На правах рукописи

ЛЕВОНЕВСКИЙ
Дмитрий Константинович

МЕТОДЫ И МОДЕЛИ ЗАЩИТЫ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ КОМПЛЕКСНЫХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург — 2020

Работа выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук

Научный руководитель:
доктор технических наук, профессор,
главный научный сотрудник, руководитель
лаборатории информационно-
вычислительных систем и технологий про-
граммирования СПИИРАН **Осипов Василий Юрьевич**

Официальные оппоненты:
доктор технических наук, доцент,
профессор кафедры информационной без-
опасности ФГАОУ ВО НИУ «Московский
институт электронной техники» **Душкин Александр Викторович**

кандидат технических наук, доцент,
доцент кафедры информационных систем
ФГАОУ ВО Санкт-Петербургский государ-
ственный электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина) **Дубенецкий Владислав Алексеевич**

Ведущая организация:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)

Защита диссертации состоится "02" апреля 2020 г. в __:__ часов на заседании диссертационного совета Д 002.199.01, созданного на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) по адресу: 199178, Санкт-Петербург, 14-а линия В.О., 39, комн. 401. Факс: (812)-328-44-50, тел: (812)-328-34-11.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук по адресу: 199178, Санкт-Петербург, 14-а линия В.О., 39 и на сайте http://www.spiiras.nw.ru/dissovet

Автореферат разослан «____»_____ 20__ года

Ученый секретарь
диссертационного совета Д 002.199.01
кандидат технических наук **Зайцева Александра Алексеевна**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность. Одним из наиболее значимых классов систем, подлежащих защите от деструктивных воздействий, выступают корпоративные информационные системы (КИС). От их успешного функционирования во многом зависит эффективность многих современных предприятий и организаций. Это масштабируемые системы, предназначенные для комплексной автоматизации всех видов хозяйственной деятельности компаний, а также корпораций, требующих единого управления. Такие системы часто основаны на углубленном анализе данных, широком использовании систем информационной поддержки принятия решений, электронном документообороте и делопроизводстве. КИС организуются на основе компьютерных сетей и подвержены сетевым атакам, но также обладают определенной спецификой как объектов защиты от деструктивных информационных воздействий, которые постоянно совершенствуются.

Не являются редкостью масштабные сетевые атаки на информационную инфраструктуру предприятий и государств. Другая цель злоумышленников – облачная инфраструктура. Облачные технологии используются в образовании, науке, банковской сфере. Такие сервисы, как Amazon, GoogleDrive, Dropbox, Яндекс.Диск, не только насчитывают сотни миллионов частных пользователей, но и предлагают корпоративные аккаунты организациям. Несанкционированный доступ злоумышленника к облачным хранилищам позволяет ему получить не только данные о пользователях (включая такую информацию, как реквизиты платёжных карт, пароли от аккаунтов, копии удостоверений личности), но и данные, составляющие коммерческую и даже, возможно, государственную тайну.

Несмотря на предпринимаемые попытки защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий, они не имеют тенденций к снижению. К причинам этого относится появление новых видов угроз, невысокая адаптивность методов и систем защиты к изменяющимся условиям функционирования корпоративных информационных систем. Необходим поиск новых методов и моделей защиты корпоративных информационных систем от таких воздействий.

Степень разработанности темы. Известны работы в области защиты КИС от деструктивных информационных воздействий. Среди них следует выделить исследования Г.В. Бабенко, Н.А. Гайдамакина, П.Н. Девянина, Д.П. Зегжды, П.Д. Зегжды, М. Лангехейнриха, М. Метцгер, Л. Хоффмана, М. Шмита и других ученых. В СПИИРАН существенный вклад в развитие и решение вопросов безопасности информационных систем внесли Р.М. Юсупов, В.И. Воробьёв, И.В. Котенко, А.А. Молдовян, Н.А. Молдовян, В.Ю. Осипов, И.Б. Саенко и другие. Процессы функционирования самих КИС исследовали А.А. Карпов, А.Л. Ронжин, А.В. Смирнов, Б.В. Соколов, А.Л. Тулупьев.

Цель исследования: повышение эффективности защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий за счет разработки методов и моделей адаптивной защиты этих систем от таких воздействий. Для достижения указанной цели в работе сформулированы и решены следующие задачи:

1. Анализ процесса обеспечения информационной безопасности корпоративных интеллектуальных систем от информационных угроз и разработка на его основе математических моделей корпоративной информационной системы как объекта защиты в условиях информационных угроз.

2. Разработка метода оценивания эффективности функционирования корпоративной информационной системы в условиях воздействия информационных угроз.
3. Разработка метода адаптивной защиты корпоративной информационной системы от информационных угроз.
4. Разработка архитектуры программной системы адаптивной защиты корпоративной информационной системы от информационных угроз.
5. Разработка обоснованных рекомендаций по повышению эффективности защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий.

Объект исследования: процесс защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий.

Предмет исследования: научный аппарат обоснования мероприятий защиты КИС от деструктивных информационных воздействий.

Методология и методы исследования. В качестве методической и теоретической основы в данном диссертационном исследовании использовались методы системного и математического анализа, положения теории вероятности и математической статистики, теории информационной безопасности.

При программной реализации разработанных методов и моделей использовались методы объектно-ориентированного программирования в языке Python. Проектирование программного обеспечения осуществлялось в методологии UML.

Научная новизна выполненных исследований заключается в следующем:

1. Разработана новая 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. Разработан 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. Разработан 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. Предложена архитектура системы адаптивной защиты КИС от комплексных деструктивных информационных воздействий, которая отличается новой совокупностью связанных блоков сбора, предобработки и анализа данных и выбора контрмер для защиты от сетевых атак и иных деструктивных воздействий, позволяющая расширить функциональные возможности такой защиты.
5. Разработаны новые запатентованные способы и средства, отличающиеся новыми последовательностями действий по обоснованию и реализации мероприятий защиты, позволяющие повысить эффективность корпоративных информационных систем.

Положения, выносимые на защиту:

1. Метод оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий, основанный на новой

марковской модели анализируемого процесса и алгоритме расчета нового показателя такой эффективности.

2. Метод адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий, ориентированный на новую архитектуру системы такой защиты с оптимизацией ее конфигурации.
3. Научно-обоснованные способы и средства защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий, повышающие эффективность КИС.

