Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

199178, Санкт-Петербург, 14 линия, 3
Телефон: (812)328-33-11
Факс: (812)328-44-50
E-mail: spiiran@iias.spb.su
http://www.spiiras.nw.ru
ОКПО 04683303, ОГРН 1027800514411
ИНН/КПП 7801003920/780101001

УТВЕРЖДАЮ

.Л.

Федерального государственного бюджетного учреждения науки
Санкт-Петербургского института информатики и автоматизации
Российской академии наук (СПИИРАН)

Диссертация «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами» выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН).

В период подготовки диссертации соискатель Лившиц Илья Иосифович работал в Федеральном государственном бюджетном учреждении науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) в должности старшего научного сотрудника, а также в Университете ИТМО на кафедре «Проблем безопасности компьютерных систем» в должности доцента. В 1995 году окончил факультет технической кибернетики Санкт-Петербургского Государственного Технического Университета по специальности «Робототехнические системы и комплексы».

Научный консультант – доктор технических наук, профессор, главный научный сотрудник лаборатории безопасности информационных систем Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) – Молдовян Александр Андреевич.

По результатам рассмотрения диссертации «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами» принято следующее заключение:

Оценка выполненной соискателем работы

В диссертационной работе Лившица Ильи Иосифовича приведен анализ существующих методов обеспечения информационной безопасности

(ИБ) для сложных промышленных объектов (СлПО). Разработанные соискателем модели (обобщенная модель ИСМ для обеспечения безопасности ИСМ, базовая модель аудита ИСМ) и методы (метод проведения аудита ИСМ для СлПО, метод исследования динамики сертификации по международным стандартам ISO для СлПО, метод многошаговой оптимизации процесса аудита ИБ в ИСМ для СлПО) прошли широкую апробацию при реализации крупных проектов в таких предметных областях как – информационные технологии, воздушный транспорт, системная интеграция, банковское дело, управления коммунальными объектами критической инфраструктуры, образовательная деятельность. Актуальность и востребованность данной тематики подтверждается большим вниманием к вопросам обеспечения ИБ с учетом значительного возрастания деструктивных действий злоумышленников.

Личное участие соискателя в получении результатов, изложенных в диссертации

Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованных работах. Подготовка к публикации полученных результатов проводилась совместно с соавторами, причем вклад диссертанта был значительным. Представленные к защите результаты получены лично автором и непосредственно связаны с его научно-практической деятельностью, в том числе, при выполнении им проектов в области ИБ на территории РФ и стран СНГ.

Достоверность результатов проведенных исследований

Достоверность и обоснованность полученных результатов подтверждается:

- сопоставлением результатов с известными аналогичными исследованиями за длительный период (Reuters, Deloitte, Ernst&Young, McKinsey, PwC);
- сопоставлением с публичными данными национальных («Эшелон», ФСТЭК, Positive Technology) и международных аналитических обзоров сертификации (ISO);
- результатами независимых оценок (аудита) ИСМ в рассматриваемых предметных областях («Русский Регистр», TUV, Lloyd, BSI, DNV);
- широким обсуждением на всероссийских и международных научных и научно-практических конференциях;
- строгостью математических соотношений, использованных для моделей и методов оценки (аудита) ИБ;
- корректностью применения апробированного в научной практике исследовательского и аналитического аппарата;
- доказанным положительным эффектом от ряда внедрений результатов представленного диссертационного исследования;
- публикацией результатов диссертационного исследования в рецензируемых научных изданиях, в т.ч. в **38** изданиях, включенных в список ВАК Российской Федерации и в **15** изданиях, индексируемых Scopus и/или Web of Science.

Научная новизна полученных результатов

Научная новизна представленной диссертационной работы состоит в следующем. 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 в СМИБ как самостоятельной СМ или в составе ИСМ. 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 связанных моделей и методов аудита ИБ, позволяющих формировать оптимальный перечень метрик ИБ и выполнять количественную оценку уровня обеспечения ИБ. Новизна комплекса моделей и методов заключается в формировании функционально завершенной структуры для выполнения аудита ИБ в ИСМ.

Практическая значимость полученных результатов

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 (*compliance*). Представленные методы и модели аудита ИБ для СлПО реализованы как функционально завершенный элемент в системе мероприятий комплекса обеспечения ИБ.

