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

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»

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук, профессор
Осипов В.Ю.

Санкт-Петербург 2020

ОГЛАВЛЕНИЕ

Обозначения и сокращения

КИС	Корпоративная информационная система
КИП	Корпоративное интеллектуальное пространство
UML	Unified Modeling Language
ИБ	Информационная безопасность
ИКТ	Информационно-коммуникационные технологии
СОА	Сервис-ориентированная архитектура
QoS	Quality of Service (качество обслуживания)
QoE	Quality of Experience (качество восприятия)
DoS	Denial of Service (отказ в обслуживании)
DDoS	Distributed Denial of Service (распределённый отказ в обслуживании)

Введение

Актуальность темы диссертации

Одним из наиболее значимых классов информационных систем, подлежащих защите от комплексных деструктивных воздействий, выступают корпоративные информационные системы (КИС) [79]. 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. Они обладают определенной спецификой как объектов защиты от комплексных деструктивных информационных воздействий, которые постоянно совершенствуются.

Не являются редкостью масштабные сетевые атаки на информационную инфраструктуру предприятий и государств. В качестве примера можно привести DDoS-атаку мощностью более 300 Гбит/с, проведённую в 2013 году против организации Spamhaus [58]. Атака затронула CDN Cloudflare и сети провайдеров, которые временно были перегружены. 23 марта 2013 года лондонская точка обмена трафиком в час пик, когда трафик обычно составляет около 1,5 Тбит/с, не справлялась с нагрузкой. Таким образом, атаки подобной мощности могут не только парализовать ресурсы организации, но и создать помехи в глобальной сети или, по крайней мере, на её значительной части. В 2018 году была зафиксирована атака мощностью 1,35 Тбит/с. Мощность атак имеет тенденции к росту. Другая цель злоумышленников – облачная инфраструктура. Облачные технологии используются в образовании, науке, банковской сфере. Такие сервисы, как Amazon, Google Drive, 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. К примеру, сервис iCloud известен инцидентами подобного рода [59].

Несмотря на предпринимаемые попытки защиты корпоративных информационных систем от таких комплексных деструктивных воздействий они не имеют тенденций к снижению. Постоянное расширение функциональности информационных систем и нарастание зависимости от информационной инфраструктуры создаёт ситуацию, когда атаки на эту инфраструктуру могут приводить к последствиям, сравнимым с последствиями террористической активности [57, 62].

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.

В целом анализ текущего состояния защиты КИС от этих угроз показывает, что возможности существующих систем и методов защиты во многом не удовлетворяют требованиям практики. Одним из существенных их недостатков выступает невысокая адаптивность к изменяющимся условиям и видам угроз.

Необходим поиск новых научно-технических решений, позволяющих повысить защищенность КИС от рассматриваемых угроз в быстро меняющихся условиях обстановки. Принципиальной особенностью современных систем является их высокая сложность, которая выражается в гетерогенности компонентов, связей и информации [67]. Эти особенности делают рассматриваемые системы особенно уязвимыми к комплексным деструктивным воздействиям, которые отличаются повышенной эффективностью из-за использования различных программных и аппаратных средств воздействия, типов информации, сценариев атаки. Такие деструктивные воздействия могут быть направлены на ряд компонентов защищаемой информационной системы и создавать угрозу различным аспектам информационной безопасности – целостности (уничтожение, искажение), доступности (перегрузка каналов связи), конфиденциальности [80].

Целью диссертационной работы является 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.

Научная новизна полученных при решении поставленных задач результатов, состоит 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.

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

Практическая ценность результатов в том, что они позволяют совершенствовать 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.

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.

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.

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.

Реализация результатов работы. 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.

Апробация работы. 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 международная 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; 11th International Conference on Security of Information and Networks (SIN’2018), Кардифф, Великобритания, 2018; 20th International Conference on Interactive Collaborative Robotics (ICR’2018), Лейпциг, Германия, 2018.

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

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.

Структура и объем работы. 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.

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 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 оценивание эффективности защиты КИС от деструктивных угроз осуществимо 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 которых достигаемые КИС эффекты могут определяться заранее.

Третья глава посвящена разработке метода адаптивной защиты корпоративной информационной системы от деструктивных воздействий. Для раскрытия предлагаемого метода построена модель системы адаптивной защиты КИС от деструктивных воздействий. 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.

Цель данной системы – обеспечение высокой адаптивности от гетерогенных деструктивных информационных воздействий на компьютерные сети, в частности – сетевых атак. Адаптация системы к актуальным условиям функционирования выполняется с помощью её реконфигурирования. Реконфигурирование подразумевает подстройку блоков системы к текущей ситуации, а также выбор подходящих методов защиты.

