

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

14 линия, 39, Санкт-Петербург, 199178
Телефон: (812) 328-33-11, факс: (812)328-44-50
E-mail: spiiran@iias.spb.su,
http://www.spiiran.nw.ru
ОКПО 04683303, ОГРН 1027800514411
ИНН/КПП 7801003920/780101001

« 15 » Инварь 20 20 г.

ТВЕРЖДАЮ
Информатика и автоматизация

н. профессор РАН
Ронжин А.Л.

« 15 » Инварь 20 20 № 60-01-01-079
На № _____ от _____

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного учреждения науки
Санкт-Петербургский институт информатики и автоматизации
Российской академии наук

Диссертация «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» выполнена в лаборатории технологий больших данных социкиберфизических систем.

В период подготовки диссертации соискатель Левоневский Дмитрий Константинович работал научным сотрудником в лаборатории технологий больших данных социкиберфизических систем Федерального государственного бюджетного учреждения науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук.

В 2014 г. окончил Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет (СПбГЭТУ «ЛЭТИ») по направлению «Информатика и вычислительная техника».

Удостоверение/справка о сдаче кандидатских экзаменов №17/207, выдана в 2017 г. Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии наук.

Научный руководитель – д.т.н., профессор Осипов Василий Юрьевич, основное место работы: заведующий лабораторией информационно-вычислительных систем и технологий программирования Федерального государственного бюджетного учреждения науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук.

По результатам рассмотрения диссертации «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» принято следующее заключение:

В диссертационной работе Левоневского Д.К. решена научная задача разработки новых методов и моделей адаптивной защиты корпоративных информационных систем (КИС) от комплексных деструктивных информационных воздействий, имеющая существенное значение для развития систем информационной безопасности. Разработаны новая математическая модель КИС, функционирующей в условиях комплексных деструктивных информационных воздействий, метод оценивания эффективности функционирования КИС и метод её адаптивной защиты от информационных угроз. Актуальность исследований подтверждается широкой распространённостью КИС, их уязвимостью, динамичностью угроз, существенным потенциальным ущербом при нарушении информационной безопасности, не полным соответствием известных методов требованиям практики.

В работе лично Левоневским Д.К. получены **следующие результаты**: 1) математическая модель корпоративной информационной системы, функционирующей в условиях комплексных деструктивных информационных воздействий, отличающаяся новым пространством состояний и множеством переходов между ними, что позволяет шире исследовать и точнее прогнозировать поведение системы при наличии этих угроз; 2) метод оценивания эффективности функционирования корпоративной информационной системы с использованием предложенной математической модели, отличающийся новым показателем эффективности КИС и правилами его расчета, позволяющий расширить возможности оценивания влияния информационных угроз на работу систем; 3) метод адаптивной защиты корпоративной информационной системы от информационных угроз, отличающийся новой математической формулировкой задачи поиска оптимальной программы защиты и алгоритмом ее решения, позволяющий адаптировать эту защиту от комплексных деструктивных воздействий; 4) архитектура системы адаптивной защиты КИС от комплексных деструктивных информационных воздействий, которая отличается новой совокупностью связанных блоков анализа данных и принятия решений, позволяющая расширить функциональные возможности такой защиты; 5) новые запатентованные способы и средства, отличающиеся новыми последовательностями действий по обоснованию и реализации мероприятий защиты, позволяющие повысить эффективность корпоративных информационных систем. Автор принимал личное участие в постановке цели исследования, формулировке основных задач, разработке методов и научно обоснованных решений по адаптивной

адаптивной защите КИС от деструктивных информационных угроз, подготовке материалов для публикации совместно с соавторами.

Достаточная степень достоверности полученных результатов обеспечивается проведением анализа существующих результатов исследований в предметной области, корректностью исходных предпосылок, соответствием результатов моделирования общим закономерностям, апробацией основных результатов работы на научных конференциях и в научной печати, реализацией результатов работы в проектах.