Результаты диссертационного исследования получили практическую реализацию в следующих предметных областях:

1. Информационные технологии. В компании ИТСК (РФ) реализован комплекс новых методов аудита ИБ с учетом иерархической системы критериев модели СМИБ (ИСМ).
2. Воздушный транспорт. В международных аэропортах Алматы и Астаны (Республика Казахстан) реализован комплекс новых моделей и методов аудита ИБ в составе ИСМ в соответствии с требованиями международных стандартов ISO и дополнительных отраслевых требований IATA (ISAGO).
3. Системная интеграция. В группе компаний «Газинформсервис» (РФ) реализован комплекс новых моделей и методов аудита ИБ при создании ИСМ, в том числе, для группы компаний «Газпром нефть».
4. 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.
5. Банковское дело. В Акционерном коммерческом банке «Рускобанк» (РФ) реализован комплекс новых методов проведения аудита ИБ, в том числе, с учетом требований ISO и СТО БР ИББС.
6. Управление коммунальными объектами критической инфраструктуры. В ГУП «Водоканал Санкт-Петербурга» (РФ) реализован комплекс новых методов

проведения аудита ИБ для СМИБ в составе ИСМ с учетом требований, предъявляемых к СлПО.

Специальность, которой соответствует диссертация

Работа соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени доктора технических наук по специальности 05.13.19 — Методы и системы защиты информации, информационная безопасность.

Полнота изложения материалов диссертации в работах, опубликованных соискателем

Основные результаты диссертации изложены в следующих работах в необходимой полноте:

Публикации, включенные в библиографические базы Web of Science и / или Scopus

1. Livshitz I., Neklyudov A., Lontsikh P. Evaluation of IT security – genesis and its state-of-art. IOP Conf. Series: Journal of Physics: Conf. Series 1015 (2018) 042029 **DOI**: 10.1088/1742-6596/1015/4/042029.
2. 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.
3. 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.
4. Livshitz, I.I., Ezrahovich, A.Y., Vladimirtsev, A.V., Lontsikh, P.A., Karaseva, V.A. Risk-based thinking of ISO 9001:2015 - The new methods, approaches and tools of risk management. Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. **DOI:** 10.1109/ITMQIS.2017.8085872.
5. 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.
6. Livshitz, I.I., Nikiforova, K.A., Lontsikh, P.A., Karaseva, V.A. The evaluation of the electronic services with accordance to IT-security requirements based on ISO/IEC 27001. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. **DOI:** 10.1109/ITMQIS.2016.7751921.
7. Livshitz, I.I., Lontsikh, P.A., Karaseva, V.A., Kunakov, E.P., Nikiforova, K.A. Implementation of information security and data processing center protection standards. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. **DOI**: 10.1109/ITMQIS.2016.7751923.
8. Livshitz, I.I., Nikiforova, K.A., Lontsikh, P.A., Drolova, E.Y., Lontsikh, N.P. The optimization of the integrated management system audit program. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. **DOI:** 10.1109/ITMQIS.2016.7751919.

9. Livshitz, I.I., Yurkin, D.V., Minyaev, A.A. Formation of the Instantaneous Information Security Audit Concept. Distributed Computer and Communication Networks, 2016. https://doi.org/10.1007/978-3-319-51917-3_28.
10. Livshitz I., Lontsikh P., Eliseev S. The Method of Implementation of the Numerical IT-Security Metrics in Management Systems. Proceedings of the FRUCT'20 (3-7 April 2017) pp. 242 – 248. ISSN 2305-7254. **DOI:** 10.23919/FRUCT.2017.8071318.
11. 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.
12. Livshitz Ilya, Podolyanets Lada. Models of Complex Industrial Facilities Assessment Based on Risk Approach. International Review of Management and Marketing, 2016, N.6 (S5) pp. 125-135. ISSN: 2146-4405.

Статьи в ведущих научных журналах и изданиях, рекомендованных ВАК Министерства образования и науки РФ:

