ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РОССИЙСКОЙ АКАДЕМИИ НАУК ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ ДОКТОРА НАУК

аттестационное дело № _____

решение диссертационного совета 29.11.2018 г. № 2

О присуждении Лившицу Илье Иосифовичу, гражданину Российской Федерации, ученой степени доктора технических наук.

Диссертация «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 21 августа 2018 г., протокол № 1 диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, Министерства науки и высшего образования Российской Федерации, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года (с изменениями согласно приказам Минобрнауки России №105/нк от 11 апреля 2012 г. №574/нк от 15 октября 2014 г., № 386/нк от 27 апреля 2017 г., №748/нк от 12 июля 2017 г.).

Диссертацию на соискание ученой степени кандидата технических наук Лившиц Илья Иосифович защитил в 2012 году в диссертационном совете, созданном на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (диплом серия ДКН номер 177661). В настоящее время Лившиц Илья Иосифович работает старшим научным сотрудником лаборатории безопасности информационных систем Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

Диссертация выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук Министерства науки и высшего образования Российской Федерации.

Научный консультант – доктор технических наук, профессор МОЛДОВЯН Александр Андреевич, основное место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), главный научный сотрудник лаборатории безопасности информационных систем.

Официальные оппоненты:

КУСТОВ Владимир Николаевич, доктор технических наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I», профессор кафедры «Информатика и информационная безопасность»,

ЗИКРАТОВ Игорь Алексеевич, доктор технических наук, профессор, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, декан факультета Информационных систем и технологий,

ЛИПАТНИКОВ Валерий Алексеевич, доктор технических наук, профессор, Военная академия связи имени Маршала Советского Союза С. М. Буденного, старший научный сотрудник дали положительные отзывы на диссертацию.

Ведущая организация – акционерное общество «Научно-производственное объединение «ЭШЕЛОН», г. Москва в своем положительном отзыве, подписанном МАРКОВЫМ Алексеем Сергеевичем, доктором технических наук, профессором, старшим научным сотрудником, ВАРЕНИЦЕЙ Виталием Викторовичем, кандидатом технических наук, директором департамента тестирования и сертификации и утвержденном ЦИРЛОВЫМ Валентином Леонидовичем, кандидатом технических наук, доцентом, генеральным директором АО «НПО «Эшелон», указала, что диссертационная работа Лившица И.И. представляет собой законченную научно-квалификационную работу, выполненную лично соискателем на актуальную тему, которая отличается научной новизной, теоретической значимостью в области менеджмента информационной безопасности. Автором в диссертации

сформулирована и решена важная научно-техническая проблема, состоящая в разработке научно-методического аппарата аудита информационной безопасности (ИБ) интегрированных систем управления сложными промышленными объектами (СлПО), имеющая важное значение для обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

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:

- Комплекс полуформальных моделей (обобщенная модель интегрированной системы менеджмента (ИСМ) 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.
- 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.
- Метод исследования динамики сертификации систем менеджмента для СлПО, позволяющий формировать прогнозные оценки рисков ИБ глобального характера.
- Метод многошаговой оптимизации процесса аудита ИБ в интегрированной системе менеджмента для СлПО (по критериям осведомленности и ресурсоемкости), позволяющий, кроме того, получать в режиме, близком к режиму реального времени, оценки результативности системы менеджмента на различных этапах ЖЦ СлПО.

Содержание и выводы представленного автореферата в полной мере соответствуют основным положениям диссертационной работы и позволяют оценить теоретическую и практическую значимость исследования. Диссертационное исследование «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами»

является законченной научно-квалификационной работой и соответствует критериям, изложенным в пп. 9-14 “Положения о присуждении ученых степеней”, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемых к докторским диссертациям, а его автор Лившиц Илья Иосифович заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет **74** опубликованных работы, в том числе по теме диссертации **67** работ, из них опубликованных в изданиях, рекомендуемых ВАК РФ – **38**, в изданиях, индексируемых Scopus и/или Web of Science – **15**, а также в иных рецензируемых научных специализированных изданиях – **12**. Основные научные результаты опубликованы в **2** учебных пособиях в соавторстве объемом **11,92** п.л., **65** научных трудах общим объемом **24,77** п.л., из которых **45** статей объемом **14,86** п.п. выполнены в соавторстве, а **20** статей объемом **9,91** п.л. – лично.

Наиболее значимые работы по теме диссертации:

1. **Livshitz,** I.I., Lontsikh, P.A., Lontsikh, N.P., Kunakov, E.P., Drolova, E.Y. Implementation and auditing of risk management for the oil and gas company. Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. DOI: 10.1109/ITMQIS.2017.8085881. *Личный вклад соискателя – 50%.*
2. **Livshitz,** I.I., Ezrahovich, A.Y., Vladimirtsev, A.V., Karasev, S.N., Drolova, E.Y. Assessment of the impact of the modern risk-oriented standards on the security of the complex industrial facilities. Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. DOI: 10.1109/ITMQIS.2017.8085873. *Личный вклад соискателя – 30%.*
3. **Livshitz**, I.I., Nikiforova, K.A., Lontsikh, P.A., Karasev, S.N. The new aspects for the instantaneous information security audit. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. DOI: 10.1109/ITMQIS.2016.7751920. *Личный вклад соискателя – 50%.*