Новизна и практическая значимость результатов исследования: в результате исследований было получено 5 научных результатов. Результаты выполненных в диссертационной работе исследований позволили усовершенствовать системы информационной защиты КИС и повысить их эффективность. Разработанные методы и модели могут быть использованы в перспективных системах защиты информации в корпоративных информационных системах, в которых предъявляются высокие требования к адаптивности и комплексности используемых методов и систем обеспечения информационной безопасности.

Разработанные в диссертационном исследовании методы и модели использованы при выполнении работ по грантам Российского фонда фундаментальных исследований №16-29-09482 «Прогнозирование информационных сетевых террористических угроз и обоснование мероприятий противодействия им в мегаполисах», Российского научного фонда №16-19-00044 «Принципы распределения задач между сервисными роботами и средствами киберфизического интеллектуального пространства при многомодальном обслуживании пользователей», в проекте «Разработка методов, моделей, алгоритмов и программных средств, основанных на выявлении отклонений в эвристиках трафика сверхвысоких объемов, для обнаружения сетевых атак и защиты от них» по соглашению с Минобрнауки России № 05.607.21.0322.

По результатам выполнения диссертационного исследования получено 3 свидетельства о регистрации программ для ЭВМ и 1 патент на изобретение.

Диссертационная работа соответствует требованиям п. 9-14 Положения о присуждении ученых степеней и п. 3, 6-10, 14 Паспорта специальностей ВАК по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» (технические науки).

Полнота изложения материалов диссертации в работах, опубликованных соискателем. Основные результаты диссертации изложены в необходимой полноте в 18 печатных работах, в том числе 6 статьях в научных журналах из Перечня ВАК, 9 докладах на международных и всероссийских конференциях:

1. Левоневский Д.К., Ватаманюк И.В., Малов Д.А. Обеспечение доступности сервисов корпоративного интеллектуального пространства посредством управления потоком входных данных. Программная инженерия, т. 10, № 1, 2019. С. 20-29. DOI: 10.17587/prin.10.20-29
2. Левоневский Д.К., Ватаманюк И.В., Савельев А.И. Многомодальная информационно-навигационная облачная система МИНОС для корпоративного киберфизического интеллектуального пространства. Программная инженерия. 2017. №3. С. 120 – 128. DOI: 10.17587/prin.8.120-128
3. Осипов В.Ю., Воробьев В.И., Левоневский Д.К. Проблемы защиты от ложной информации в компьютерных сетях. Труды СПИИРАН. 2017. № 53. С. 97-117. DOI: 10.15622/sp.53.5
4. Левоневский Д.К. Игровое обучение как облачный сервис. Программные системы: теория и приложения. 2017. № 8:1(32), С. 209–217. DOI: 10.25209/2079-3316-2017-8-1-209-217}
5. Левоневский Д.К., Ватаманюк И.В., Савельев А.И., Денисов А.В. Корпоративная информационная система обслуживания пользователей как компонент киберфизического интеллектуального пространства. Известия высших учебных заведений. Приборостроение. Т. 59, ноябрь 2016. С. 906-912. DOI: 10.17586/0021-3454-2016-59-11-906-912
6. Фаткиева Р.Р., Левоневский Д.К. Применение бинарных деревьев для агрегации событий систем обнаружения вторжений. / Труды СПИИРАН, 2015, № 3, стр. 110-121. DOI: 10.15622/sp.40.8
7. Левоневский Д.К., Фаткиева Р.Р. Разработка системы обнаружения аномалий сетевого трафика // Научный вестник Новосибирского государственного технического университета. 2014. № 3 (56). С. 108-114.
8. Levonevskiy D., Vatamaniuk I., Saveliev A. Integration of Corporate Electronic Services into a Smart Space Using Temporal Logic of Actions. Proceedings of the 2nd International Conference on Interactive Collaborative Robotics (ICR-2017), Springer, 2017, pp. 134-143. DOI: 10.15622/sp.48.4
9. Novikov F., Fedorchenko L., Vorobiev V., Fatkueva R., Levonevskiy D. Attribute-Based Approach of Defining the Secure Behavior of Automata Objects. Proceedings of the 10th International Conference On Security Of Information And Networks (SIN-2017), Jaipur, India, October 13-15, 2017. DOI: 10.15622/sp.48.4
10. Vorobiev V., Evnevich E., Fatkueva R., Fedorchenko L., Levonevskiy D. Criteria and Indices of Computer Network Protection. 9th International Conference on Security of Information and Networks (SIN 2016), New Jersey, USA, 20-22 July 2016. В сборнике: ACM International Conference Proceeding Series 9. Сер. "Proceedings of the 9th International Conference on Security of Information and Networks, SIN 2016", 2016, pp. 176-177. DOI: 10.1145/2947626.2951956

