Эшелон
комплексная безопасность

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ЭШЕЛОН»

107023, г. Москва, ул. Электрозаводская, д. 24, стр. 1, тел./факс: +7 (495) 223 23 92, 645 38 11, mail@npo-echelon.ru, www.npo-echelon.ru

Исх. № 1207/1 от « 1 » октября 2018 г.

Утверждаю
Генеральный директор
АО «НПО «Эшелон»

лов

«

ОТЗЫВ

ведущей организации - Акционерного общества «Научно-производственное объединение «Эшелон»

на диссертационную работу 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

I. Актуальность проблематики и темы диссертационного исследования

Актуальность и востребованность работы объясняется практической потребностью разрешения проблемной ситуации, состоящей в противоречии между необходимостью обеспечения гарантированного уровня информационной безопасности (ИБ) ресурсов сложных промышленных объектов (СлПО) критических информационных инфраструктур и в недостаточном уровне развития

теоретических исследований и разработанности моделей и методов аудита ИБ интегрированных систем управления (менеджмента) СлПО.

Следует согласиться с автором, что высокая степень неопределенности тематики обусловлена динамичностью, разнородностью и зачастую рассинхронизацией нормативной базы (при одновременном наличии отраслевых, национальных, международных аутентичных и неэквивалентных стандартов, в отдельных случаях еще относящихся к «Оранжевой книге», 1983 г.), низким уровнем интеграции разнородных по целям (зачастую противоположным), по задачам, мерам, уровню востребованности систем менеджмента и уровню зрелости сегментов организации, а также весьма высокой долей субъективизма при построении и эксплуатации интегрированной системы менеджмента организации, особенно с учетом современных аспектов управления уровнем ИБ. Можно добавить, что современные системы менеджмента, основанные на процессорном подходе, в отличие от информационных и технических систем, главным образом зависят именно от человеческого фактора, в частности квалификации эксперта и «зрелости» топ-менеджмента организации. Соответственно оценка процессорного цикла таких систем происходит в условиях высокой степени неопределенности, нечеткости, разнородности, а некоторые показатели, по мнению многих специалистов, вообще не поддаются количественной оценке.

Тема диссертации, направленность проведенных исследований и полученных результатов соответствует Паспорту специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» по п. 15 (модели и методы управления информационной безопасностью), п. 14 (модели, методы и средства обеспечения внутреннего аудита…) и др.

II. Обоснованность научных положений, выводов и рекомендаций, сформулированных в диссертации, их достоверность и новизна

Судя по автореферату, в диссертационном исследовании автор, опираясь на проведенный анализ современных критических информационных инфраструктур отраслей промышленности, СлПО и защищенности их активов, НПА и международных и отраслевых стандартов в области ИБ и менеджмента,

интегральных систем менеджмента и их составных частей и моделей, таксономий и систематик ИБ (включая метрики СМИБ и реестры уязвимостей), механизмов и мер безопасности, а также современных систем и средств защиты информации, инструментальной базы контроля и мониторинга защищенности, современных методов и моделей управления рисками и оценки соответствия систем менеджмента, а также прикладных пакетов имитационного моделирования, демонстрирует системность и комплексность своего подхода к постановке и разрешению научной проблемы.

Наиболее существенные новые научные результаты, полученные в диссертации, состоят в предложении **нового научно-обоснованного** концептуального подхода, методов, полуформальных и математических моделей, а также методик решения поставленных в диссертации задач. К новым научным результатам, полученным в диссертационном исследовании, следует отнести следующие:

1. Комплекс полуформальных моделей (обобщенная модель интегрированной системы менеджмента для обеспечения ИБ СлПО, базовая модель аудита интегрированной системы менеджмента) и система формальных метрик (численных показателей) ИБ для выполнения аудита интегрированной системы менеджмента, которые позволяют формировать количественную оценку уровня ИБ организации.

2. Метод проведения «мгновенного» аудита ИБ в интегрированной системе менеджмента для СлПО, учитывающий меру адекватности и достаточности выполнения применимых требований ИБ к различным видам СлПО и позволяющий уточнять оценки уровня ИБ в процессе аудита.