4. **Livshitz** I., Lontsikh P., Eliseev S. The Optimization Method of the Integrated Management System Security Audit. Proceedings of the FRUCT'20 (3-7 April 2017) pp. 248 – 254. ISSN 2305-7254. DOI: 10.23919/FRUCT.2017.8071319. *Личный вклад соискателя – 50%.*
5. **Лившиц** И.И. Менеджмент информационной безопасности // Стандарты и качество. – 2017. – № 9. – С. 48-52.
6. **Лившиц** И.И. Методика оптимизации программы аудита интегрированных систем менеджмента // Труды СПИИРАН. – 2016. – № 5. – С. 52 – 68.
7. **Лившиц** И.И. Оценка методических подходов для формирования систем безопасности сложных промышленных объектов топливно-энергетического комплекса // Вопросы защиты информации. – 2016. – № 1. – С. 56 – 61.
8. **Лившиц** И.И. Методика определения активов при внедрении и сертификации СМИБ в соответствии с требованиями ГОСТ Р ИСО серии 27001 и СТО Газпром СОИБ серии 4.2 // Вопросы защиты информации. – 2015. – № 4. – С. 43 – 51.
9. **Лившиц** И.И. Формирование концепции мгновенных аудитов информационной безопасности // Труды СПИИРАН. – 2015. – № 6 (43). – С. 253 – 270.
10. **Лившиц** И.И. Определение активов при внедрении и сертификации СМИБ // Стандарты и качество. – 2015. – № 6 (936). – С. 84 – 85.
11. **Лившиц** И.И. Исследование динамики сертификации по международным стандартам ISO для целей обеспечения комплексной безопасности // Вопросы защиты информации. – 2015. – № 2. – С. 48 – 56.
12. **Лившиц** И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. – 2014. – № 6. – С. 72 – 94.
13. **Лившиц** И.И. Применение модели СМИБ для оценки защищенности интегрированных систем менеджмента // Труды СПИИРАН. – 2013. – № 8 (31). – С. 147 – 162.

Оригинальность содержания диссертации составляет не менее **92%** от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в

соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На автореферат диссертации поступило **25** отзывов, все отзывы положительны:

1) Омский Государственный технический университет. Отзыв составила д.т.н., профессор кафедры «Автоматизированные системы обработки информации и управления» Денисова Л.А. Замечания: Схема разделения по двум интерфейсам множества данных A (требований к аудиту ИБ), K (мер и средств обеспечения ИБ), T (совокупности требований в аспекте ИБ для СлПО) и G (совокупности ДД и выявленных рисков) на рисунке 2 (страница 14) отражает только соответствие отдельным стандартам ISO и ISO/IEC, не учитывая дополнительные отраслевые требования (указанные на странице 15); Используемое диссертации понятие «сложный промышленный объект (СлПО)» не в полной мере учитывает уже существующие термины «КВО», «КИИ», «КСИИ». Вероятнее, правильнее было бы говорить об опасных объектах, применительно к определенной отрасли, не вводя обобщения и определяя четкие границы конкретных объектов (как показано на стр. 27-29).
2) Санкт-Петербургский государственный экономический университет. Отзыв составила к.э.н., доцент, профессор кафедры корпоративных финансов и оценки бизнеса Пузыня Н.Ю. Замечания: Тезисы автора об экономической сути угроз безопасности информации (УБИ) и деструктивных действиях злоумышленников, приведенных на стр. 6 и 17 автореферата, выглядят недостаточно обоснованными. Представляется, что при выбранной теме диссертационного исследования для описания аспектов экономической безопасности нужны дополнительные инструменты анализа, особенно для описания характеристик объектов нематериального характера; В автореферате не приведены ссылки на аналогичные или близкие работы по той же тематике, выполненных в мире, например, в области противодействия целевым атакам; Наличие конкретных примеров метрик ИБ при описании предложенного метода оптимизации метрики для аудитов ИБ сложных промышленных объектов могло бы улучшить восприятие материала; Наличие сведений о комплексных стоимостных (экономических) показателях,

применяемых при оценке ущерба активам СлПО при описании предложенного метода «мгновенных» аудитов, могло бы улучшить восприятие материала.

3) Иркутский национальный исследовательский технический университет. Отзыв составила д.т.н., профессор, профессор кафедры математики Сергиенко Л.С., утвердил ректор ФГБОУ ВО ИРНИТУ д.т.н. Корняков М.В. Замечания: При формировании обобщенной модели аудитов ИСМ для обеспечения безопасности СлПО (рис. 1 на стр.12) были приняты во внимание только несколько существующих стандартов ГОСТ Р ИСО/МЭК, как переводы международных стандартов тех же серий (например, серии 9001, 27001, 22301 и пр.). В дальнейшем при изучении практических примеров для конкретных объектов требования обеспечения безопасности СлПО могли бы быть рассмотрены более подробно, например, с учетом требований ГОСТ Р МЭК серии 61508, серии 61511. Дополнительно можно отметить, что учет требований и ГОСТ Р ИСО/МЭК серии 15408 также мог улучшить в целом работу; Отсутствие в автореферате конкретных способов практического применения предложенных моделей и методов для выбранного объекта (аэропортовых комплексов) в аспекте оптимизации метрик для аудитов ИБ не позволяет в полной мере оценить практическую значимость для обеспечения безопасного функционирования выбранной категории объектов; В автореферате детально не раскрыт подход к формированию альтернативных множеств мер (средств) обеспечения безопасности в соответствии с предложенным методом оптимизации программы аудитов ИБ. В частности, при выполнении проверок ФСТЭК России для значимых объектов КИИ меры (средства) должны выбираться из официальных приказов № 235 и № 239.