Теоретическая значимость полученных результатов состоит в развитии научного аппарата оценивания эффективности и обоснования мероприятий защиты КИС от деструктивных информационных воздействий.

Практическая значимость. 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, при создании решений по обнаружению сетевых атак и защите от них на основе выявления в эвристиках трафика для обеспечения информационной безопасности информационно-телекоммуникационных систем.

Внедрение результатов. Модель корпоративной информационной системы и метод оценивания эффективности её функционирования использованы в составной части опытно-конструкторской работы «Разработка устройства сопряжения инфракрасного анализатора с локальной сетью предприятия» в ООО «ЭКАН» в рамках задач, посвящённых разработке прикладного программного обеспечения.

Результаты диссертационного исследования используются в образовательном процессе факультета БИТ Университета ИТМО по направлениям подготовки бакалавриата 10.03.01, магистратуры 10.04.01 в виде использования материалов исследования для подготовки лекционных и практических занятий по дисциплинам «Основы информационной безопасности», «Теория и методы управления корпоративной информационной безопасностью», «Комплексное обеспечение функциональной безопасности».

Также 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.

Степень достоверности и апробация результатов. Достоверность полученных результатов обеспечивается корректностью исходных предпосылок, соответствием результатов моделирования общим закономерностям, апробацией основных результатов работы на конференциях и в научной печати, реализацией результатов работы в проектах, в том числе 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, проекте № 16-19-00044 по договору с РНФ № 16-19-00044 от 14.01.2016 г. «Принципы распределения задач между сервисными роботами и средствами киберфизического интеллектуального пространства при многомодальном обслуживании пользователей»; в составной части опытно-конструкторской работы «Разработка устройства сопряжения инфракрасного анализатора с локальной сетью предприятия» в ООО «ЭКАН» в рамках задач, посвящённых разработке прикладного программного обеспечения.

Основные результаты работы докладывались, одобрены и опубликованы в материалах следующих конференций: 19th International Conference on Soft Computing and Measurements (SCM’2016), Санкт-Петербург, Россия, 2016; Юбилейная XV Санкт-Петербургская междуна-родная конференция «Региональная информатика (РИ-2016)», Санкт-Петербург, Россия, 2016; 10th International Conference On Security Of Information And Networks (SIN’2017), Джайпур, Индия, 2017; 19th International Conference on Interactive Collaborative Robotics (ICR’2017), Хатфилд, Великобритания, 2017; XIII международная конференция по электромеханике и робототехнике «Завалишинские чтения – 2018», Санкт-Петербург, Россия, 2018; 20th International Conference on Interactive Collaborative Robotics (ICR’2018), Лейпциг, Германия, 2018.

Публикации. Основные результаты диссертации отражены в 18 печатных работах, в том числе 6 статьях в научных журналах из перечня ВАК РФ, 9 докладах на международных и всероссийских конференциях, 3 свидетельствах о регистрации программ, 1 патенте на изобретение.

Личный вклад автора. Все выносимые на защиту научные результаты получены лично автором. Автор принимал личное участие в постановке цели исследования, формулировке основных задач, разработке методов и научно обоснованных решений по адаптивной защите корпоративных информационных систем от деструктивных информационных угроз, подготовке материалов для публикации совместно с соавторами.

Структура и объем диссертации. Диссертация состоит из введения, четырех разделов, заключения, списка использованных источников из 101 наименований. Общий объем работы – 144 страницы, в том числе основной текст – 132 страницы, 15 таблиц, 36 рисунков.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность проводимых исследований, определены цели и задачи исследования, отражена научная новизна и практическая значимость работы, сформулированы результаты, выносимые на защиту.

В первой главе анализируется процесс защиты КИС от комплексных деструктивных информационных воздействий. Уточняются цели, задачи и возможности КИС как объектов защиты. Раскрываются особенности информационных угроз для КИС. Дается анализ известных систем и методов защиты КИС от комплексных деструктивных информационных воздействий. Под комплексными деструктивными угрозами для КИС понимаются те, которые затрагивают сразу несколько компонентов системы и аспектов информационной безопасности. Обосновывается необходимость поиска новых методов и средств повышения эффективности защиты КИС от таких угроз - математических методов, моделей и алгоритмов сбора и предобработки показателей эффективности функционирования системы и сетевого трафика, протекающего в ней,

оценивания данных о функционировании КИС, алгоритмов выбора контрмер для защиты от деструктивных воздействий, технических принципов и методических подходов к организации развертыванию решений по обнаружению деструктивных воздействий и защите от них. Формулируется решаемая научная задача разработки новых методов и моделей адаптивной защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий.

Во второй главе раскрыт предлагаемый новый **метод оценивания** эффективности защиты корпоративных информационных систем от деструктивных информационных воздействий. В интересах его раскрытия приведена формальная постановка задачи и обоснованы показатели эффективности защиты КИС от этих угроз. Разработана новая марковская модель защищаемой корпоративной информационной системы. Предложен алгоритм оценивания эффективности защиты КИС от комплексных деструктивных информационных воздействий по новому интегральному показателю с использованием этой модели. Оценивание эффективности защиты КИС предлагается осуществлять с учетом времени нахождения системы в каждом состоянии и достигаемых прикладных эффектов. Кроме интегрального показателя для оценивания защищенности КИС предложено использовать также приращения показателей реализации сервисов системы: длительностей загрузки и инициализации приложений, актуализации данных в них; долей выполненных заявок и отказов; задержек времени в выполнении пользовательских заданий. В частном случае оценивания эффективности защиты КИС от деструктивных угроз осуществима по приращению взвешенных сумм значений частных показателей КИС без мероприятий защиты и при использовании средств защиты. Кроме этого, эффективность КИС и ее системы защиты может соотноситься с типовыми условиями и состояниями функционирования. Для этих состояний заранее могут определяться достигаемые КИС эффекты.

Для большинства практических случаев процесс функционирования корпоративной информационной системы в условиях комплексных деструктивных информационных воздействий предлагается формализовать в виде графа состояний на рис. 1.