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

1. Анализ процесса защиты корпоративных информационных систем от комплексных деструктивных воздействий

1.1. Цели, задачи и возможности защиты корпоративных информационных систем

Известно, что корпоративные информационные системы (КИС) предназначены для комплексной автоматизации всех видов деятельности корпораций (больших и средних предприятий, организаций). От эффективности современных КИС во многом зависит успешность управления этими предприятиями, достигаемые ими экономические, социальные и другие результаты [66]. В тоже время на эффективность самих КИС существенное влияние оказывают проводимые мероприятия по защите их от комплексных деструктивных информационных воздействий (КДВ). При этом с одной стороны защита КИС от таких угроз позволяет снижать возможные риски от нарушения безопасности, а с другой стороны – она может предусматривать существенные расходы на эту безопасность. Желательно, чтобы соблюдался некоторый баланс между уровнем предоставляемой защиты КИС в конкретных условиях и расходами на ее обеспечение. С учетом этого цели и задачи защиты КИС от КДВ в зависимости от сложившихся условий могут существенно различаться. В ряде случаев основными целями защиты КИС могут выступать максимальное снижение возможных рисков, как для самих этих систем, так и обеспечивающих прикладных процессов. В других случаях могут преследоваться цели снижения затрат на саму защиту при обеспечении заданного уровня функционирования КИС и обеспечиваемого предприятия. Достижение этих целей зависит от многих факторов, в том числе от классов защищаемых КИС. Среди КИС различают автоматизированные системы управления предприятием (АСУП), корпоративные интеллектуальные пространства (КИС), киберфизические пространства (КФП). Такие системы

используют современные методы и средства ИКТ – реляционные и NoSQL-базы данных, компьютерную графику, сервис-ориентированную архитектуру (СОА), CASE-технологии. Концепции и средства реализации КИС динамично развиваются и приобретают черты, характерные для систем Industry 4.0 [27-28]. Также ERP реализуются на принципах открытых систем [69].

К примеру, корпоративное интеллектуальное пространство как класс КИС представляет собой сервис-ориентированную инфраструктуру для возможности обеспечения общего доступа к информации различными устройствами [1]. Одной из сфер применения интеллектуальных пространств является развитие информационной инфраструктуры предприятий, позволяющей пользователям (сотрудникам и гостям предприятия) взаимодействовать с этой инфраструктурой и получать доступ к ряду корпоративных сервисов (например, к сервисам корпоративного телевидения, справочной системы, видеоконференцсвязи). Эффективность работы этих сервисов в различных условиях может оцениваться с помощью известных показателей качества обслуживания (Quality of Service, QoS) и качества восприятия (Quality of Experience, QoE) [82].

В литературе [47, 50, 51] предложены объективные и субъективные определения QoE. Объективное QoE определяет качество восприятия, предоставляемое пользователю информационной системы с точки зрения измеримых показателей производительности услуг, сети и приложений. Субъективное QoE определяет качество, воспринимаемое пользователем с позиции получаемых им эмоций, биллинга услуг и соответствия опыта его взаимодействия с системой.

В работах [2, 49] приводится такая оценка для сервиса корпоративного телевидения, в [93] также учитываются условия функционирования такого сервиса в среде «Интернета вещей». Такие характеристики отражают долю выполненных пользовательских задач и степень их выполнения, временные задержки, актуальность выполнения задач и другие подобные величины.

Обеспечение информационной безопасности КИС состоит в обеспечении целостности, доступности и конфиденциальности информации, находящейся в КИС, что позволяет достигать допустимых значений показателей качества обслуживания и восприятия. Для обеспечения конфиденциальности информации используются известные модели разграничения доступа, методы идентификации, аутентификации и авторизации, криптографические методы защиты информации [63]. Контроль целостности строится на основе хэширования и электронно-цифровой подписи, а также резервного копирования [64]. К способам обеспечения доступности информации относят реализацию систем бесперебойного питания, резервирование и распределение мощностей для обеспечения необходимой пропускной способности [3]. Эти способы являются экстенсивными, и их реализация требует увеличения затрат, а в ряде случаев такие способы нереализуемы из-за ограниченной возможности человека воспринимать информацию. Например, когда речь идёт об интерактивном корпоративном телевидении в многопользовательской среде, невозможно удовлетворить одновременные запросы пользователей на получение различной информации без частичной потери доступности.

Процесс взаимодействия пользователей и КИС имеет ряд особенностей, которые необходимо учитывать при их защите от КДВ [9]. Среди них следующие свойства:

1. Повсеместность: система интегрирована в её окружение, и процесс взаимодействия не ограничивается отдельной точкой доступа. Эта особенность позволяет добиться удобного и естественного способа коммуникации [92]. С точки зрения безопасности это означает, что информация поступает в систему через множество распределённых каналов доступа. Эта особенность приводит к увеличению рисков реализации угроз, но она же создаёт дополнительные возможности для анализа поступающей от разных источников информации на достоверность и противоречивость.

