ОТЗЫВ

официального оппонента на диссертацию
Лившица Ильи Иосифовича
«Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами»,
представленную на соискание ученой степени доктора технических наук по специальности 05.13.19 — Методы и системы защиты информации, информационная безопасность

Актуальность избранной темы

Увеличение атак злоумышленников на элементы систем управления (СУ) и технологические процессы сложных промышленных объектов (СлПО) привели к объективной потребности изучения проблемы создания интегрированных систем менеджмента (ИСМ) как компонентов СУ для обеспечения информационной безопасности (ИБ) и разрешения противоречий между текущим состоянием теории и требованиями практики обеспечения ИБ для СлПО. Следует отметить, что современный уровень развития информационных технологий (ИТ) обеспечивает значительно больший охват производственных процессов, и, в том числе, реализацию процедур аудита ИБ в СлПО. Все сказанное выше обуславливает актуальность диссертационного исследования Лившица Ильи Иосифовича.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Глубокое изучение и анализ отечественной (263 источников) и зарубежной (132 зарубежных источника) литературы позволили автору диссертации получить объективное представление о состоянии изучаемой проблемы, определить цель, ряд задач научного характера и необходимые методы исследования. Обоснованность основных положений диссертации Лившица И.И., выводов и практических рекомендаций обеспечиваются современным уровнем и непротиворечивостью исходных теоретических положений, адекватной задачам

работы, логикой плана исследования, применением надежных и апробированных методов, соответствующих поставленным цели и задачам.

Достоверность и новизна исследования, полученных результатов, выводов и рекомендаций, сформулированных в диссертации

Достоверность результатов диссертационного исследования Лившица И.И. обеспечивается корректной интерпретацией и количественным анализом полученных результатов. 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, моделях и методах выполнения аудита ИБ.

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 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.

Значимость для науки и практики полученных автором результатов

Предложенные в диссертации Лившица И.И. методы и модели представляют собой новые научные результаты, имеющие большое значение для теории и практики обеспечения безопасности сложных промышленных объектов, например, новые модели и методы выполнения аудитов ИБ для СлПО, новые подходы для количественного оценивания уровня соответствия современным риск-ориентированным стандартам. Эти результаты могут рассматриваться как решение поставленных в исследовании научных задач, практическая значимость которых выражается в улучшении методов эффективного противодействия деструктивным действиям злоумышленников, достижении требуемого уровня ИБ, минимизацию

потерь при возникновении ситуаций риска ИБ, присущих СлПО, а также повышение степени соответствия законодательным требованиям. Цель исследования можно считать достигнутой.

Рекомендации по использованию результатов и выводов диссертации

Результаты диссертации целесообразно использовать для обеспечения безопасности объектов критической инфраструктуры РФ с учетом новых законодательных инициатив (например, ФЗ-187), а также в качестве методического сопровождения в ИСМ процессов автоматизации формирования численных показателей (метрик) ИБ для выполнения аудита, сокращения длительности процессов планирования, выполнения и анализа результатов аудита ИБ в СлПО.

Оценка содержания диссертации и ее завершенности

Диссертационная работа Лившица И.И. изложена на 407 страницах, состоит из введения, 6 глав, заключения, перечня сокращений, перечня терминов и определений, список литературы (395 наименований на 29 страницах) и приложения, в котором представлены 7 актов, подтверждающих реализацию результатов.

Во введении обоснована актуальность темы диссертации, проведен анализ исследуемой научной проблемы и обоснован подход к ее решению, сформулированы цель и задачи диссертационного исследования, определена научная новизна и практическая значимость результатов, сформулированы основные научные положения, выносимые на защиту. Всего на защиту выносятся 4 научных положения:

- Первое научное положение – обобщенная модель ИСМ для обеспечения безопасности СлПО, базовая модель аудита ИСМ и система численных показателей (метрик) ИБ для выполнения аудита ИСМ.
- Второе научное положение – метод проведения аудита ИСМ для СлПО.
- Третье научное положение – метод исследования динамики сертификации по международным стандартам ISO для СлПО.

– Четвертое научное положение – метод многошаговой оптимизации процесса аудита ИБ в ИСМ для СлПО.

Первая глава диссертации посвящена исследованию направлений развития теоретических и методологических аспектов теории ИБ и постановке задач, направленных на разрешение выявленных противоречий между состоянием теории и требованиями практики при планировании и проведении аудита ИБ в СлПО. Эта глава содержит материалы исследований, относящиеся к первому защищаемому положению.

Вторая глава посвящена вопросам уточнения множества ограничений (в том числе законодательных) для базовой модели аудита ИБ для СлПО, выполняемого ИСМ. Исследование показало, что одной из важнейших задач является точное определение объекта аудита – СлПО. Выявлено, что в настоящее время на законодательном уровне РФ не в полной мере определены механизмы взаимодействия и ответственность субъектов, прямо или косвенно участвующих в обеспечении безопасности КИИ: органов государственной власти, служб безопасности, разработчиков решений в области ИБ.

В третьей главе представлены материалы исследований, относящиеся к второму защищаемому положению. Проблема выполнения измерений (как процесс оценки) для больших и/или сложных систем рассматривалась в классических трудах Н. Винера, Р. Кини, Х. Райфа, И. Пригожина.

В четвертой главе представлены материалы исследований, относящиеся к третьему защищаемому положению. Представляет интерес создание нового метода для получения достоверных статистических данных о динамике применения международных стандартов ISO за длительный интервал наблюдений, что позволит ЛПР принимать рациональные решения еще в начале ЖЦ интегрированной СУ для СлПО.

В пятой главе представлены материалы исследований вопросов оптимизации системы внутреннего аудита, относящиеся к четвертому защищаемому положению. В диссертации подробно рассмотрены существующие «классические»

стандарты системы аудита (в частности ISO, ISAGO, СТО БР ИББС, СТО Газпром СОИБ).