3. Метод исследования динамики сертификации систем менеджмента для СлПО, позволяющий формировать прогнозные оценки рисков ИБ глобального характера.

4. Метод многошаговой оптимизации процесса аудита ИБ в интегрированной системе менеджмента для СлПО (по критериям осведомленности и ресурсоемкости), позволяющий кроме того получать в РВ оценки результативности системы менеджмента на различных этапах ЖЦ СлПО.

Достоверность основных выводов и результатов диссертационного исследования подтверждается следующим:

- в работе корректно использован аппарат теории множеств, теории вероятностей, теории оптимизации и методы системного анализа;

- научный замысел базируется на анализе потребностей практики проведения аудита и сертификации систем менеджмента;

- научные положения и теоретические выводы подтверждены их сопоставлением с практическими данными, полученными при внедрении в практику менеджмента предприятий отраслей промышленности;

- представлены проверяемые данные, факты и статистическая информация;

- в ряде случаев установлено совпадение полученных результатов с результатами тематических исследований систем менеджмента, полученных из независимых источников.

Достоверность и прикладная значимость научных результатов подтверждены актами о внедрении в работу российских организаций: ГУП «Водоканал Санкт-Петербурга», АО «Рускобанк», ООО «Газинформсервис» и «ИТСК», а также зарубежных - международных аэропортов Алматы и Астаны (Казахстан) и компании AQS (Азербайджан).

III. Теоретическая значимость и практическая ценность результатов исследований

Теоретическая значимость результатов состоит в развитии концептуальных основ аудита информационной безопасности оригинальной системой показателей и методами оценки, оптимизации и прогнозирования. Можно согласиться с автором, что основную теоретическую значимость работы составляет дополнение существующих подходов в области аудита ИБ авторским методом оценки (близкого к РВ) результативности системы менеджмента ИБ на основе модифицированного метода анализа иерархий (МАИ), дополненным решением ряда оптимизационных задач (Парето-оптимальных решений).

Практическая ценность исследования определяется тем, что результаты диссертационного исследования представлены в том числе в виде как функционально завершенного элемента (в терминах автора), а именно - предложений по построению и аудиту современных и перспективных систем менеджмента, а так и в использовании результатов исследования при проектировании и разработке интегрированных систем менеджмента (с учетом требований ИБ) ряда российских компаний и компаний ближнего зарубежья. Несомненный прикладной интерес имеют авторские имитационные модели систем менеджмента.

IV. Характеристика опубликованности результатов и положений, выносимых на защиту

Опубликованность научных результатов и положений диссертационной работы - согласно РИНЦ - подтверждается четырьмя десятками научных статей, опубликованных в рецензируемых научных изданиях ВАК (касающихся проблематики информационной безопасности), в том числе десятью статьями в рецензируемых журналах, включенных в систему цитирования Scopus/WoS, а также участием автора в 30-ти международных и всероссийских научных конференциях.

Ознакомление с научными трудами автора позволяет сделать однозначный вывод, что диссертация является **единолично** написанной научно-квалификационной работой.

V. Замечания и недостатки диссертационной работы

Несмотря на огромный научно-практический интерес к исследованию, диссертационная работа, на наш взгляд, не свободна от недостатков и рекомендаций, к которым, например, могут быть отнесены следующие:

1. При анализе нормативно-методической базы в работе встречаются отдельные некорректности переводов или интерпретации зарубежных стандартов, например:

- в табл. 1.1 (с.62) требование FAU_ARP («Автоматическая реакция аудита…»), на наш взгляд, некорректно сопоставляется с мерой A.9.1.2 (по ISO

27001:2005 – «Защита физического периметра», а по ISO 27001:2013 – «Ограничение доступа к сетям»);

- в табл. 1.3 (с.65) автор использует устаревший стандарт (2005 г. вместо 2013 г.) и некорректный перевод названий доменов, например: «Безопасность человеческих ресурсов» вместо «Вопросы информационной безопасности, связанные с персоналом»;

- на с. 101 база описания дефектов (weakness) в исходном коде (Common Weakness Enumeration) определена как система оценки уязвимостей (vulnerabilities).

