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

1. Актуальность темы диссертационной работы

Современный уровень развития информационных технологий (ИТ) позволил обеспечить больший охват и оперативность управления производственных процессов, поддержку лиц, принимающих управленческие решения (ЛПР), а также реализацию процедур аудита сложных промышленных объектов (СлПО). Применение ИТ призвано снизить сложность управления критичными производственными процессами в режиме, близком к режиму реального времени, но, вместе с тем, привнесло характерные риски в обеспечение безопасности СлПО. Соответственно, повысилась важность исследования проблемы обеспечения информационной безопасности (ИБ) для СлПО различной отраслевой принадлежности, и в этой связи тема диссертационной работы Лившиц И.И., несомненно, актуальна.

2. Научная новизна результатов работы

Научная новизна полученных в диссертационной работе Лившица И.И. результатов, выводов и рекомендаций заключается в следующем:

1) 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.

2) 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.

3) Новизна комплекса моделей и методов заключается в формировании функционально завершенной структуры для выполнения аудита ИБ в ИСМ.

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

Достоверность и обоснованность научных положений, выводов и рекомендаций, полученных в диссертационной работе Лившица И.И., подтверждается:

- 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, Касперский) и международных аналитических обзоров ISO;
- доказанным положительным эффектом от ряда внедрений результатов представленного диссертационного исследования;
- 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).

Достоверность также подтверждается апробацией защищаемых научных положений диссертационной работы на значимых международных и общероссийских научных и научно-технических конференциях, большим количеством публикаций в рецензируемых научных изданиях.

4. Теоретическая и практическая значимость

Теоретическая значимость диссертационного исследования 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 полученных результатов в исследовании Лившица И.И. состоит в улучшении методов оценки (аудита) ИБ для СлПО, основанных на применении оптимального множества риск-ориентированных стандартов в составе ИСМ, что обеспечивает эффективное противодействие деструктивным действиям злоумышленников, достижение требуемого уровня ИБ, минимизацию потерь при возникновении ситуаций риска ИБ, присущих СлПО, а также повышение степени соответствия законодательным требованиям. Представленные методы и модели аудита ИБ для СлПО реализованы как функционально завершенный элемент в системе мероприятий комплекса обеспечения ИБ.

Результаты работы Лившица И.И. позволяют судить о значительной экономической выгоде при внедрении нового методического сопровождения процессов автоматизации формирования численных показателей (метрик) ИБ, для сокращения длительности процессов планирования, выполнения и анализа результатов аудита ИБ в ИСМ для СлПО.

5. Полнота опубликованных результатов и соответствие паспорту специальности

Основные научные положения диссертационной работы Лившица И.И. впервые содержащие защищаемые научные положения, опубликованы в 38 статьях в научных журналах, рекомендованных ВАК РФ, в 15 изданиях, индексируемых Scopus и/или Web of Science, а также в 12 публикациях в иных рецензируемых научных специализированных изданиях. Также можно отметить, что по данным диссертации (стр. 27 – 29) основные результаты выполненных исследований обсуждены на многих известных международных и общероссийских конференциях и семинарах, посвященных вопросам обеспечения информационной безопасности.

Достигнутые результаты работы 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

1. На рисунке 1.13 (стр. 79, Глава 1) в диссертации присутствует упоминание стандарта риск-менеджмента ISO/IEC 27005, при этом в автореферате отсутствует в явном виде принятая в нем структура оценки рисков информационной безопасности. Представляется разумным, поскольку в тексте диссертации на рисунке 2.4 (стр. 106, Глава 2) упоминается и стандарт ISO 31000, пояснить дополнительно, какой из них обладает большими преимуществами и на основании каких критериев для выбранной темы исследования.

2. На рисунке 1.13 (стр. 79, Глава 1) в диссертации приведена базовая модель аудитов ИБ, в которой не указаны широко используемые в РФ ГОСТ Р ИСО семейства 15408, а также не отражено взаимодействие с Банком данных угроз безопасности информации ФСТЭК России. Это взаимодействие могло бы повысить универсальность предложенных автором моделей.

3. В тексте диссертации при избыточно подробном анализе существующих подходов зачастую весьма лаконично приведено математическое обоснование предлагаемых решений при обосновании моделей и методов (стр. 174, 180), что иногда затрудняет оценку их адекватности.

4. При описании метода «мгновенных аудитов» желательно более аргументированно определить условия и факторы, влияющие на частоту (период) проведения аудитов.

5. В тексте диссертации встречаются аббревиатуры, не вошедшие в список сокращений. Кроме того, в тексте диссертации зачастую не приводится физическая интерпретация полученных результатов и выводов.

6. Автор не приводит в диссертации информацию о программном обеспечении, примененном для практической оценки разработанных методик и моделей (например, рис. 5.4 и 5.5 в Главе 5), кроме краткого описания созданной среды имитационного моделирования в Главе 6.

Указанные замечания носят дискуссионный характер и не снижают положительной оценки диссертации в целом.

ЗАКЛЮЧЕНИЕ

В соответствии с п. 9 и п. 10 «Положения о присуждении ученых степеней», диссертационная работа Лившица И.И., выполненная на тему «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами», является законченной научно-квалификационной работой, в которой изложены новые научно обоснованные решения, внедрение которых вносит значительный вклад в обеспечение безопасности страны.

Представленная работа Лившица И.И. характеризуется новизной и значимостью результатов, которые можно признать достоверными и обоснованными. Автореферат и печатные работы Лившица И.И. полностью отражают основное содержание диссертационной работы, что соответствует п. 11 и п. 13 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24 сентября 2013 г. № 842.

В диссертационной работе Лившица И.И. решена значимая научно-техническая проблема, заключающаяся в создании как теоретических основ формирования новых перспективных подходов обеспечения информационной безопасности в интегрированных системах управления для сложных промышленных объектов, так и разработки практических методов снижения длительности и стоимости аудита информационной безопасности, формирования количественной оценки уровня обеспечения информационной безопасности,

выбора наилучшего множества мер (средств) обеспечения информационной безопасности для сложных промышленных объектов.

Заключение по результатам теста на плагиат и итоговая оценка оригинальности: 93,9%, позволяют сделать заключение, что диссертационная работа Лившица И.И. выполнена автором самостоятельно на высоком уровне. Содержание и выводы автореферата соответствуют основным положениям диссертационной работы и позволяют оценить теоретическую и практическую значимость исследования.

Считаю, что диссертационная работа Лившица Ильи Иосифовича по содержанию, научному уровню и завершенности исследования соответствует критериям п. 9 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24 сентября 2013 г. № 842, а ее автор, Лившиц Илья Иосифович, заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Официальный оппонент,
декан факультета информационных систем и технологий,
доктор технических наук, профессор

Зикратов Игорь Алексеевич

Организация: Федеральное государственное бюджетное о
«Санкт-Петербургский государственный университет тел
Бруевича» (СПбГУТ)
Юридический адрес: набережная реки Мойки, д. 61, Санкт-Петербург, 191186
Почтовый адрес: пр. Большевиков, д. 22, корп. 1, Санкт-Петербург, 193232
Тел.: (812) 3263156, факс (812) 3263159, e-mail: rector@sut.ru, web-сайт: www.sut.ru