Представленные выше теоретические и научно-практические положения нуждаются в оценке практического применения с целью подтверждения корректности предположений и возможности практического использования моделей и методов аудита ИСМ как компоненты интегрированной СУ для СлПО и последующего анализа результатов апробации. Этому посвящена 6 глава.

В заключении приведены основные результаты, полученные в выполненном диссертационном исследовании. Диссертационная работа Лившица И.И. в целом имеет завершенный характер. Качество оформления соответствует предъявляемым требованиям. Представленный автореферат соответствует содержанию диссертации.

Достоинства и недостатки в содержании и оформлении диссертации, мнение о научной работе соискателя в целом

К достоинствам работы Лившица И.И. следует отнести всестороннее энциклопедическое изучение существующих работ в области теории и практики защиты информации, глубокий основательный анализ существующих методологических подходов и критичных аспектов рассматриваемых вопросов.

К недостаткам представленной работы можно отнести следующие:

1) При исследовании предметной области оценки рисков информационной безопасности в нотации надежности технических систем, представленной на рис. 1.13 (стр. 79) диссертации, очевидно, необходимо было опираться на существующие методики применимых национальных ГОСТ Р ИСО/МЭК серии 27001, ГОСТ Р ИСО/МЭК серии 15408. Это позволит оценивать не абстрактную (теоретическую), а действительно практическую применимость предложенных новых методов. Кроме того, необходимо отметить, что стандарты ISO серии 27005 и 31000 прошли актуализацию в 2018 г. и этот факт определенным образом было бы желательно отразить в диссертации.

2) 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 СлПО. Кроме того, необходимо отметить, что не отражена в полной мере роль Банка данных угроз ФСТЭК России.
3) Отсутствие в автореферате конкретных примеров реализации предложенной модели оптимизации метрик для аудитов информационной безопасности (кроме рисунка 3 на стр. 15) не позволяет в полной мере оценить практическую значимость для обеспечения безопасного функционирования СлПО.
4) В автореферате отсутствуют сведения о комплексных стоимостных показателях, используемых для оценки ущерба активам СлПО при выполнении аудитов ИБ предложенной методикой «мгновенных» аудитов ИБ. Вообще, термин «мгновенный аудит» следовало бы разъяснить более подробно: это не фиксированный аудит, как следует из текста диссертации, но нужно пояснить предел частотности его проведения для конкретных ситуаций.
5) В тексте диссертации несколько раз встречается неудачный оборот «*обобщенная модель ИСМ для обеспечения безопасности ИСМ*» (стр. 20, 22 и 359), что может вызвать сложности при анализе 1-го защищаемого научного положения. Очевидно, должна быть представлена иная корректная формулировка: «*обобщенная модель ИСМ для обеспечения безопасности СлПО*», в автореферате представлена именно такая формулировка.
6) Можно отметить неудобство чтения текста диссертации, когда на одном листе присутствуют 6 и более сносок, а на страницах 51 и 101 таких сносок даже 8. При необходимости цитирования множества источников и предоставления доказательности научным положениям следовало бы перенести их в раздел литературы.
7) Можно отметить и ряд хотя и мелких, но затрудняющих знакомство с диссертацией недостатков, таких как многочисленное наличие нерасшифрованных сокращений в тексте диссертации (общее число

сокращений в списке – 90, а кроме этого использовано еще 53 сокращения, не внесённых в список), а также можно указать на отсутствие достаточных пояснений к некоторым рисункам (например, 1.12, 2.3, 2.15, 2.19), частое отсутствие знаков препинания при отображении математических соотношений, некорректности в отображении схемы алгоритма на рис 5.6, вызывает также сомнение корректность выражения 5.3 на стр. 314.

Указанные недостатки, хотя и незначительно снижают качество оформления, но не носят принципиального характера и не изменяют общего положительного мнения в целом о работе, выполненной соискателем диссертации.

Заключение о соответствии диссертации критериям, установленным Положением о порядке присуждения ученых степеней

Диссертация написана автором самостоятельно, обладает внутренним единством, содержит новые научные положения, выдвигаемые для публичной защиты, и свидетельствует о личном вкладе автора диссертации в науку.

Личный вклад автора в основных публикациях с соавторами оформлен корректно. Итоговая оценка оригинальности согласно опубликованному отчету анти-плагиата составляет 93,86%. Основные научные результаты диссертации опубликованы в рецензируемых изданиях, в том числе в 38 статьях, опубликованных в научных журналах, рекомендованных ВАК РФ и в 15 изданиях, индексируемых Scopus и/или Web of Science.

В диссертационной работе Лившица И.И. представлено успешное решение крупной научно-технической проблемы, заключающейся в создании и применении новых методов обеспечения информационной безопасности в интегрированных системах управления для сложных промышленных объектов, созданных для снижения длительности и стоимости аудита информационной безопасности, формирования количественной оценки уровня обеспечения информационной безопасности и парирования рисков в сложных промышленных объектах.

Таким образом, диссертация Лившица Ильи Иосифовича является завершенной научно-квалификационной работой, в которой изложены новые, научно обоснованные методические решения, внедрение которых вносит значительный вклад в обеспечение ИБ СлПО. Представленная диссертация Лившица И.И. соответствует требованиям п. 9 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, а ее автор заслуживает присуждения ученой степени доктора технических наук.

Официальный оппонент Кустов Владимир Николаевич
доктор технических наук, пр

Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I»

Профессор кафедры «Информатика и информационная безопасность»

Адрес: Россия, 190031, Санкт-Петербург, Московский пр., д. 9

Телефон: +7 (812) 310-34-72
E-mail: inib@pgups.ru
https://w