4) Томский политехнический университет. Отзыв составила д.т.н., профессор Отделения Автоматизации и робототехники Захарова А.А. Замечания: Введенное понятие «сложный промышленный объект» (СлПО) не в полной мере ссылается на уже существующие термины «КВО», «КИИ», «КСИИ». Даже с учетом того, что эти термины все разные и даже КСИИ в мае 2018 г.

отменен ФСТЭК России, было бы корректно говорить об опасных объектах, применительно к определенной отрасли, не вводя такие обобщения; В автореферате следовало бы привести несколько кратких примеров реальных метрик, применяемых при аудитах ИБ. Это позволило бы объективно оценивать результаты их оптимального отбора и результативного применения для заданных целей аудита, особенно с учетом многих актов о внедрении; В автореферате на рис. 2 (стр. 14) и рис. 9 (стр.29) в предложенных моделях аудитов ИБ не указаны широко используемые в РФ стандарты оценки по «общим критериям» ГОСТ Р ИСО 15408, а также не отражено взаимодействие с Банком данных угроз безопасности информации ФСТЭК России.

5) ООО «Русский Регистр – Московская инспекция». Отзыв подготовил директор, к.т.н., старший научный сотрудник Крикун В.М. Замечания: Процедуры оценки рисков (см. рисунки 1 и 2) приведены только в соответствии со стандартом ISO 31000:2009 и ISO/IEC 27005:2011. В соответствии с данным стандартом процесс оценки рисков (risk assessment) состоит из трёх последовательных процедур: идентификации рисков (identify risks), анализа рисков (analyse risks) и оценивания или сравнительной оценки рисков (evaluate risks). В диссертации не рассматриваются подробно аспекты расчета количественной оценки риска (risk estimation) и оценивания риска (risk evaluation) применительно к заявленному новому методу «мгновенных» аудитов.
6) Журнал «Стандарты и Качество». Отзыв подготовил д.т.н., д.э.н., профессор Воронин Г.П. Замечания: Приведено достаточно общее описание предложенного метода оптимизации метрик для аудитов информационной безопасности, не позволяющее в должной мере оценить его оригинальность и значимость для процесса обеспечения безопасного функционирования объектов критичной инфраструктуры; При формировании обобщенной модели аудитов ИСМ в автореферате недостаточно учитывается отраслевая специфика предприятий, отнесенных к СлПО. Это обстоятельство не дает объективных условий для формирования результатов оценки уровня

защищенности и, как следствие, может повлечь за собой ряд сложностей при формировании корректного перечня мер (средств) обеспечения ИБ.

7) АО «ЦНИИМФ». Отзыв подготовил к.в.н., доцент Юрин И.В. Замечания: Представляется, что Глава 2 в диссертационной работе несколько перегружена, а некоторые разделы и подразделы излишни. Следовало бы приводить в тексте более «концентрированные» научные результаты, что улучшило бы общую ясность и повысило бы компактность диссертации; Для оценки ущерба от возможных негативных сценариев для СлПО в диссертации предложена методика формирования показателей (метрик) оценивания ИБ, что требует дополнительных пояснений, в том числе экономического характера. Следует предположить, что без учета вопросов экономического блока весьма сложно исследовать проблемы обеспечения безопасности и достигнуть цели исследования, состоящей в повышении качества аудита в интегрированных системах менеджмента для сложных промышленных объектов.
8) ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» Отзыв подготовил д.т.н., профессор кафедры «Комплексное обеспечение информационной безопасности» Ныpков А.П. Замечания: Для оценки ущерба от возможных негативных сценариев для сложных промышленных объектов предложена методика формирования показателей (метрик) оценивания информационной безопасности, что требует дополнительных пояснений; Наличие конкретных примеров реализации, помимо простого перечисления применения в различных отраслях промышленности, предложенной модели оптимизации метрик для аудитов ИБ, могло бы улучшить восприятие защищаемых положений; Можно отметить ряд незначительных недостатков, таких как отсутствие достаточных пояснений к некоторым представленным рисункам и таблицам.
9) НИИ «Вектор». Отзыв подготовил начальник сектора системной интеграции Центра защиты информации к.т.н. Белкин Т.Г. Замечания: В автореферате не определены явно возможность адаптации представленных в работе моделей и методов для определенного широкого класса сложных промышленных

объектов с системой управления «жесткого реального времени». Предполагается, что помимо стандартов серии ISO/IEC могут быть применены «целевые» стандарты IEC серии 61508 и 61511; В автореферате не приводится оценка достоверности и полноты данные, на основе которых осуществлялся расчёт показателей, относящихся к третьему защищаемому положению: методу определения динамических зависимостей сертификации ISO. Предполагается, что это объективная статистика ISO, но только ссылки на сайт отчета недостаточно для научных исследований; На рис. 2 (стр. 14) и рис. 9 (стр.29) в предложенных моделях аудитов ИБ не указаны широко используемые в РФ стандарты ГОСТ Р ИСО 15408, а также не отражено взаимодействие с Банком данных угроз безопасности информации ФСТЭК России; В тексте отсутствует пояснение, каким образом и с какими ограничениями новые предложенные модели и методы были использованы при выполнении экспериментальных исследований (см. Таблицу 6 стр. 30).

