ОТЗЫВ

официального оппонента

на диссертационную работу Лившица Ильи Иосифовича «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами», представленную на соискание учёной степени доктора технических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность»

1. Актуальность темы диссертационной работы

В связи с развитием информационного общества и современных технологий обработки информации резко увеличивается значимость ее потери. Значительное увеличение объема потребляемой и производимой информации предприятиями интегрированных структур в условиях возможных чрезвычайных ситуаций при решении операционных задач, а также рост влияния этой информации на позицию предприятия и повышением динамичности экономических процессов, диктует потребность в разработке и внедрении новых, более эффективных методик и применении лучших мировых практик управления ИТ-службой компании. Особенно это актуально для объектов информатизации являющихся, основными центрами по обработки информации для критически важных объектов. В этом случае последствия от несанкционированного доступа могут привести к техногенным катастрофам и человеческим жертвам.

Актуальность темы диссертационной работы Лившица И.И. обоснована тем, что в настоящее время увеличивается количество атак злоумышленников, направленных не столько на данные, сколько на элементы систем управления (СУ) и технологические процессы различных критичных объектов. Соответственно, значительно увеличилась актуальность изучения общей проблемы создания интегрированных

систем менеджмента (ИСМ) как компонентов СУ для обеспечения безопасности объектов, именуемых сложными промышленными объектами (СлПО).

2. Научная новизна результатов работы

Научная новизна полученных в диссертационной работе Лившица И.И. результатов, выводов и рекомендаций заключается в том, что в ней впервые в целостном функциональном представлении сформулирован научно-методический аппарат для обеспечения аудита информационной безопасности для СлПО, основанный на современном комплексном риск-ориентированном подходе, специальных моделях и методах выполнения аудита.

Новые разработанные обобщенная модель ИСМ для обеспечения безопасности, базовая модель аудита и система численных показателей (метрик) информационной безопасности для выполнения аудита отличаются от известных расширением набора критериев при оценке уровня.

Метод проведения аудита ИСМ для СлПО отличается от известных подходов тем, что введены действия оценки роста уровня обеспечения информационной безопасности в СлПО.

Метод исследования динамики сертификации по международным стандартам ISO для СлПО усовершенствован процессом определения коэффициентов зависимости (корреляции).

Метод многошаговой оптимизации процесса аудита информационной безопасности СлПО, который, в отличие от известных стандартов ISO, обеспечивает координацию, распределение ресурсов и оперативное информирование аудитора по оценке результативности аудита.

Результатом исследования нескольких смежных научных областей (теории управления, теории множеств и теории принятия решений), явилось развитие понятийного аппарата теории обеспечения

информационной безопасности для СлПО, а также разработка новых моделей и методов аудита, позволяющих формировать оптимальный перечень метрик и выполнять количественную оценку уровня обеспечения информационной безопасности.

3. Достоверность и степень обоснованности научных положений, выводов и рекомендаций

Достоверность и обоснованность научных положений, выводов и рекомендаций 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», ФСТЭК России, Positive Technology) и международных обзоров сертификации;
- 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 том числе, индексируемых Scopus и/или Web of Science.

4. Теоретическая и практическая значимость

Теоретическая значимость результатов исследований, изложенных в работе Лившица И.И., состоит в обосновании возможности применения новых моделей и 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 ИБ в ИСМ (как компоненты интегрированной СУ) для СлПО.

Практическая значимость работы определяется тем, что результаты диссертационного исследования использовались в следующих предметных областях:

1. Информационные технологии (в компании ИТСК);
2. Воздушный транспорт (в международных аэропортах Алматы и Астаны);
3. Системная интеграция (в группе компаний «Газинформсервис»);
4. Образование (в международной компании AQS, Азербайджан);
5. Банковское дело (в Акционерном коммерческом банке «Рускобанк»);
6. Управление коммунальными объектами (в ГУП «Водоканал Санкт-Петербурга»).

О теоретической и практической значимости также свидетельствуют различные акты об использовании результатов диссертационной работы и получении значимых преимуществ.

5. Полнота опубликованных результатов и соответствие паспорту специальности

Основные научные положения диссертации, впервые содержащие защищаемые научные положения, нашли отражения в 38 статьях,

опубликованных в научных журналах, рекомендованных ВАК 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.

