ИНТЕЛТЕХ INTELTECH

Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»)

Экз. № 1

УТВЕРЖДАЮ

Первый заместитель генерального директора

ной работе,

доцент

И.А. Кулешов

2018 г.

ОТЗЫВ

на автореферат диссертации Лившица Ильи Иосифовича на тему «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»

Анализ предметной области проведенного диссертационного исследования Лившица И.И. свидетельствует, что наряду с имеющимися существенными достижениями в области обеспечения информационной безопасности (ИБ) в соответствии с требованиями международных и государственных стандартов и отраслевых требований, в настоящее время недостаточно разработаны методические подходы к обеспечению ИБ для сложных промышленных объектов (СлПО). Для современных же подходов по созданию, внедрению, документированию и сопровождению интегрированных систем менеджмента (ИСМ) существенным недостатком является практическое отсутствие достоверного методического аппарата, контроля адекватности

процесса оценивания (аудита ИБ) и получения достоверных оценок уровня ИБ в СлПО для лиц принимающих решение (ЛПР) в режимах, близким к реальному времени (РРВ). До настоящего времени не предложен метод оценки векторов возможных решений при условии значительного различия их значимости (ценности) и возможных замещений – применительно к задачам обеспечения ИБ для СлПО. Почти отсутствуют работы, предлагающие гибкий и простой математический аппарат для формирования оптимального множества метрик ИБ, чувствительных к динамически изменяемым требованиям к ИСМ. В этих условиях представленное соискателем решение научной проблемы разрешения противоречий между состоянием теории ИБ и современными требованиями практики по обеспечению ИБ в СлПО является важным и актуальным.

Личный вклад автора в науку определяют следующие научные положения, выносимые на защиту:

первое научное положение – обобщенная модель ИСМ для обеспечения безопасности СлПО, базовая модель аудита ИСМ и система численных показателей ИБ для выполнения аудита ИСМ. Раскрыта специфика процесса планирования, выполнения и анализа результатов аудита ИБ в СлПО, заключающаяся в широком применении системы численных показателей ИБ для оценки результативности ИСМ как компоненты интегрированной системы управления согласно применимым требованиям. Предложенные новые модели дополняют существующие традиционные методы аудита и позволяют применять численные оценки показателей ИБ как оценки результативности ИСМ в статическом и динамическом 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, который в отличие от известных, позволяет учесть расширенный перечень критериев аудита и отличается применением численных показателей ИБ с учетом специфики обеспечения безопасности различных видов СлПО. Он реализует новый принцип управления аудитом ИБ по частоте и предоставляет ЛПР

оценку роста уровня обеспечения ИБ в СлПО как показатель результативности 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, учитывающий приоритеты отраслей в соответствии с международными кодами экономической деятельности, позволяющий оценить «входные» динамические изменения потребностей бизнеса, выраженные в изменении предпочтений ЛПР по составу внедряемых систем менеджмента, прошедших независимый аудит в составе ИСМ и формировать прогноз оценки;

четвертое научное положение – метод многошаговой оптимизации процесса аудита ИБ в ИСМ для СлПО, который, в отличие от известных стандартов ISO и ISO/IEC, обеспечивает координацию, распределение ресурсов и оперативное информирование ЛПР по оценке результативности аудита ИСМ. Предложенный метод обеспечивает научно обоснованное и целенаправленное функционирование ИСМ как компоненты интегрированной системы управления, и отличается от существующих циклическим непрерывным оцениванием ИБ на основе оптимальной системы численных показателей (метрик) ИБ.

Теоретическая значимость диссертационного исследования 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 системы управления) для СлПО.

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. Представленные методы и модели аудита ИБ для СлПО реализованы автором как функционально завершенный элемент в системе мероприятий комплекса обеспечения ИБ.

Вместе с тем, по автореферату имеются отдельные недостатки:

1) из базовой модели аудита ИСМ, представленной на рис. 2 автореферата, и ее описания не ясно, что подразумевает соискатель под множеством значений определенных и неопределенных факторов A, A′, A″ и A‴, сущность которых в описании модели не раскрыта;

2) в четвертом научном положении представляется не совсем корректным использование автором термина обеспечения ИБ на этапах «жизненного цикла сложного промышленного объекта» – (ЖЦ СлПО), поскольку, в большей степени, в работе идет речь о процессах обеспечения информационной безопасности в интегрированной системе менеджмента (как компоненты интегрированной системы управления) для СлПО, т.е. речь идет о жизненном цикле ИСМ (или интегрированной системы управления), но не о ЖЦ СлПО.

Однако, отмеченные недостатки не носят принципиального характера, очевидно связаны с ограниченным объемом автореферата, не ставят под сомнение основные научные результаты полученные автором самостоятельно и не снижают общей высокий теоретический и прикладной уровень работы.

Вывод: Судя по автореферату, в диссертационной работе Лившица Ильи Иосифовича *решена крупная научно-техническая проблема*, заключающаяся в создании теоретических основ формирования перспективных подходов и применения новых методов обеспечения ИБ в интегрированных системах управления для СлПО, созданных 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. По своей новизне, уровню научной проработки и практической значимости работа соответствует критериям раздела II «Положения о присуждении ученых степеней» (утвержденного постановлением Правительства Российской Федерации от 24.09.2013 г. № 842), предъявляемым к докторским диссертациям, 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»

Отзыв обсуждён и одобрен на заседании теоретической секции НТС ПАО «Интелтех». Протокол №19 от 11 октября 2018 г.

Отзыв подготовили:
ученый секретарь ПАО «Интел
доктор технических наук, проф Будко Павел Александрович

заместитель директора научно- нтра по научной работе
доктор военных наук, профессо ов Александр Александрович

Подписи ученого секрет телтех» доктора технических наук, профессора Будко Павла Александровича и заместителя директора научно-технического центра по научной работе доктора военных наук, профессора Густова Александра Александровича ЗАВЕРЯЮ.

Начальник отдела кадров ПАО «Инт ева Елена Оттовна
«11» октября 2018 г.