13. Лившиц И.И. Оценка современных условия обеспечения безопасности сложных промышленных объектов / И.И. Лившиц, А.В. Неклюдов, А.Т. Танатарова // Энергобезопасность и энергосбережение. – 2018. – № 2. – С. 5-14. DOI: 10.18635/2071-2219-2018-2-5-14.
14. Лившиц И.И. Модель интегрированной системы менеджмента для обеспечения безопасности сложных объектов / Лившиц И.И., Фаткиева Р.Р. // Вопросы кибербезопасности. – 2018. – № 1 (25). – С. 64-71. DOI: 10.21681/2311-3456-2018-1-64-71
15. Лившиц И.И. Менеджмент информационной безопасности // Стандарты и качество. – 2017. – № 9. – С. 48-52.
16. Лившиц И.И. Гибридная методика оценки безопасности информационных технологий / И.И. Лившиц, А.В. Неклюдов // Автоматизация в промышленности. – 2017. – № 7. – С.36-41.
17. Лившиц И.И. Анализ существующих ИТ активов для обеспечения информационной безопасности / И.И. Лившиц, А.В. Неклюдов // Вопросы защиты информации. – 2017. – № 1 (116). – С. 46-57.
18. Лившиц И.И. Методика оптимизации программы аудита интегрированных систем менеджмента // Труды СПИИРАН. – 2016. – № 5. – С. 52 – 68. DOI: 10.15622/sp.48.3.
19. Лившиц И.И. Формирование метрик для измерения результативности систем менеджмента информационной безопасности / И.И. Лившиц, П.А. Лонцих // Вестник Иркутского государственного технического университета. – 2016. – № 5. – С. 65 – 72. DOI: 10.21285/1814-3520-2016-5-65-72.
20. Лившиц И.И. Практические аспекты выполнения аудитов ИБ в соответствии с требованиями стандартов СТО БР ИББС // Деньги и кредит. – 2016. –№ 2. – С.54 –58.
21. Лившиц И.И. Оценка методических подходов для формирования систем безопасности сложных промышленных объектов топливно-энергетического комплекса // Вопросы защиты информации. – 2016. – № 1. – С. 56 – 61.
22. 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.
23. Лившиц И.И. Формирование концепции мгновенных аудитов информационной безопасности // Труды СПИИРАН. – 2015. – № 6 (43). – С. 253 – 270. DOI: http://dx.doi.org/10.15622/sp.43.14
24. Лившиц И.И. Оценка защищенности объектов топливно-энергетического комплекса // Энергобезопасность и энергосбережение. – 2015.– № 5. – С. 5 – 10.
25. Лившиц И.И. Определение активов при внедрении и сертификации СМИБ // Стандарты и качество. – 2015. – № 6 (936). – С. 84 – 85.

26. Лившиц И.И. Методика выполнения комплексных аудитов промышленных объектов для обеспечения эффективного внедрения систем энергоменеджмента // Энергобезопасность и энергосбережение. – 2015. – № 3. – С. 10-15.
27. Лившиц И.И. Исследование динамики сертификации по международным стандартам ISO для целей обеспечения комплексной безопасности // Вопросы защиты информации. – 2015. – № 2. – С. 48 – 56.
28. Лившиц И.И. Анализ уязвимостей и угроз национальной платежной системы Российской Федерации // Вопросы защиты информации. – 2015. – № 1. – С. 75 – 80.
29. Лившиц И.И. Методический подход к оценке защищенности информации в телекоммуникационных системах на основе анализа их доступности / И.И. Лившиц, В.В. Маликов // Вестнік Сувязі. – 2015. – № 2. – С. 57-61.
30. 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.
31. Лившиц И.И. Применение модели СМИБ для оценки защищенности интегрированных систем менеджмента // Труды СПИИРАН. – 2013. – № 8 (31). – С. 147 – 162.
32. Лившиц И.И. Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI / ISO // Информатизация и связь. –2013.–№6.– С.62–67.
33. Лившиц И.И. Подходы к решению проблемы учета потерь в интегрированных системах менеджмента // Информатизация и связь. – 2013. – № 1. – С. 57 – 62.
34. Лившиц И.И. Подходы к синтезу модели оценки защищенности персональных данных в соответствии с требованиями стандарта ISO/IEC 27001:2005 // Труды СПИИРАН. – 2012. – № 4 (23). – С. 80 – 92.

Рецензируемые учебные пособия

35. Лившиц И.И. Нормативное обеспечение эксплуатации средств защиты информации: учебное пособие /А.В. Красов, И.И. Лившиц, Д.В. Юркин, А.В. Малых, Ю.О. Изотова; СПбГУТ. – СПб., 2017. – 68 с.
36. Лившиц И.И. Аудит систем менеджмента информационной безопасности для сложных промышленных объектов: учебное пособие / А.В. Красов, И.И. Лившиц, Д.В. Юркин; СПбГУТ. – СПб., 2016. – 75 с.

Диссертация «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами» Лившица Ильи Иосифовича рекомендуется к защите на соискание ученой степени доктора технических наук по специальности 05.13.19 — Методы и системы защиты информации, информационная безопасность.

Заключение принято 6.07.2018 г.
Присутствовало на семинар а» — 11 чел.,
«против» — 0 чел., «воздерж .07.2018 г.

Председатель семинара
главный научный сотрудник
интеллектуальных систем СП
доктор технических наук, пр С. Лебедев
«06» июля 2018 г.