Основные результаты диссертационной работы Лившица И.И. обсуждались на многочисленных российских и международных научно-технических семинарах и конференциях.

Полученные результаты соответствуют паспорту специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность» 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).

6. Замечания по диссертации и автореферату

При изучении представленной работы Лившица И.И. возникли следующие вопросы и замечания:

1. В тексте диссертации встречается оборот «обобщенная модель ИСМ для обеспечения безопасности ИСМ» (стр. 20, 22 и 359), что несколько противоречит логике формулировки и вывода 1-го защищаемого научного положения. Следует заметить, что далее по тексту приведена уже только корректная формулировка: «обобщенная модель ИСМ для обеспечения безопасности СлПО».

2. Глава 2 в диссертационной работе, как представляется, немного перегружена, некоторые разделы и подразделы, вероятно, излишни. Следовало бы приводить в тексте более «концентрированные» научные результаты, что, возможно, улучшило бы общую ясность и повысило бы компактность диссертации.
3. Следует отметить, что недостаточно подробно раскрыто новое понятие, введенное в Главе 2 «сложный промышленный объект» (СлПО), и не в полной мере определена взаимосвязь нового понятия и первого защищаемого научного положения: «обобщенная модель ИСМ для обеспечения безопасности СлПО, базовая модель аудита ИСМ и система численных показателей (метрик) ИБ для выполнения аудита ИСМ».
4. В Главе 3 для определения направлений движения к перспективным методам выполнения аудита (оценки) уровня обеспечения информационной безопасности предложено получать точное представление о текущей ситуации без применения прогнозирования, которое является одним из наиболее важных моментов в принятии управленческих и организационных решений.
5. В Главе 3 приведено достаточно краткое описание предложенной модели оптимизации метрик для аудитов информационной безопасности, не позволяющее в должной мере оценить его оригинальность и значимость для процесса обеспечения безопасного функционирования объектов критичной инфраструктуры.
6. В Главе 6 диссертации не представлен детальный и подробный анализ результативности и параметров быстродействия по модифицированной формуле Apdex в ходе проводимого экспериментального исследования.

7. Процесс оценки уровня обеспечения безопасности для СлПО – аэропортовых комплексов в Главе 6 диссертации формируется по модели аудита информационной безопасности для ИСМ в аэропортовых комплексах как оценка результативности по множеству критериев известного метода анализа иерархий (Т.Саати), оцениваемых в процессе аудита всех типов без учета связи с процессами корректирующих и предупреждающих действий.

Указанные выше незначительные замечания не влияют на общую положительную оценку представленной диссертации Лившица И.И.

Заключение

Диссертация Лившица И.И. представляет собой целостную и законченную научно-квалификационную работу, в которой на основании выполненных автором исследований разработаны теоретические положения, имеющие важное хозяйственное значение.

В диссертационной работе Лившица И.И. решена важная научно-техническая проблема, заключающаяся в создании теоретических основ формирования перспективных подходов и применения новых методов обеспечения информационной безопасности в интегрированных системах управления для сложных промышленных объектов и применения наилучшего в методах оптимизации аудитов множества мер (средств) обеспечения информационной безопасности для парирования выявленных рисков.

Заключение анти-плагиата доступно и позволяет оценить, что работа выполнена автором самостоятельно на высоком уровне. Содержание и выводы автореферата соответствуют основным положениям диссертационной работы и позволяют оценить теоретическую и практическую значимость исследования.

Диссертация и автореферат полностью удовлетворяют требованиям п.п. 9-14 «Положения о присуждении учёных степеней», утверждённого Постановлением Правительства РФ от 24.09.2013 № 842, предъявляемым к докторским диссертациям, а её автор, Лившиц Илья Иосифович, заслуживает присуждения учёной степени доктора технических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент Липатников Валерий Алексеевич

Старший научный сотрудник
Военная академия связи им. Маршала Советского Союза С. М. Буденного
доктор технических наук, профессор

Адрес: 194064, г. Санкт-Петербург, К-64, Тихорецкий проспект, д.3
Телефон: +8 (921) 912-70-81
E-mail: lipatnikovanl@mail.ru
http://vas.mil.ru