10) Белорусский Государственный институт Стандартизации и Сертификации. Отзыв подготовила директор, к.т.н., Осмола И.И. Замечания: В автореферате приведено много сокращений, что значительно затрудняет анализ представленных научных положений и практических результатов, а также отсутствует достаточное количество пояснений к некоторым рисункам; В автореферате автору следовало бы привести несколько примеров состава метрик, применяемых при аудитах ИБ. Это позволило бы в полной мере определить объективность результатов их оценки для заданных целей аудита. Только на основании рисунка 3 не представляется возможным выполнить такой анализ.

11) УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь. Отзыв подготовил к.т.н., доцент, подполковник Маликов В.В. Замечания: В автореферате довольно кратко представлено описание модели оптимизации метрик для аудитов ИБ и не приводятся примеры конкретных сценариев (методов) применения разработанных новых моделей; В автореферате отсутствуют сведения о комплексных стоимостных показателях,

применяемых при оценки ущерба активам СлПО при выполнении аудита ИБ с помощью предложенной методики «мгновенных» аудитов ИБ; В автореферате отсутствуют ссылки на аналогичные или близкие работы по той же тематике, выполненных в мире, например, в области противодействия целевым атакам.

12) Белоруссий государственный университет информатики и радиоэлектроники. Отзыв подготовил заведующий кафедрой защиты информации д.т.н., профессор Т.В. Борботько. Замечания: При формировании обобщенной модели аудитов ИСМ в автореферате не отражена отраслевая специфика предприятий, отнесенных к СлПО. Это обстоятельство не в полной мере позволяет обеспечить объективность результатов оценки уровня защищенности и, как следствие, может повлечь за собой ряд ограничений при формировании корректного перечня мер (средств) обеспечения ИБ; В автореферате не раскрыт подход к формированию альтернативных множеств мер (средств) обеспечения безопасности, с учетом заявленных ограничений предложенного метода оптимизации программы аудитов ИБ.

13) Морской государственный университет им. адмирала Г.И. Невельского. Отзыв подготовила к.п.н., доцент, зав. каф. информационных аналитических систем информационной безопасности Щербинина И.А. Замечание: недостаточное внимание уделено анализу научных трудов по схожей проблематике, выполненных российскими авторами в академических институтах, и существующих программных комплексов оценки рисков возникновения чрезвычайных ситуаций, в том числе на объектах критической инфраструктуры.

14) Московский государственный психолого-педагогический университет. Отзыв подготовил д.т.н., профессор Воронов М.В., заведующий кафедрой прикладной математики. Замечания: Предложенный метод оптимизации численных показателей для аудитов информационной безопасности ориентирован, как видно из текста, только на применение международных ISO/IEC и национальных стандартов ГОСТ РФ ИСО/МЭК. Очевидно, было бы более целесообразно рассмотреть и иные нормативные документы по

аудиту, касающиеся аспектов информационной безопасности; Наличие конкретных примеров реализации предложенного метода для аудитов информационной безопасности могло бы улучшить восприятие материала; В тексте автореферата отсутствуют достаточно убедительные пояснения, каким образом предложенные в диссертации модели и методы были использованы при выполнении экспериментальных исследований и расчетов; Имеет место использование нерасшифрованных сокращений и отсутствуют достаточно полные пояснения к некоторым рисункам.

15) Учебный центр «Спецпроект». Отзыв подготовил ведущий преподаватель, д.т.н., профессор, Швед В.Г. Замечания: Для оценки ущерба от возможных негативных сценариев для сложных промышленных объектов в работе предложена методика формирования показателей (метрик) оценивания информационной безопасности, что требует дополнительных пояснений, в том числе, экономического характера. Следует предположить, что без учета вопросов экономического характера и соответствующих рисков (остаточных рисков) весьма сложно исследовать проблемы обеспечения безопасности и достигнуть цели исследования, состоящей в повышении качества аудита в интегрированных системах менеджмента для сложных промышленных объектов; На рис. 2, стр. 14 в диссертации приведена базовая модель аудитов ИБ, в которой не указаны широко используемые в РФ ГОСТ Р ИСО 15408, а также не отражено взаимодействие с Банком данных угроз безопасности информации ФСТЭК России; В автореферате отсутствуют практические рекомендации по применению разработанных моделей и методов оценки соответствия (аудита) информационной безопасности для формирования требований защиты специальных ведомственных и отраслевых корпоративных информационных систем.

16) ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)». Отзыв подготовил профессор кафедры ИБ, д.т.н., профессор Петренко С.А. Замечания: На рис. 2 (стр. 14) приведена базовая модель аудитов ИБ, в которой не указаны широко используемые в РФ стандарты, в частности,

ГОСТ Р ИСО 15408; В тексте отсутствуют достаточно убедительные пояснения, каким образом модели и методы, предложенные в диссертации как защищаемые научные положения, были использованы при выполнении экспериментальных исследований; Автор не приводит в автореферате достаточную информацию о лицензионной чистоте программного обеспечения, применяемого для практической оценки разработанных моделей и методов; Можно отметить ряд незначительных недостатков, таких как наличие нерасшифрованных сокращений в тексте или отсутствие достаточных пояснений к некоторым рисункам, представленные в автореферате.