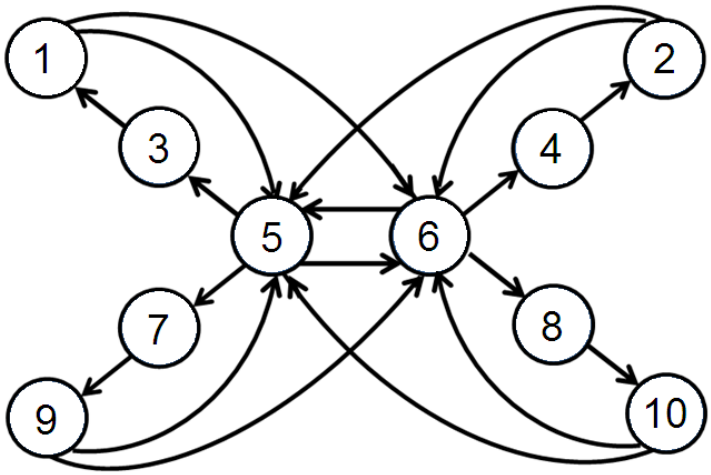

Рис. 1. Модель функционирования защищаемой КИС

Вершины графа обозначают состояния процесса, дуги – переходы из одних состояний в другие. Выделяются 10 состояний (S1-S10) рассматриваемого процесса, которые перечислены в таблице 1. Отличия этих состояний заключаются в условиях, в которых функционирует система в заданный момент времени. Приведённое множе-

ство состояний является полной группой событий. Переходы между состояниями, показанные на рис.1, определяются на основе характера анализируемого процесса.

Переходы S5→S6, S6→S5 могут происходить при усилении или ослаблении активности злоумышленников, реконфигурации системы, изменении её контрагентов, а также при модификации других условий функционирования системы. Изменение этих условий существенно влияет на процессы актуализации и деактуализации угроз.

Таблица 1. Состояния процесса функционирования системы

Номер состояния	Условия функционирования
1	Реализация защитных мер для устранения обнаруженной угрозы
2	Корректная оценка ситуации при отсутствии угрозы
3	Получение истинной информации о наличии угрозы
4	Получение истинной информации об отсутствии угрозы
5	Отсутствие информации об угрозах при наличии угрозы
6	Отсутствие информации об угрозах при отсутствии угрозы
7	Пропуск угрозы при её наличии
8	Ложное распознавание угрозы при её отсутствии (ложная тревога)
9	Восприятие ложной информации как истинной
10	Реализация ошибочных мер защиты при отсутствии угрозы

Принимая во внимание потоковый характер, свойственный процессам функционирования КИС, а также ориентируясь на предельную теорему для суммарных потоков, рассмотренному выше графу соответствует система из 10 линейных дифференциальных уравнений. Каждое из уравнений описывает зависимость вероятностей нахождения системы в соответствующем состоянии S1…S10 от времени и интенсивностей переходов λ_{ij} из одних состояний в другие. Решение конкретной системы уравнений позволяет рассчитывать вероятности, нахождения системы на интересующий момент времени в возможных состояниях при защите от конкретной угрозы с помощью конкретной программы защиты PRG_k. Если интенсивности переходов и начальные условия известны, система дифференциальных уравнений легко решается известными методами численно или аналитически. Распознавание актуального состояния системы для определения начальных условий может выполняться модулем анализа эффектов системы защиты. Кроме того, для каждого типа угроз и программ защиты, модель будет иметь свои начальные значения и параметры. При наличии возможности распознавания актуального состояния системы и известных интенсивностях λ_{ij}, появление угроз может быть предсказано.

Предлагаемый алгоритм оценивания эффективности защиты КИС по новому интегральному показателю с применением разработанной марковской модели включает в себя следующие шаги:

1. Расчет вероятностей $P_z^*(t)$, $P_{zk}(PRG_k, t)$ нахождения КИС в выделенных состояниях без применения мер защиты и с этими мерами на заданный момент времени.

2. Оценивание t_z^* и $t_{zk}(PRG_k)$ суммарного времени нахождения КИС в состояниях $S_z \in \{S_1,...,S_{10}\}$ в случае отсутствия и реализации защитной программы PRG_k:

$$t_z^* = \int_0^T P_z\,(t)dt,\; t_{zk}(PRG_k) = \int_0^T P_{zk}(PRG_k, t)dt,$$

где $P_{zk}(PRG_k, t)$ означает вероятность нахождения системы в состоянии z при реализации защитной программы PRG_k; T – анализируемый период времени.

3. Каждому состоянию z ставится в соответствие величина эффекта V_z, связанная с показателями качества обслуживания, доставляемого пользователю в единицу времени.

4. Рассчитываются совокупные эффекты L^*, $L(PRG_k)$ КИС без мероприятий защиты и с ними:

$$L^* = \sum_{z=1}^{Z} V_z \cdot t_я^*,\; L(PRG_k) = \sum_{z=1}^{Z} V_z \cdot t_{zk}(PRG_k),$$

где Z – число всех состояний КИС. Следует учесть, что значения эффектов V_z могут быть как положительными, так и отрицательными (при наличии ущерба).Учитывая, что показатели качества обслуживания зависят от времени, расчёт совокупного эффекта может выполняться по формулам:

$$L^* = \sum_{z=1}^{Z} L_z^*,\; L(PRG_k) = \sum_{z=1}^{Z} L_z(PRG_k),$$

$$L_z^* = \int_0^T V_z(t)P_z^*(t)dt,\; L_z(PRG_k) = \int_0^T V_z(t)P_{zk}(PRG_k, t)dt$$

5. Расчёт прироста $\Delta L = L_z(PRG_k) - L_z^*$ эффективности КИС за счет реализуемых мероприятий защиты.

Предлагаемый новый метод оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий может быть использован для широкого круга различных по назначению и структурным особенностям КИС.

Третья глава посвящена разработке метода адаптивной защиты корпоративной информационной системы от деструктивных воздействий. Для раскрытия предлагаемого метода рассмотрим модель системы адаптивной защиты КИС от деструктивных воздействий. Структура этой системы приведена на рис. 2. Отличительная черта данной системы состоит в новом множестве функциональных блоков и связей между ними. Она позволяет повысить способность прикладной системы выявлять и устранять деструктивные информационные воздействия в автоматическом режиме.

