального директора к.т.н. Кирюшкина С.А., начальника группы службы технического директора к.т.н. Юркина Д.В. и главного специалиста группы анализа и управления качеством доцента, к.в.н. Колпакова А.М., составила настоящий акт в том, что при проведении аудитов информационной безопасности, оценки защищенности сложных информационных объектов в соответствии с требованиями ГОСТ Р ИСО/МЭК серии 27001 использованы следующие результаты, полученные в диссертационной работе Лившица И.И.:

- модель проведения аудитов интегрированных систем менеджмента для сложных промышленных объектов;
- метод многошаговой оптимизации процесса аудитов интегрированных систем менеджмента для сложных промышленных объектов;
- система численных показателей (метрик) информационной безопасности, применение которых расширяет существующие методы выполнения аудитов систем менеджмента и позволяют получать численные уровня обеспечения информационной безопасности для сложных промышленных объектов.

Указанные результаты опубликованы Лившицем И.И в работах: «Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации – ИСО 27001 и СТО Газпром» (Труды СПИИРАН, 2015 г., вып. 3), «Определение бюджета для реализации проекта системы менеджмента информационной безопасности на основании оценки последствий инцидентов» (Вестник Иркутского ГТУ, 2015 г., вып. 6) и «Effectiveness assessment of IT-security management system processes» (Proceeding DCCN-2015).

Предложенные Лившицем И.И. модель проведения аудитов интегрированных систем менеджмента и метод многошаговой оптимизации процесса аудитов интегрированных систем менеджмента для сложных промышленных объектов нашли свое применение при реализации ряда проектов 2014 – 2016 гг. по совершенствованию системы обеспечения информационной безопасности для предприятий группы компаний «Газпром» и «Газпром нефть».

Использование результатов диссертационного исследования Лившица И.И. позволило снизить сроки выполнения аудитов системы обеспечения информационной безопасности, а также повысить качество успешной сертификации системы менеджмента информационной безопасности ООО «Газпром трансгаз Москва» на соответствие требованиям стандарта ГОСТ Р ИСО/МЭК серии 27001 с опережением на 4 месяца.

УТВЕРЖДАЮ:

Председатель комиссии:

Генеральный директор _____ В.Ф. Пустарнаков, с.н.с., к.ф.-м.н.

Члены комиссии:

Советник Генерального директора _____ / С.А. Кирюшкин, к.т.н.

Начальник группы службы
технического директора _____ / Д.В. Юркин, к.т.н.

Главный специалист группы анализа
и управления качеством _____ / А.М. Колпаков, к.в.н., доцент

Приложение А.7 Акт о внедрении ГУП «Водоканал Санкт-Петербурга»

ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА
Государственное унитарное предприятие
«ВОДОКАНАЛ САНКТ-ПЕТЕРБУРГА»
(ГУП «Водоканал Санкт-Петербурга»)
Кавалергардская ул., д.42, Санкт-Петербург, 191015
Телефон (812) 305-09-09, факс (812) 274-13-61
E-mail: office@vodokanal.spb.ru
http: //www.vodokanal.spb.ru
ОКПО 03323809 ОГРН 1027809256254
ИНН/КПП 7830000426/783450001

«УТВЕРЖДАЮ»
Директор по персоналу
ГУП «Водоканал Санкт-Петербурга»
_____ / П.Б. Михайлов
«__» _____ 2016 г.

_____ № _____

На № _____ от _____

АКТ

об использовании результатов диссертационной работы на соискание ученой степени доктора технических наук Лившица Ильи Иосифовича (Специальность: 05.13.19 – «Методы и системы защиты информации, информационная безопасность»)

ГУП «Водоканал Санкт-Петербурга» подтверждает, что результаты диссертационной работы на соискание ученой степени доктора технических наук Лившица И.И. внедрены и используются в процессах обучения по программам выполнения аудитов систем менеджмента информационной безопасности (СМИБ), оценки и самооценки интегрированных систем менеджмента (ИСМ) в соответствии с требованиями стандартов ISO/IEC.

Следующие научные результаты (методика исследования динамки сертификации по международным стандартам ISO для СлПО, метод многошаговой оптимизации процесса аудитов ИСМ), полученные лично Лившицем И.И и опубликованные в работах: «Формирование требований к защищенности сложных промышленных объектов» (Стандарты и качество. 2016. № 2. С. 46-47), «Оценка методических подходов для формирования систем безопасности сложных промышленных объектов» (Вопросы защиты информации. 2016. № 1 (112). С. 56-61) и «Учет активов при сертификации систем менеджмента информационной безопасности» (Методы менеджмента качества. 2015. № 5. С. 34-39) и применяются в ГУП «Водоканал Санкт-Петербурга» в процессах обучения аудиторов / ведущих аудиторов СМИБ и ИСМ в период 2014 – 2016 гг.

Предложенный Лившицем И.И. метод многошаговой оптимизации процесса аудитов ИСМ нашел свое применение в процессах обучения аудиторов / ведущих аудиторов ГУП «Водоканал Санкт-Петербурга» на соответствие требованиям ISO/IEC 27001:2013. Использование результатов диссертационного исследования Лившица И.И. позволило значительно повысить результативность процессов обучения аудиторов / ведущих аудиторов СМИБ в ГУП «Водоканал Санкт-Петербурга» по данным итоговой аттестации слушателей.

Председатель комиссии:
Руководитель по качеству менеджмента _____ / Киримитчиев А.П.

Члены комиссии:
Директор Департамента
информационных технологий _____ / Чемоданов Е.Н.

Главный специалист по защите информации
Департамента информационных технологий _____ / Старченко С.В.