17) ООО «Газпром нефтехим Салават». Отзыв подготовил главный специалист отдела ИБ СКЗ к.т.н. Павловский А.В. Замечания: В автореферате не приводится точно состав метрик, применяемых при аудитах ИБ, что не позволяет в полной мере определить объективность результатов их оценки. Не представляется возможным выполнить такой анализ в полной мере только на основании рис. 1 и рис. 2; В автореферате довольно кратко представлено описание модели оптимизации метрик для аудитов информационной безопасности и не приводятся примеры конкретных сценариев (методов) применения разработанных новых моделей; В автореферате не определена явно возможность и целесообразность адаптации представленных в работе моделей и методов для СлПО с системой управления «жесткого реального времени»; Наличие конкретных сведений о комплексных стоимостных показателях, применяемых при оценке ущерба активам сложных промышленных объектов при применении предложенной модели «мгновенных» аудитов информационной безопасности могло бы улучшить восприятие материала.

18) ПАО «Интелтех». Отзыв подготовили, д.т.н., профессор Будко П.А. и д.в.н., профессор Густов А.А, утвердил первый заместитель ген. директора к.т.н., доцент И.А. Кулешов. Замечания: Из базовой модели аудита ИСМ, представленной на рис. 2 автореферата и ее описания не ясно, что подразумевал соискатель под множеством значений определенных и

неопределенных факторов А, А', А'' и А''', сущность которых в описании модели не раскрыта; 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.

19) ОАО «АГАТ – системы управления», Республика Беларусь. Отзыв подготовил главный специалист по защите информации д.т.н., профессор Бобов М.Н. Замечания: Не представлено детальное обоснование формирования набора применяемых метрик в предложенном методе (см. рисунок 3, стр. 15); Отсутствует анализ результативности и параметров быстродействия по модифицированной формуле Apdex в ходе проводимого экспериментального исследования (см. формулу 11, стр. 30); В тексте отсутствует пояснение, каким образом новые предложенные модели и методы были использованы при выполнении экспериментальных исследований (см. таблицу 6, стр. 30); В автореферате отсутствуют сведения о комплексных стоимостных показателях, применяемых при оценки ущерба активам СлПО при выполнении аудита ИБ с помощью предложенной методики «мгновенных» аудитов ИБ (стр. 19-20);

20) Новосибирский государственный технический университет. Отзыв подготовили профессор кафедры электротехнических комплексов д.т.н., с.н.с. Порсев Е.Г. и доцент кафедры ЭТК к.т.н., доцент Малоземов Б.В. Замечания: Предложенный метод оптимизации численных показателей (метрик) для аудитов информационной безопасности (первое защищаемое научное положение) учитывает только требования модальных сертификационных международных стандартов ISO/IEC и национальных стандартов ГОСТ Р ИСО/МЭК. Очевидно, следовало бы рассмотреть и иные нормативные документы по аудиту, касающиеся аспектов информационной безопасности, в

частности, ФСБ и ФСТЭК России; Можно отметить, что наличие в тексте конкретных спецификаций в примерах реализации предложенного метода для аудитов информационной безопасности указанных объектов (аэропортовых комплексов) могло бы улучшить восприятие материала; В тексте не представлены достаточные пояснения, каким образом предложенные в диссертации модели и методы аудита информационной безопасности в интегрированных системах менеджмента, были использованы при выполнении экспериментальных исследований и расчетов, в частности, анализа быстродействия; Можно отметить ряд незначительных недостатков, таких как наличие нерасшифрованных сокращений в тексте или отсутствие достаточных пояснений к некоторым рисункам, представленные в автореферате, например, для рис. 9 (стр. 29) не ясно, как именно получено такое распределение.

21) Институт проблем управления РАН. Отзыв подготовил главный научный сотрудник, д.т.н., профессор Ицкович Э.Л. Замечания: Не ясен смысл и цель рассуждений автора об экономической сути угроз безопасности информации и деструктивных действий, приведенных на стр. 6 и 17. Очевидно, что в диссертации, которая не посвящена в полном объеме изучению аспектов экономической безопасности, наличие такого анализа представляется несколько избыточным в заявленном контексте; При исследовании предметной области оценки рисков информационной безопасности в нотации надежности технических систем, представленной на рис. 1 (стр. 12), 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.

22) Институт пути, строительства и сооружений Российского университета транспорта (МИИТ). Отзыв подготовил профессор кафедры «Менеджмент качества», д.т.н., профессор Азаров В.Н. Замечания: В представленном варианте не в полной мере отражена специфика функционирования объектов

КИИ (как это требуется по ФЗ-187). Более явный и математически корректный учет отраслевой специфики для выбранного примера – объектов ТЭК при формировании обобщенной модели аудитов ИСМ мог бы улучшить восприятие материала; Приведенный пример формирования и практического применения обобщенной модели аудитов ИСМ с учетом специфики аэропортовых комплексов нуждается в дополнительных пояснениях: как по составу функциональных подсистем, так и по представленным оценкам весовых коэффициентов (α, β, φ, μ); В автореферате не приводятся данные, на основе которых осуществлялся расчёт показателей, относящихся к третьему защищаемому положению: методу исследования динамических зависимостей сертификации ISO. Это обстоятельство несколько затрудняет анализ результатов, приведенных в таблице 2; Предоставленное в автореферате краткое описание практического применения предложенных моделей и методов содержит ссылку на ПО MPriority. Но в тексте автореферата не показано точно, какие расчеты и какие необходимые математические самопроверки выполнялись с помощью указанного ПО для матриц парного сравнения в методе МАИ.

23) ФГБУ «Главный научный метрологический центр» Минобороны России. Отзыв подготовил главный научный сотрудник, д.т.н., профессор Храменков В.Н. Замечания: В главе 3 автореферата приведено недостаточно подробное описание предложенной модели оптимизации метрик для аудитов информационной безопасности, не позволяющее в должной мере оценить его оригинальность и значимость для процесса обеспечения безопасного функционирования объектов критичной инфраструктуры. Кроме того, в модели проблемной ситуации, представленной выражением (1) было бы целесообразно в составе общей информации указать место измерительной информации, получаемой с помощью средств измерения и измерительного контроля.

24) ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева». Отзыв подготовил д.т.н., профессор Сергеев В.В. Замечания: При исследовании предметной области и

формировании обобщенной модели ИСМ (интегрированной системы менеджмента) для обеспечения безопасности сложных промышленных объектов (рис. 1 на стр. 12) были учтены частично требования только нескольких существующих стандартов ГОСТ Р ИСО/МЭК. При изучении конкретных объектов могли бы быть рассмотрены более подробно требования обеспечения безопасности сложных промышленных объектов; Не в полной мере раскрыто новое введенное понятие «сложный промышленный объект» (СлПО), не представлена явная связь с первым защищаемым положением «модели ИСМ для обеспечения безопасности СлПО»; В автореферате не раскрыт подход к формированию альтернативных множеств мер (средств) обеспечения безопасности с учетом заявленных ограничений предложенного метода оптимизации программы аудитов информационной безопасности; В частности, при выполнении официальных проверок ФСТЭК России для значимых объектов КИИ меры (средства) должны выбираться из официальных приказов (№ 235 и № 239).

25) ООО «ТМС РУС». Отзыв подготовила ведущий эксперт по системам менеджмента д.э.н., профессор Скрипко Л.Е. Замечания: Не ясен смысл и цель рассуждений автора об экономической сути угроз безопасности информации, приведенных на стр. 5 и 6. Очевидно, что в диссертации, которая не посвящена в полном объеме изучению аспектов экономической безопасности, наличие такого анализа представляется несколько избыточным в заявленном контексте; При вычислении стоимости защищаемых активов в тексте диссертации в формуле на стр. 14 не используются веса, поэтому все не все виды последствий от деструктивных действий (например, финансовые, репутационные, производственные и т.п.) могут считаются равнозначными; В автореферате довольно кратко представлено описание модели сценариев реализации угроз и не приводятся примеры конкретных сценариев.

Выбор **официальных оппонентов** и ведущей организации обосновывается тем, что доктор технических наук, профессор КУСТОВ Владимир Николаевич является известным ученым в области обеспечения информационной безопасности,

исследованиях степени защиты критичных систем, как государственных информационных систем, так и коммерческих систем обеспечения безопасности, ведет большую научную и преподавательскую деятельность;

доктор технических наук, профессор ЗИКРАТОВ Игорь Алексеевич, является известным ученым в области методов кодирования и защиты информации, теории передачи сигналов, общей теории связи, ведет большую научную и преподавательскую деятельность;

доктор технических наук, профессор ЛИПАТНИКОВ Валерий Алексеевич, является известным ученым в области обеспечения информационной безопасности, проведении аудитов информационной безопасности современных систем менеджмента, ведет большую научную и преподавательскую деятельность.

Ведущая организация – акционерное общество «Научно-производственное объединение «ЭШЕЛОН», г. Москва, является широко известной как в России, так и за рубежом организацией в области разработки и создания систем защиты информации, составляющей государственную тайну, а также защиты конфиденциальной информации, работ в области аудита информационных систем, аттестации и сертификации средств защиты информации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны новые модели, направленные на обеспечение информационной безопасности сложных промышленных объектов (СлПО), и система численных показателей информационной безопасности (ИБ), характеризующих качество проведения аудита ИБ интегрированных систем управления (ИСУ) СлПО;

метод проведения аудита ИБ ИСУ СлПО, обеспечивающий сокращение временных и ресурсных затрат при сохранении требуемого качества результатов аудита;

метод исследования динамики сертификации ИСУ СлПО, ориентированный на использование как отечественных, так и международных стандартов ISO;

метод многошаговой оптимизации процесса аудита ИБ ИСУ СлПО, который, в отличие от известных методов, обеспечивает своевременные координацию и

распределение ресурсов, а также оперативное информирование лица, принимающего решение (ЛПР), об оценке результативности аудита ИСУ.

предложены: обобщенная модель ИСУ СлПО, отражающая особенности аудита ИБ и базовая модель аудита ИСУ СлПО, в которых раскрыта специфика процесса планирования, выполнения и анализа результатов аудита ИБ ИСУ СлПО, заключающаяся в широком применении системы численных показателей качества аудита ИБ ИСУ СлПО как компонента ИСУ СлПО согласно применимым требованиям;

расширенный перечень критериев, используемый в разработанном методе проведения аудита ИБ ИСУ СлПО, который ориентирован на учет требований регуляторов и/или отраслевой специфики и применение численных показателей качества аудита ИБ ИСУ СлПО с учетом специфики обеспечения ИСУ различных видов СлПО;

новый принцип управления аудитом ИБ ИСУ СлПО по частоте с предоставлением ЛПР оценки роста уровня ИБ ИСУ СлПО как показателя результативности ИСУ и соответствия ИБ применимым требованиям;

новый подход к обоснованию динамически изменяемых требований ИБ СлПО, выраженных в изменении предпочтений ЛПР по составу внедряемых систем менеджмента качества как компонентов ИСУ СлПО, прошедших внешний независимый аудит ИБ с формированием прогнозных оценок уровня ИБ ИСУ СлПО;

новый подход к оптимизации трудно формализуемых процессов, примером которых является аудит ИБ ИСУ СлПО, реализованный в разработанном методе многошаговой оптимизации процесса аудита ИБ ИСУ СлПО и обеспечивающий, в отличие от существующих методов циклической непрерывной оценкой ИБ, научно-обоснованное и целенаправленное функционирование ИСУ СлПО.