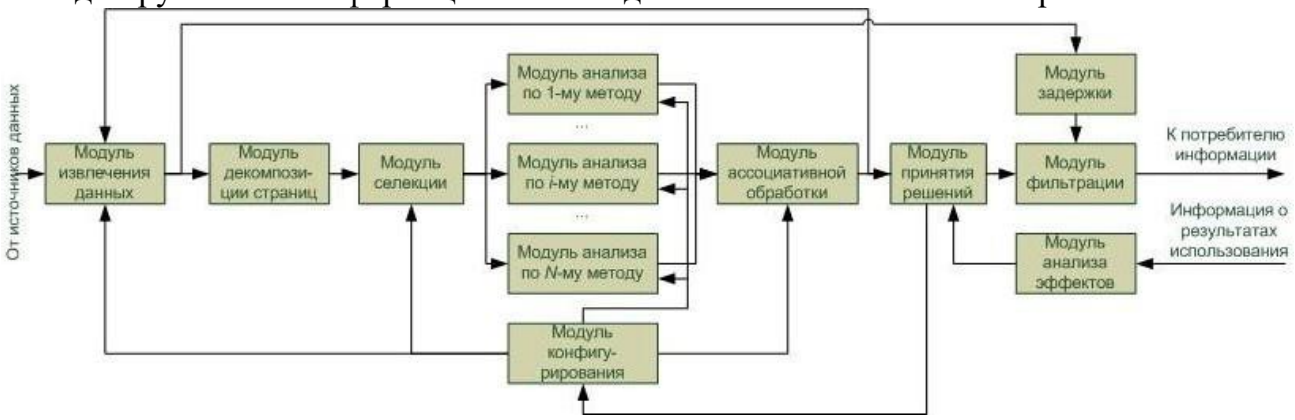

Рис. 2. Структура системы адаптивной защиты

Цель данной системы – обеспечение высокой адаптивности от гетерогенных деструктивных информационных воздействий на компьютерные сети, в частности – сетевых атак. Адаптация системы к актуальным условиям функционирования выпол-

няется с помощью её реконфигурирования. Реконфигурирование подразумевает подстройку блоков системы к текущей ситуации, а также выбор подходящих методов защиты.

В процессе конфигурирования системы защиты определяется состав применяемых методов и систем защиты, а также их параметры. Конфигурирование должно выполняться с учётом как активных, так и возможных угроз, а также состояния защищаемой системы. В общем случае, необходимо решать оптимизационную задачу для нахождения подходящего способа защиты от рассматриваемых угроз. Для этого необходимо обладать моделью процессов в защищаемой системе. В качестве примера может быть рассмотрена модель, описанная в главе 2.

В рамках рассмотренного алгоритма должна осуществляться оптимизация конфигурации системы защиты КИС от деструктивных воздействий. Для оптимизации такой конфигурации предлагается решать следующую математическую задачу. Согласно ей требуется найти оптимальную программу PRG_{opt} для конфигурации системы защиты от выбранных угроз, при реализации которой достигается максимум совокупного эффекта $L_{opt}(PRG_{opt})$ на интервале времени *[0; T]*:

$$L_{opt}(PRG_{opt}) = \max_{k} \sum_{z=1}^{Z} \int_{0}^{T} V_z(t) P_{zk}(PRG_k, t) dt \quad (1)$$

при следующих ограничениях:

$$t_k(PRG_k) \le t_D, \quad (2)$$

$$PRG_k \in R, \quad (3)$$

$$z = \overline{1, Z}, k = \overline{1, K} \quad (4)$$

В формулах (1) - (4) приняты следующие обозначения:

R– конечное множество результативных программ конфигурации системы защиты (под результативной программой понимается такая программа, которая достигает цели за конечное число шагов);

K – количество программ в множестве *R*;

Z – количество состояний в модели защищаемой системы;

$V_z(t)$ – эффект, достигаемый системой в момент времени *t* при условии, что система находится в состоянии *z*;

$P_{zk}(PRG_k, t)$ – вероятность нахождения защищаемой системы в состоянии *z* в момент времени *t* при условии, что программа PRG_k реализована;

T – интервал времени, в течение которого оцениваются совокупные эффекты;

$t_k(PRG_k)$ - время выполнения программы PRG_k ;

t_D - максимально допустимое время выполнения программы.

Эта модель подразумевает, что поиск оптимальной программы PRG_{opt} для конфигурации системы защиты может выполняться только на множестве программ, удовлетворяющих условиям (2) и (3). Учёт этих ограничений существенно сокращает сложность задачи.

В некоторых случаях такая оптимизация может также выполняться с целевой функцией минимизации возможного ущерба на заданном интервале времени.

Согласно (1)-(4), алгоритм решения сформулированной задачи поиска оптимальной программы PRG_{opt} состоит из следующих шагов:

1. Определение начальных данных – значений *T, Z, K,* t_D, множеств $\{V_z(t)\}$, $\{P_{zk}(t=0)\}$, $\{PRG_k\}$, $\{t_k(PRG_k)\}$, $\{\lambda_{ijk}\}$ – интенсивностей перехода в Марковской модели защищаемого процесса после реализации конфигурационной программы PRG_k. Установка начальных значенийпеременных: $k = 0$, $L_{opt} = 0$.
2. $k = k + 1$; $z = 0$; $L_k = 0$.
3. Если $k>K$, перейти к шагу 16.
4. Выбрать k-ю альтернативную программу из множества $\{PRG_k\}$.
5. Проверить условие (3): $PRG_k \in R$. Если условие не выполняется, перейти к шагу 2.
6. Проверить условие (2): $t_k(PRG_k) \le t_D$. Если условие не выполняется, перейти к шагу 2.
7. Выбрать соответствующие программе PRG_k интенсивности переходов $\{\lambda_{ij}\}_k$ из множества $\{\lambda_{ijk}\}$.
8. $z = z + 1$.
9. Если $z>Z$, перейти к шагу 14.
10. Вычислить значения $P_{zk}(PRG_k, t)$ с помощью Марковской модели защищаемого процесса, используя начальные условия $\{P_{zk}(t=0)\}$ и интенсивности переходов $\{\lambda_{ij}\}_k$ для программы PRG_k.
11. Вычислить$L_{kz} = \int_0^T V_z(t) P_{zk}(PRG_k, t)dt$.
12. $L_k = L_k + L_{kz}$
13. Перейти к шагу8.
14. Если $L_{opt}<L_k$, то $L_{opt} = L_k$, $PRG_{opt} = PRG_k$.
15. Перейти к шагу2.
16. Вывести программу PRG_{opt} на исполнение.

В рассмотренном случае, значения $t_k(PRG_k)$ должны быть известны (определены до решения оптимизационной задачи) для заданных программ конфигурации из множества $\{PRG_k\}$.