На наш взгляд, работа бы выиграла, если бы автор привел дополнительный анализ (например, в разделе 1.6.5) концептуальных подходов и техник, представленных в тематических стандартах: ГОСТ Р ИСО/МЭК 27007-2014 («Руководства по аудиту СМИБ…»), ГОСТ Р 56045-2014 и ISO/IEC TR 27008:2011 («Рекомендации для аудиторов в отношении мер и средств контроля и управления ИБ…»), NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, NSA Infosec Assessment Methodology, NSA Infosec Evaluation Methodology.

2. В работе, на наш взгляд, без подробного критического анализа приведено множество определений понятия риска и его производных относительно проблематики ИБ (на с. 107 даже допускается его положительное/отрицательное значение, а на с. 82 базовое определение имеет несколько тавтологический оттенок – «вероятность реализации вероятного ущерба»). К слову, по этой же причине не совсем понятно, как соотнести формулу (1.1) к хоть каким-нибудь системам обеспечения ИБ (с. 36).

3. Можно было бы рекомендовать в перспективе актуализировать некоторые современные процедуры и меры в области аудита и управления ИБ, а именно учесть связь с БД угроз (и уязвимостей) ФСТЭК России, а также рассмотреть аудит и сертификацию систем менеджмента предприятий промышленности по ГОСТ Р 56939-2016 («Разработка безопасного программного обеспечения…»).

4. В работе встречаются отдельные оформительские опечатки, например, не все формулы пронумерованы, в формуле на с. 82 не раскрыты все используемые обозначения, на с. 84 имеются ссылки на ненаучные источники (представителей

масс-медиа), допустимый объем автореферата незначительно превышен, встречается технический сленг (например, «практический кейс», с.198).

В целом отмеченные недостатки не снижают научной значимости работы, так как поставленная в работе цель (судя по приведенным в работе значениям показателей имитационных моделей) достигнута. К достоинствам работы необходимо отнести широкий кругозор автора, полноту, актуальность и востребованность, самостоятельность, оригинальность. Оформление работы в целом соответствует ГОСТ.

Содержание и выводы представленного автореферата в полной мере соответствуют основным положениям диссертационной работы и позволяют оценить теоретическую и практическую значимость исследования.

Автореферат характеризуется логичностью изложения и соответствующим научным стилем написания. Выносимые положения аргументированы и понятны.

Можно **рекомендовать использование научно-практических результатов** диссертационной работы (соответственно, с учетом фактов успешного внедрения) предприятиям Комитета по энергетике и инженерному обеспечению (например, ГУП "ПИПГИС "Ленгипроинжпроект"), лицензиатам ФСТЭК России и ФСБ России (например, ООО «УЦ ГИС»), а также ОАО «Аэропорт «Пулково».

VI. Вывод

Таким образом, на наш взгляд, диссертационная работа Лившица И.И. представляет законченную научно-квалификационную работу, выполненную лично соискателем на актуальную тему, которая отличается научной новизной, теоретической значимостью и практической ценностью в области менеджмента информационной безопасности.

Автором в диссертации сформулирована и решена проблема, состоящая в разработке научно-методического аппарата аудита информационной безопасности интегрированных систем управления сложными промышленными объектами, имеющая важное значение для обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

На наш взгляд, диссертационная работа соответствует критериям (п.п. 9-14) «Положения о присуждении учёных степеней», утвержденным постановлением Правительства РФ от 24.09.2013 г. № 842, предъявляемым к диссертациям на соискание ученой степени доктора наук, а её автор, Лившиц Илья Иосифович, заслуживает присуждения ему учёной степени доктора технических наук по специальности 05.13.19 - Методы и системы защиты информации, информационная безопасность.

Отзыв заслушан, обсужден и одобрен *на заседании НТС АО «НПО «Эшелон».*

Протокол № 16/014 от 20 сентября 2018 г.

Президент АО «НПО «Эшелон»
доктор технических наук, старший научный сотрудник

Сергеевич Марков

Директор департамента тестирования и сертификации
кандидат технических наук

Виталий Викторович Вареница

« 1 » октября 2018 года

Контактная информация:
107023, Москва, ул.Электрозаводская, 24; тел./факс: +7 (495) 645-3810,
эл.почта: mail@npo-echelon.ru