введены: новый термин «сложный промышленный объект» (СлПО), под которым понимается «технический объект, имеющий систему управления, несанкционированное изменение штатного режима функционирования которого, связанное с нарушением свойств ИБ, может привести к угрозе техногенных катастроф с необратимыми последствиями»;

новая метрика «лидер ранга», которая применяется при определении коэффициентов зависимости относительных величин, характеризующих уровень ИБ СлПО для различных отраслей; при этом ранжирование СлПО отраслей по введенной метрике «лидер ранга» позволяет проследить их взаимосвязь с общим достигнутым эффектом по конкретной отрасли для «лидеров» разных рангов и обеспечивает получение обобщенной оценки СлПО по существующим кодам ЕАС, не зависимой от имеющихся ограничений.

Теоретическая значимость исследования состоит в:

обосновании возможности применения новых моделей и методов обеспечения ИБ путем проведения ее независимой оценки, которую обеспечивает аудит ИБ ИСУ СлПО, созданных в соответствии с требованиями современных риск-ориентированных стандартов;

определении новых критериев обоснования и выбора требований аудита ИБ, оптимальных для конкретного СлПО, а также новых условий формирования этих критериев;

развитии научного аппарата независимой оценки ИБ ИСУ СлПО.

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) **использованы** методы системного анализа, декомпозиции и агрегирования, теории автоматизированного управления, теории множеств, теории вероятностей, теории многокритериального выбора при фиксированном наборе альтернатив.

Теоретическое значение имеют следующие научные результаты:

Первое научное положение позволяет расширить границы применимости теории обеспечения ИБ для СлПО, отличительными свойствами которой являются:

– непредсказуемость последующих состояний и наличие иерархической структуры исследуемого объекта, усложняющей создание точных адекватных универсальных моделей;

– постоянное изменение требований: юридических, технологических и пр., приводящих к появлению возмущений в существующих каналах управления;

– крайне малое время реакции на возмущения, требующее создания новых моделей, позволяющих ЛПР принимать «разумные решения» в режиме, близком к реальному масштабу времени.

Второе научное положение позволяет на основе принципа «мгновенных аудитов» ИБ ИСУ СлПО реализовать ряд существенно важных методических аспектов:

– раздельные интерфейсы для внешних и внутренних заинтересованных сторон аудита ИБ, реализующие предоставление информации с заданной частотностью;

– включение контуров гибкой обратной связи по всем типам аудита, что позволяет повысить уровень обеспечения ИБ и оперативно агрегировать всю необходимую информацию для ЛПР;

– вовлечение в принятие «разумных решений» ЛПР, которое может являться коллегиальным органом управления, в том числе, с участием внешних заинтересованных сторон.

Третье научное положение позволяет на основе учета результатов исследования динамики сертификации по стандартам ISO использовать необходимую информацию в интересах поддержки принятия «разумных решений» ЛПР при обеспечении ИБ ИСУ СлПО благодаря:

– формированию основанных на публичной достоверной статистике ISO оценок приемлемости выбора: по составу систем менеджмента качества, по необходимости внешней оценки (аудита) для функций обеспечения стабильного роста, безопасности и устойчивости бизнес-процессов, защиты ценных активов (в том числе нематериальных);

– определению и учету коэффициентов зависимости для отраслей, являющихся «лидерами по рангам», рассчитываемых для произвольного количества отраслей промышленности.

Четвертое научное положение включает систему методов многошаговой оптимизации аудита ИБ ИСУ СлПО и позволяет реализовать гибкий подход к выполнению аудита ИБ в зависимости от фазы жизненного цикла СлПО.

Выдвинутые теоретические положения подтверждены практикой в процессе выполнения диссертационного исследования и открывают новые перспективы для работ в области управления ИБ, в частности, аудита ИБ.

Практическая ценность полученных результатов состоит в улучшении методов независимой оценки (аудита) ИБ для СлПО, основанных на применении оптимального множества риск-ориентированных стандартов в составе ИСУ, 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 ИСУ СлПО реализованы как функционально завершенный элемент в системе мероприятий комплекса обеспечения ИБ СлПО. Результаты диссертационного исследования получили практическую реализацию в следующих предметных областях:

–Информационные технологии: в компании ИТСК (Российская Федерация) реализован комплекс новых методов аудита ИБ с учетом иерархической системы критериев модели ИСУ;

–Воздушный транспорт: в международных аэропортах Алматы и Астаны (Республика Казахстан) реализован комплекс новых моделей и методов аудита ИБ в составе ИСУ в соответствии с требованиями международных стандартов ISO и дополнительных отраслевых требований IATA (ISAGO);

–Системная интеграция: в группе компаний «Газинформсервис» (Российская Федерация) реализован комплекс новых моделей и методов аудита ИБ при создании ИСУ, в том числе для группы компаний «Газпромнефть»;

–Образование: в международной компании AQS (Азербайджан) реализованы новые принципы обучения аудиторов (ведущих аудиторов) ИБ, основанные на разработанных методах проведения аудита ИБ, в том числе, с учетом требований международных стандартов ISO.