В более общем случае, альтернативные программы могут не быть предопределены, а могут синтезироваться автоматически [65]. В этом случае значения $t_k(PRG_k)$ должны быть рассчитаны в зависимости от структуры программы и времени выполнения её функций.

Для большого количества альтернативных программ полный поиск может быть заменён известными методами оптимизации, например, методом ветвей и границ, и т. п.

Рассмотренный метод оптимизации конфигурации системы защиты КИС отличается от других известных решений новым набором правил, позволяющих реализовывать адаптивную защиту от информационных угроз. Реконфигурирование системы защиты должно выполняться с целью достижения максимального роста совокупного

эффекта или минимального ущерба в рамках заданного временного интервала с ограничениями на время поиска и реализации управляющей программы.

Применительно к структуре системы защиты, решение оптимизационной задачи (1) - (4) можно реализовать в модуле конфигурирования на рис. 2.

Таким образом, предложенный метод адаптивной защиты корпоративной информационной системы от деструктивных воздействий ориентирован на новую архитектуру системы защиты КИС от деструктивных воздействий. В основе его лежит разработанный алгоритм адаптивной защиты (рис. 3), а также метод оптимизации конфигурации системы такой защиты. Метод позволяет расширить возможности систем защиты по обнаружению и устранению деструктивных воздействий.

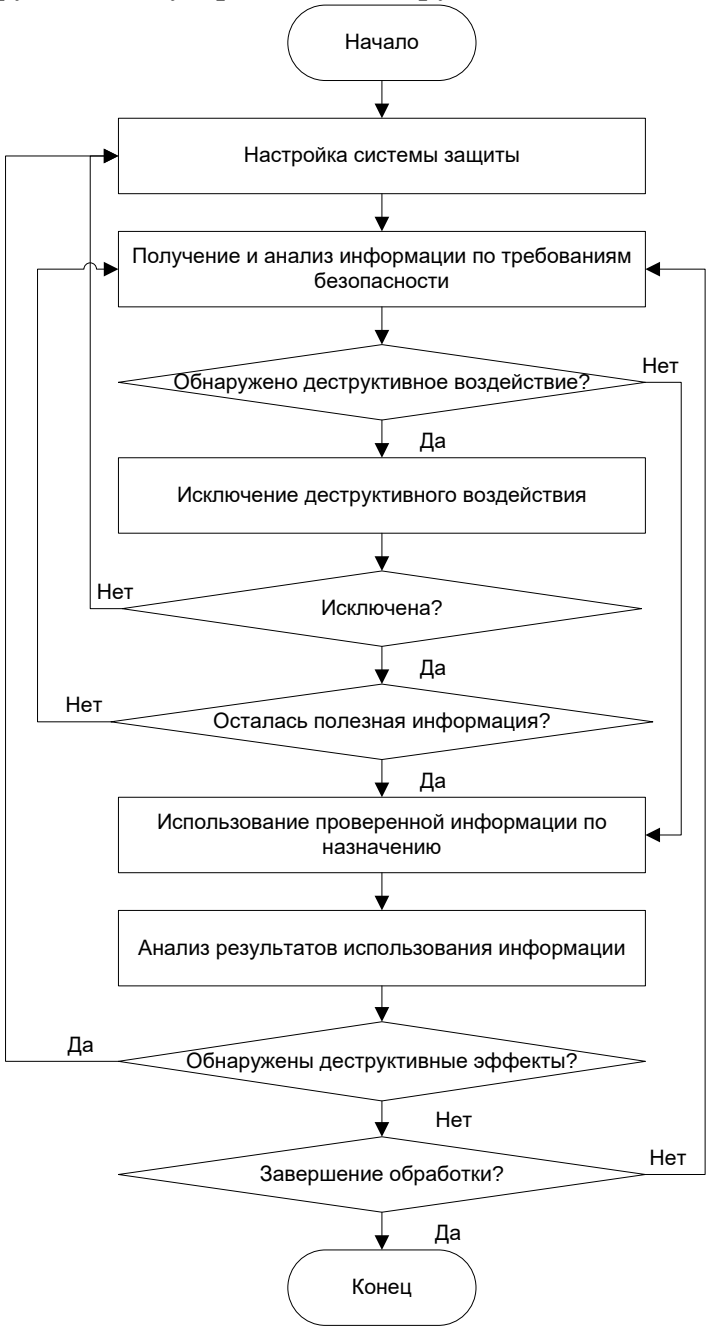

Рис. 3. Алгоритм адаптивной защиты от информационных угроз

В четвертой главе для исследования эффективности предложенных методов и моделей было проведено математическое моделирование на примере сервиса интерактивного корпоративного телевидения.

Для проведения эксперимента была проведена симуляция потоков пользовательских заявок и процесса их обработки. Для этой цели была использована модель массового обслуживания, построенная средствами языка Python (рис. 4).

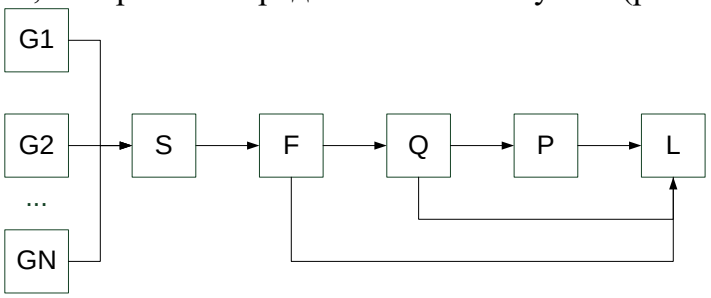

Рис. 4. Модель массового обслуживания

Приведённая модель состоит из следующих блоков: генераторы потоков (G1…GN), диспетчер сессий (S), фильтр (F), контроллер очереди (Q), обработчик запросов (P) и логгер (L).