11. Vatamaniuk I., Levonevskiy D., Saveliev A., Denisov A. Scenarios of Multimodal Information Navigation Services for Users in Cyberphysical Environment. 18th International Conference on Speech and Computer (SPECOM-2016), Budapest, Hungary, August 23-27, 2016, pp. 588-595. DOI: 10.1007/978-3-319-43958-7_71

12. Levonevskiy, D., Fedorchenko, L., Afanasieva, I., Novikov, F. Architecture of the software system for adaptive protection of network infrastructure. ACM International Conference Proceeding Series, 17, 2018.

13. Levonevskiy, D., Vatamaniuk, I., Saveliev, A. Processing models for conflicting user requests in ubiquitous corporate smart spaces. MATEC Web of Conferences, 161, 3006. DOI: 10.1051/mateconf/201816103006

14. Levonevskiy, D., Vatamaniuk, I., Saveliev, A. Providing availability of the smart space services by means of incoming data control methods. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 11097 LNAI, 170-180, 2018. DOI: 10.1007/978-3-319-99582-3_18

15. Novikov F., Fedorchenko L., Vorobiev V., Fatkueva R., Levonevskiy D. Attribute-Based Approach of Defining the Secure Behavior of Automata Objects. Proceedings of the 10th International Conference On Security Of Information And Networks (SIN-2017), Jaipur, India, October 13-15, 2017. DOI: 10.1145/3136825.3136887

16. Vatamaniuk I., Levonevskiy D., Saveliev A., Denisov A. Scenarios of Multimodal Information Navigation Services for Users in Cyberphysical Environment. 18th International Conference on Speech and Computer (SPECOM-2016), Budapest, Hungary, August 23-27, 2016, pp. 588-595. DOI: 10.1007/978-3-319-43958-7_71

17. Александров В.В., Воробьёв В.И., Кулешов С.В., Левоневский Д.К., Марков В.С., Фаткеева Р.Р., Юсупов Р.М. Глава 5. Формирование и развитие информационной инфраструктуры инновационного развития Санкт-Петербурга. Перспективные направления развития науки в Петербурге. / Отв. ред. Ж.И. Алфёров, О.В. Белый, Г.В. Двас, Е.А. Иванова. - СПб.: Изд-во ИП Пермяков С.А., 2015. - 543 с. ISBN 978-5-9631-0333-3.

18. Левоневский Д.К. Архитектура облачной системы распределения контента в киберфизических системах. Научный журнал «Моделирование, оптимизация и информационные технологии». 2019. Т. 7. № 4. DOI: 10.26102/2310-6018/2019.27.4.027

Ценность научных работ соискателя заключается в том, что они раскрывают методологию и результаты решения задач, поставленных с диссертационном исследовании, а также обеспечивают воспроизводимость полученных научных результатов.

Диссертация «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» Левоневского Дмитрия Константиновича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности

05.13.19 «Методы и системы защиты информации, информационная безопасность».

Заключение принято на расширенном семинаре лабораторий информационно-вычислительных систем и технологий программирования и технологий больших данных социокиберфизических систем СПИИРАН.

Присутствовало на заседании 10 чел.

Результаты голосования: «за» - 10 чел., «против» - нет, «воздержалось» - нет, протокол № 5 от «24» декабря 2019 г.

Председатель семинара:
доктор технических наук, профессор,
главный научный сотрудник

Николай Андреевич Молдовян

Секретарь семинара:
программист лаб. ИВСиТП

Ольга Леонидовна Смирнова