–Банковское дело: в Акционерном коммерческом банке «Рускобанк» (Российская Федерация) реализован комплекс новых методов проведения аудита ИБ, в том числе, с учетом требований ISO и СТО БР ИББС;

–Управление коммунальными объектами критической инфраструктуры: в ГУП «Водоканал Санкт-Петербурга» (Российская Федерация) реализован комплекс новых методов проведения аудита ИБ ИСУ с учетом требований, предъявляемых к СлПО.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

–метод проведения внутренних аудитов интегрированной системы менеджмента;

–методы снижения издержек в процессе разработки и внедрения интегрированной системы менеджмента;

внедрены в Международном аэропорту Алматы (Республика Казахстан):

–метод обеспечения доступности информационных систем на основе требований международных стандартов

–методы снижения издержек в процессе разработки и внедрения интегрированной системы менеджмента

–метод проведения внутренних аудитов интегрированной системы менеджмента

внедрены в Международном аэропорту Астаны (Республика Казахстан):

–метод обеспечения доступности информационных систем на основе требований международных стандартов

–модель аудитов интегрированных систем менеджмента для критичных объектов

внедрены в компании ИТСК (Российская Федерация):

–модель оптимизации проведения аудитов кредитных организаций.

–модель управления приоритетных изменений показателей информационной безопасности

–метод минимизации затрат на внедрение мер и средств обеспечения информационной безопасности

внедрены в АКБ «Рускобанк» (Российская Федерация):

–метод многошаговой оптимизации процессов аудита интегрированной системы менеджмента

–метод исследования динамики сертификации на основе требований международных стандартов

внедрены в компании AQS (Азербайджан):

–модель проведения интегрированной системы менеджмента для сложных промышленных объектов

–метод многошаговой оптимизации процессов аудита интегрированной системы менеджмента

–система численных показателей (метрик) информационной безопасности.

внедрены в компании Газинформсервис» (Российская Федерация) и в ГУП «Водоканал Санкт-Петербурга»:

–метод многошаговой оптимизации процессов аудита интегрированной системы менеджмента

–метод исследования динамики сертификации на основе требований международных стандартов.

сформулированы рекомендации по применению результатов работы с учетом новых законодательных инициатив (в частности, ФЗ-187) для обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации. Научные положения, представленные в диссертации, обеспечивают методическое сопровождение процессов автоматизации формирования численных показателей ИБ, сокращения длительности процессов планирования, выполнения и анализа результатов аудита ИБ ИСУ СлПО.

представлены перспективы дальнейшей разработки тематики:

–разработка модели перехода от фиксированного перечня угроз безопасности информации к модели комплексного оценивания рисков в процессе реализации

аудита ИБ. В прогнозируемой перспективе это позволит обеспечить «единое управленческое поле» обеспечения безопасности всех процессов в современных и перспективных ИСУ СлПО.

–разработка модели реализации комплексного аудита ИБ, которая позволила бы предоставлять оценки всех процессов в современных ИСУ СлПО в едином пространстве, а не по отдельности (управление персоналом, управление инцидентами, управление рисками и пр.), что значительно повысило бы шансы на успех в информационном противоборстве с потенциальными злоумышленниками.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ

достоверность полученных результатов подтверждена:

–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 («НПО «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 аудита ИБ;

–результатами независимых оценок (аудита) ИСУ в рассматриваемых предметных областях («Русский Регистр», TUV, Lloyd, BSI, DNV);

–публикацией результатов диссертационного исследования в рецензируемых научных изданиях, в том числе, индексируемых в международных базах цитирования Scopus и Web of Science.

теория построена на известных принципах, проверенных достоверных публичных данных и проверенных научных фактах с использованием современных известных и апробированных методов исследования, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области защиты информации, в том числе для обеспечения безопасности объектов критической инфраструктуры;

использованы полученные характеристики для сравнения с данными, приведенными в современной научной литературе по защите информации и иных достоверных публичных статистических материалах;

использованы современные методы сбора, обработки, анализа исходной информации, представительные выборочные совокупности с обоснованием подбора объектов (единиц) наблюдения (в частности, статистики ISO за длительный интервал наблюдений и т.п.)

Личный вклад соискателя состоит в:

– анализе современного состояния дел в области защиты информации, в том числе для обеспечения безопасности объектов критической инфраструктуры;

– формировании и представлении нового подхода к учету рисков ИБ и выполнению аудита ИБ ИСУ СлПО;

– разработке и представлении нового метода «мгновенных аудитов» ИБ;

– формировании и представлении новых метрик аудита ИБ ИСУ СлПО;

– формировании и представлении новых подходов к выбору активов СлПО и оценке их ИБ;

– формировании новых оценок доступности элементов информационных и телекоммуникационных систем при выполнении аудита ИБ ИСУ СлПО;

– формировании и представлении новых методов определения результативности ИСУ СлПО;

– подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Лившиц И.И. в своей диссертационной работе решил крупную научно-техническую проблему разработки методологических и методических основ оптимизации процессов аудита информационной безопасности интегрированных систем управления сложными промышленными объектами, имеющую важное государственное значение.

На заседании 29.11.2018 г. диссертационный совет принял решение присудить Лившицу И.И. ученую степень доктора технических наук.

При проведении тайного голосования диссертационный совет в количестве 21 человека, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из **26** человек, входящих в состав совета, проголосовали: за 14, против 3, недействительных бюллетеней 4.

Председат

доктор тех

член-корр Юсупов Рафаэль Мидхатович

Ученый се

кандидат т Зайцева Александра Алексеевна

29.11.2018