При низкой интенсивности запросов вероятность конфликта между запросами низка, и значение эффекта близко к 1. При возрастании интенсивности запросов при наличии угрозы и отсутствии фильтрации часть запросов будет отклоняться при реализации управляющей стратегии. В частности, при наличии угроз доступности типа DDoS-атак легитимные запросы могут быть отклонены, а нелегитимные – выполнены, причём из-за большого количества нелегитимных запросов при DDoS-атаке последние будут чаще передаваться на исполнение. Следовательно, значение эффекта будет падать. На рис. 5 представлена зависимость значения эффекта $E = L(0)$ от средней интенсивности возникновения запросов λ_R и потоков λ_S при условии, что потоки легитимны:

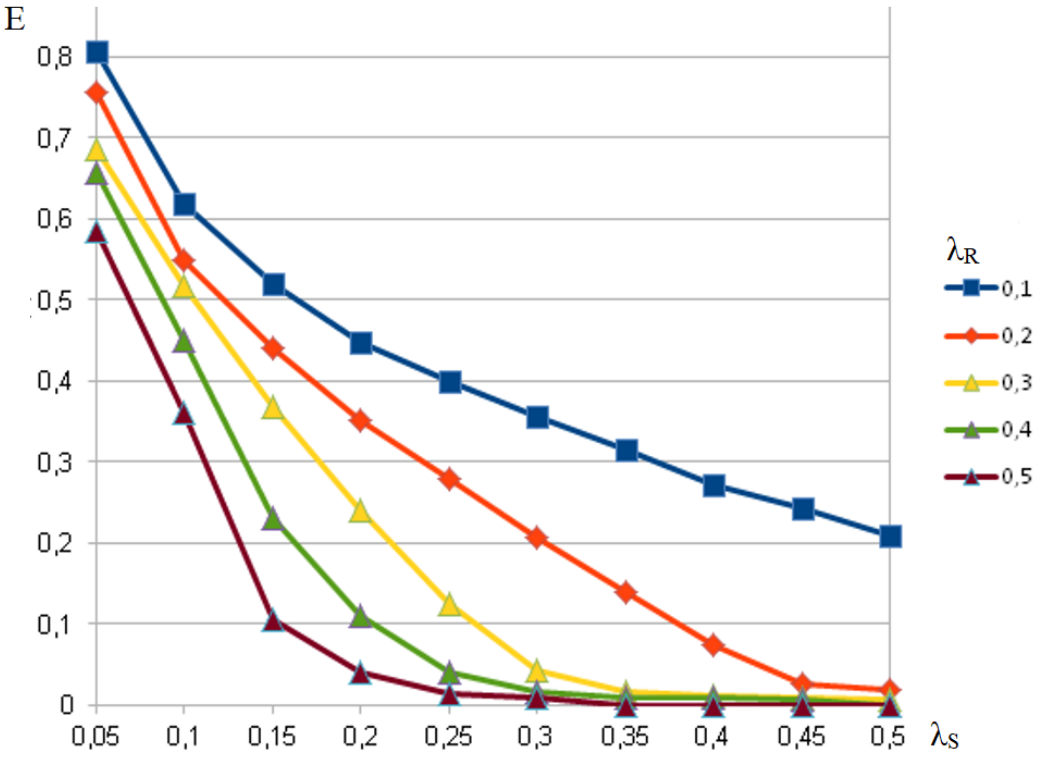

Рис. 5. Зависимость эффекта от λ_R и λ_S

Значение эффекта также значительно снижается при появлении паттернов нелегитимных запросов с интенсивностями λ_M (рис. 6):

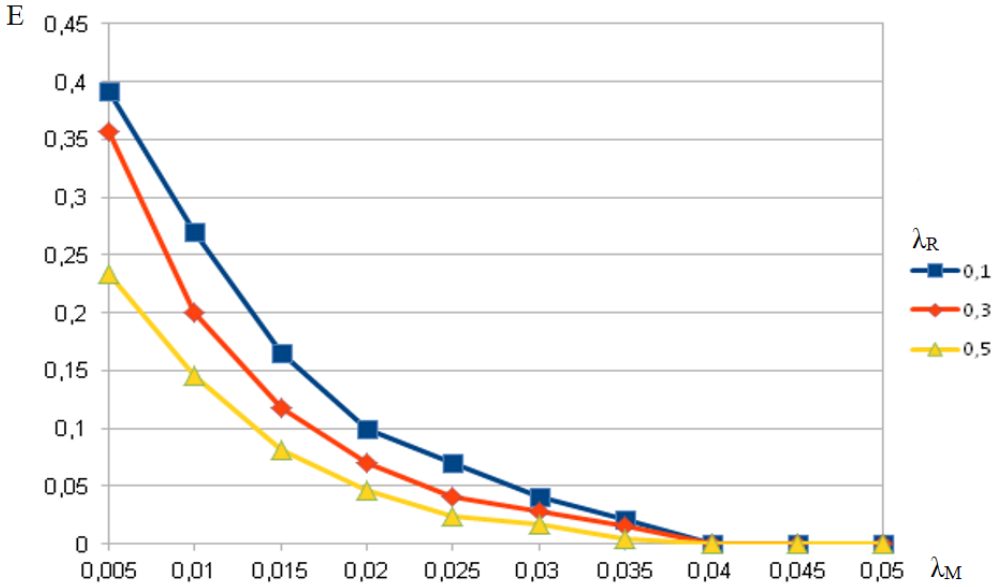

Рис. 6. Зависимость эффекта от λ_R и $\lambda_M(\lambda_S = 0{,}1)$

Фильтрация позволяет частично устранить нелегитимные запросы и увеличить значения эффекта. Было проведено моделирование для оценивания значений эффекта с использованием фильтрации по разным пороговым значениям статистических моментов и энтропии. Рис. 7 иллюстрирует изменение эффекта при изменении порога математического ожидания для частоты появления запросов. Рис. 8 характеризует ту же величину в зависимости от порога среднеквадратического отклонения. Рис. 9 отражает зависимость эффекта от допустимого нижнего порога энтропии.

