ОТЗЫВ

на автореферат диссертации

Лившица Ильи Иосифовича

на тему «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами»

представленной на соискание ученой степени доктора технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»

Актуальность темы представленной диссертации не вызывает сомнений, поскольку в настоящее время увеличивается количество атак злоумышленников, направленных на технологические процессы и элементы систем управления критичных объектов. Соответственно, значительно увеличилась актуальность общей проблемы создания интегрированных систем менеджмента как элемента системы управления для обеспечения безопасности объектов, именуемых в диссертации сложными промышленными объектами.

Представленная работа представляет собой частное решение общего известного противоречия между требованиями практики и существующими положениями теории обеспечения информационной безопасности. Научная проблема представленной диссертационной работы формулируется как проблема разрешения противоречий между состоянием теории информационной безопасности (в частности, неполноты определения требований к аудиту) и современными требованиями практики по обеспечению информационной безопасности для сложных промышленных объектов. Для решения данной проблемы автор предлагает выполнить пересмотр существующих статичных моделей угроз безопасности информации и деструктивных действий, всеобъемлющую интеграцию риск-менеджмента, учет требований, предъявляемых к планированию, выполнению и совершенствованию системы аудита информационной безопасности и принятие решения при фиксированном множестве альтернатив.

Цель диссертационного исследования Лившица И.И. определена как снижение длительности и стоимости аудита информационной безопасности за счет использования новых моделей и методов аудита интегрированных систем менеджмента, реализующих оперативное формирование количественной оценки уровня обеспечения информационной безопасности в сложных промышленных объектах, выбор и применение наилучшего множества средств (мер) обеспечения информационной безопасности для обработки выявленных рисков. Достижение поставленной цели потребовало решения ряда задач, которые, как следует из автореферата, были успешно решены.

Теоретическая значимость диссертационного исследования Лившица И.И. состоит в обосновании возможности применения новых моделей и

методов обеспечения информационной безопасности на основании независимой оценки (аудита) информационной безопасности в сложных промышленных объектах, созданных в соответствии с требованиями современных риск-ориентированных стандартов; определении новых критериев выбора множества требований, оптимальных для конкретного объекта; определении новых условий формирования оптимального множества критериев оценки (метрик) информационной безопасности и развитии научного аппарата независимой оценки информационной безопасности в интегрированной системе менеджмента (как компоненты интегрированной системы управления) для сложного промышленного объекта.

Достоверность результатов, полученных в диссертационной работе Лившица И.И., подтверждается их 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, Cisco, SAP); сопоставление с публичными данными национальных («Эшелон», ФСТЭК, 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).

Основные результаты и положения работы Лившица И.И. докладывались на ведущих международных и всероссийских научных и научно-технических конференциях, в том числе ежегодных: DCCN, FRUCT, «Комплексная защита информации», «ИБ АСУТП КВО», IT&MQ&IS и пр. Основные результаты диссертационного исследования, впервые содержащие защищаемые научные положения, нашли отражения в 38 статьях, опубликованных в научных журналах, рекомендованных ВАК Российской Федерации, 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.

В целом диссертация Лившица И.И. является завершенным научным трудом, выполненным лично автором и создающим положительное впечатление. Содержание автореферата соответствует существу научных задач, решаемых в диссертационной работе.

Замечания по работе:

1. В автореферате довольно кратко представлено описание модели оптимизации метрик для аудитов информационной безопасности и не приводятся примеры конкретных сценариев (методов) применения разработанных новых моделей.

2. В автореферате отсутствуют сведения о комплексных стоимостных показателях, используемых для оценки ущерба активам сложных промышленных объектов при выполнении аудита информационной безопасности с помощью предложенной методикой «мгновенных» аудитов информационной безопасности.

3. В автореферате отсутствуют ссылки и анализ аналогичных или близких работ по той же тематике, выполненных в мире, например, в области противодействия целевым атакам.

Указанные замечания касаются частных сторон представленной диссертационной работы Лившица И.И. и не ставят под сомнение ее значимые основные научные результаты.

Выводы:

1. Представленная диссертационная работа Лившица Ильи Иосифовича имеет важное теоретическое и прикладное значение, в полной мере удовлетворяет требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени доктора технических наук.

2. Автор работы, Лившиц Илья Иосифович, заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Начальник цикла
технических и специальных дисциплин
учебного отдела
УО «Центр повышения квалификации
руководящих работников и спе
Департамента охраны
МВД Республики Беларусь
кандидат технических наук, до
подполковник милиции ликов
17.09.2018

Почтовый адрес:
223030, Республика Беларусь, Минский район, Горанский с/с, р-н д. Горани
телефон/факс: + 375 17 5026399,
адрес электронной почты: centr@ohrana.by