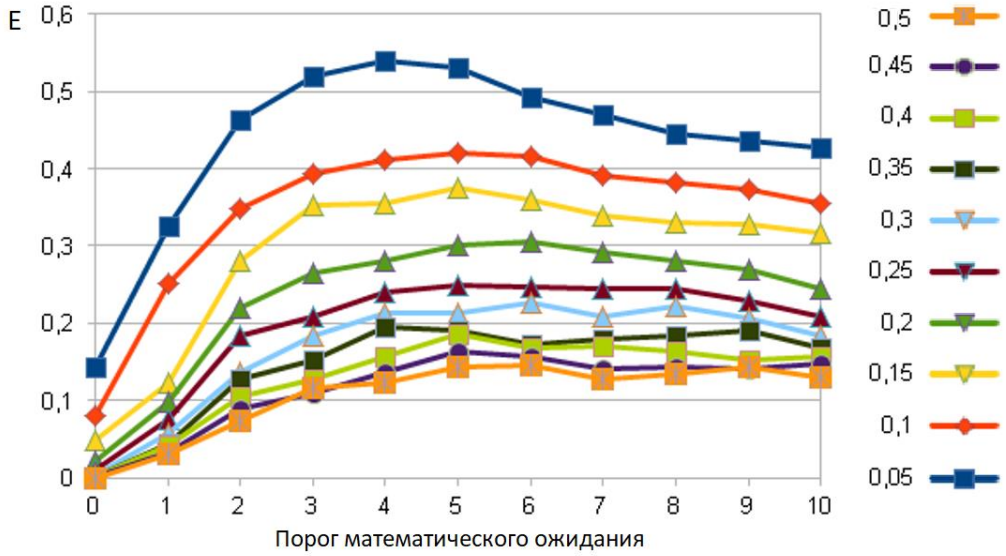

Рис. 7. Зависимость эффекта от интенсивности запросов и допустимого порога среднего значения

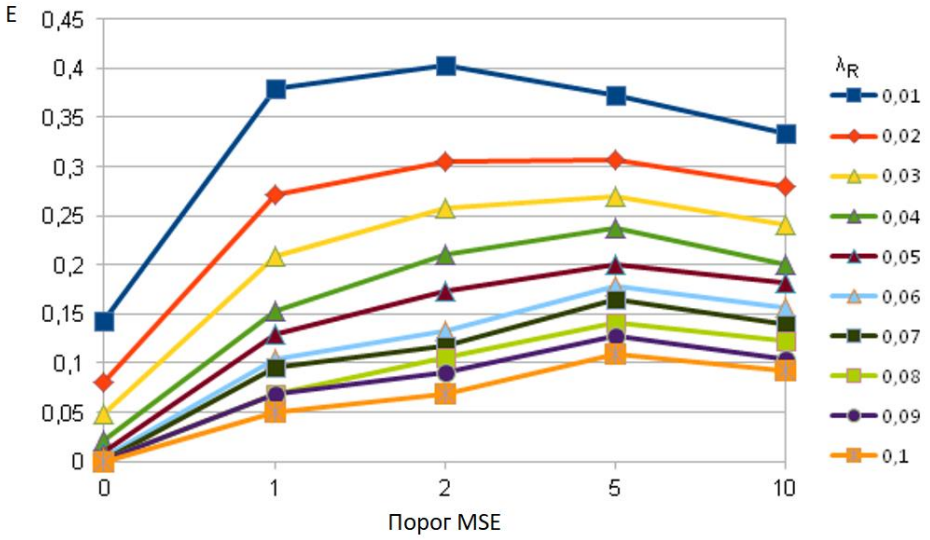

Рис. 8. Зависимость эффекта от интенсивности запросов и допустимого порога среднеквадратического отклонения

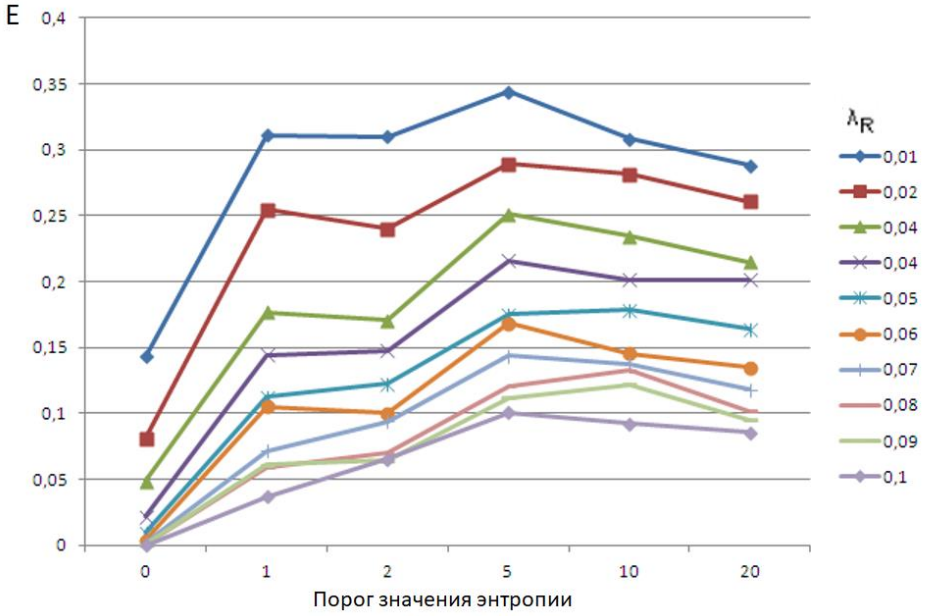

Рис. 9. Зависимость эффекта от интенсивности запросов и допустимого порога энтропии

Эксперимент показывает, что значение эффекта имеет максимумы, которые зависят как от выбранных пороговых значений, так и от условий функционирования (интенсивностей запросов). Изменение условий функционирования системы может быть учтено с помощью адаптивного подхода к управлению методами фильтрации.

Рассмотренные зависимости позволяют оценить плотности эффектов Vz(t) для различных состояний ИБ защищаемой системы. Для изучения поведения системы можно применить модель, предложенную во второй главе.

Рис. 10 показывает зависимости эффекта от времени на примере двух защитных конфигураций. В задаче защиты компьютерной сети от DDoS-атак к первому типу конфигурации относится применение методов, основанных на выявлении сетевых аномалий с помощью сигнатур или статистических моментов невысокого порядка (быстрый анализ входных данных). Ко второму типу относятся методы, основанные на машинном обучении (углублённый анализ входных данных).

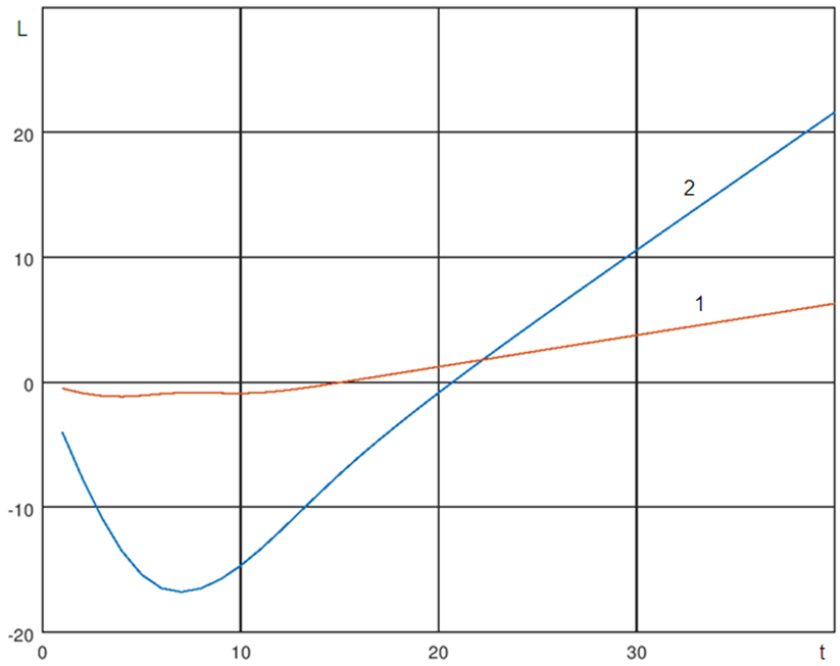

Рис. 10. Величина эффекта при двух защитных конфигурациях: 1 – быстрый анализ входных данных; 2 – углублённый анализ входных данных

Согласно рис.10, реализация метода углублённого анализа входных данных приводит к существенным потерям на начальном этапе моделируемого процесса. Это связано с задержкой при вводе в строй инфраструктуры анализа данных, которая связана с необходимостью развёртывания, конфигурирования и ввода в строй соответствующего программного обеспечения. Таким образом, на начальном этапе система защиты работает неэффективно, но в дальнейшем позволяет достичь более высоких значений эффекта по сравнению с методом быстрого анализа, который не требует существенных временных и трудовых затрат для реализации, но обеспечивает не столь значительный прирост эффекта в будущем.

Приведённые результаты моделирования демонстрируют, что предложенный метод не противоречит известным фактам и закономерностям.

ЗАКЛЮЧЕНИЕ

В результате проведённого исследования успешно решена научная задача разработки новых методов и моделей адаптивной защиты КИС от комплексных деструктивных информационных воздействий, имеющая существенное значение для развития систем информационной безопасности, в том числе получены следующие новые научные результаты:

1. Разработана новая 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. Разработан 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. Разработан 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. Предложена архитектура системы адаптивной защиты КИС от комплексных деструктивных информационных воздействий, которая отличается новой совокупностью связанных блоков сбора, предобработки и анализа данных и выбора контрмер для защиты от сетевых атак и иных деструктивных воздействий, позволяющая расширить функциональные возможности такой защиты.
5. Разработаны новые запатентованные способы и средства, отличающиеся новыми последовательностями действий по обоснованию и реализации мероприятий защиты, позволяющие повысить эффективность корпоративных информационных систем.

Разработанные методы позволяют количественно оценивать процессы, протекающие в защищаемых КИС. Предложенные модели и методы могут быть применены для высокоуровневой формализации процессов функционирования корпоративных информационных систем на производственных предприятиях, в социальных учреждениях, транспортных объектах, моллах, и т. д. Подобные модели и методы могут также успешно применяться в задачах планирования и выбора контрмер для противодействия угрозам в сетях этих организаций. Эта возможность может быть обоснована корректностью исходных предпосылок, соответствием результатов моделирования общим закономерностям, апробацией основных результатов работы на конференциях и в научной печати, реализацией результатов работы в проектах.

Дальнейшие исследования включают построение частных моделей, отражающих процессы, протекающие в сервисах КИС в условиях наличия угроз. Также предполагается развитие методов, позволяющих определять состав мероприятий защиты, в том числе – формализация защитных программ для конкретных условий функционирования КИС, анализ и выбор наиболее эффективных методов оптимизации для поиска защитных программ, обеспечивающих лучшие значения показателей функционирования КИС.

Полученные результаты соответствуют п. 6 «Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования», п. 8 «Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем» и п. 10 «Модели и методы оценивания эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты» паспорта специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК и изданиях, приравненных к ним:

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., 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
5. 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
6. Левоневский Д.К., Фаткиева Р.Р. Разработка системы обнаружения аномалий сетевого трафика. Научный вестник Новосибирского государственного технического университета. 2014. № 3 (56). С. 108-114.
7. Левоневский Д.К. Игровое обучение как облачный сервис. Программные системы: теория и приложения. 2017. №1 (28). С. 209-217.
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. Vorobiev V., Evnevich E., Fatkieva 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
10. 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
11. 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.
12. Levonevskiy, D., Vatamaniuk, I., Saveliev, A. Processing models for conflicting user requests in ubiquitous corporate smart spaces. MATEC Web of Conferences, 161, 3006, 2019. DOI: 10.1051/matecconf/201816103006
13. 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
14. Novikov F., Fedorchenko L., Vorobiev V., Fatkieva 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

15. Levonevskiy D., Afanasieva I., Fedorchenko L., Novikov F. Verification of Internet Protocol Properties Using Cooperating Automaton Objects. Proceedings of the 12th International Conference on Security of Information and Networks (SIN-2019). 2019. С. 1-4. DOI: https://doi.org/10.1145/3357613.3357639

В других изданиях:

1. 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
2. Александров В.В., Воробьёв В.И., Кулешов С.В., Левоневский Д.К., Марков В.С., Фаткиева 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.
3. Ватаманюк И.В., Левоневский Д.К., Малов Д.А., Яковлев Р.Н., Савельев А.И. Модели и способы взаимодействия пользователя с киберфизическим интеллектуальным пространством. СПб: Лань, 2019. – 176 с. ISBN 978-5-8114-3877-8.

Автореферат диссертации

ЛЕВОНЕВСКИЙ
Дмитрий Константинович

МЕТОДЫ И МОДЕЛИ ЗАЩИТЫ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ КОМПЛЕКСНЫХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

Текст автореферата размещен на сайтах:
Высшей аттестационной комиссии Министерства образования
и науки Российской Федерации
https://vak.minobrnauki.gov.ru/
Федерального государственного бюджетного учреждения науки Санкт-
Петербургского института информатики и автоматизации Российской академии наук
(СПИИРАН)
http://www.spiiras.nw.ru/dissovet/

Подписано в печать “31” января 2020 г.
Формат 60x84 1/16. Бумага офсетная. Печать офсетная.
Усл.печ.л. 1,0. Тираж 100 экз.
Заказ №