2. Сервис-ориентированная архитектура: КИС представляет собой множество слабо связанных, относительно независимых микросервисов, решающих частные задачи [48].

3. Целостность [96]: сервисы работают в едином информационном пространстве, а их деятельность направлена на решение общих задач КИС (обеспечение связи, распространение информации, сбор сведений).

4. Гетерогенность: система включает компоненты, отличающиеся типом аппаратного и программного обеспечения, пропускной способностью, используемыми протоколами, что негативно сказывается на уязвимости системы. В работе [10] отмечается трудность в построении унифицированных моделей для изучения таких систем.

5. Открытость [98]: система динамически включает в себя новые компоненты, такие как мобильные устройства пользователей, которые могут работать с ошибками или быть источником угрозы, что необходимо учитывать при разработке методов обеспечения информационной безопасности.

6. Многомодальность [97]: различные модальности (программные, речевые, жестовые интерфейсы) характеризуются разными вероятностями ошибочного восприятия и возможностями успешной подделки информации, но в многомодальных системах возможно снижать эти вероятности с помощью интегрированных методов обработки информации – например, в работе [11].

7. Большое количество пользователей: различные пользователи могут конкурировать за ресурсы сервисов и создавать противоречивые запросы, поэтому необходимо решать задачу приоретизации заявок, которая учитывает их достоверность и непротиворечивость [53].

8. Распределённость [95]: архитектура системы предполагает пространственную разнесённость компонентов, причём система может достигать масштаба городов [60], а также быть составлена из компонентов, находящихся в разных государствах и на разных континентах.

9. Учёт пространственной и временной привязки [94]: для корректной оценки свойств поступающей информации необходимо оценивать не только её содержание, но и пространственный и временной контекст, который влияет на её достоверность. Информация, как правило, достоверна не сама по себе, а в некотором контексте, включающем пространство, время или другие факторы, которые могут не упоминаться ни в самом информационном объекте, ни в его метаданных. Без учёта этого существует высокий риск получить ложную оценку информации, которая может в свою очередь повлиять на оценку её источника.

В качестве типовых примеров угроз доступности информации в сервисах КИС могут выступать:

1. Целенаправленные деструктивные воздействия на КИС с помощью недостоверной или некорректной информации. В этом случае источником угрозы является пользователь КИС, который может быть как легитимным, так и нелегитимным. Типовым примером реализации такой угрозы является атака «отказ в обслуживании» (DoS), и, в частности, атака распределённого отказа в обслуживании (DDoS), генерируемая сетями заражённых компьютеров (ботнетами) [99].

2. Нецеленаправленные воздействия на КИС в условиях поступления от множества пользователей заявок, которые не могут быть выполнены сервисами КИС в сроки, при которых актуальность заявок сохраняется. В этом случае источником угрозы является легитимный пользователь КИС. Пример реализации угрозы – исчерпание пропускной способности канала передачи данных при возникновении эффекта «flash crowd» [100].

3. Ошибочное восприятие сервисами КИС поступающих заявок. Эта угроза вероятна при использовании многомодальных средств человеко-машинного взаимодействия – при взаимодействии с сервисами с помощью речи, жестов, при распознавании образов на видео. Также угроза может

реализоваться из-за ошибок в клиентском или серверном программном обеспечении. Источник угрозы – программное обеспечение КИП. Обработка сервисами ошибочно воспринятых данных негативно сказывается на доступности сервисов для легитимных пользователей.

Как правило, реализация угроз проявляется в аномалиях сетевого трафика [101].

Аномалии сетевого трафика могут иметь различные причины и быть связаны с деятельностью хакеров, некомпетентных пользователей, неисправностью аппаратуры и дефектами программного обеспечения. Аномалии могут быть видимыми и проявляться непосредственно в некорректной работе информационно-вычислительной системы, а могут не иметь видимых признаков, но привести к сбоям через длительное время. Они могут быть связаны как с атакующими воздействиями, так и с некорректной или недостоверной информацией [72].

Кроме того, необходимо учитывать изменчивость условий функционирования КИС, которая связана с изменением состава пользователей, данных, сервисов, программных и аппаратных компонентов системы, а также изменением множества угроз и их источников. Для учёта этих условий необходимо обеспечить адаптивность средств защиты. Например, авторы [29] описывают биоинспирированный гибридный подход к построению средств защиты информации, адаптивность которых отражена в разделении функций защиты на иммунные, проверяющие форму представления информации, и рецепторные, реализующие взаимодействие со средой и накопление опыта.

Таким образом, для обеспечения оптимального качества обслуживания пользователей в КИС необходимо совершенствование систем и разработка адаптивных методов защиты от КДВ, учитывающих особенности условий функционирования.

1.2. Особенности информационных угроз для корпоративных информационных систем

Для спецификации угроз, актуальных для КИС, необходимо рассмотреть их возможные источники. Источники угроз систематизированы на рис. 1.

Рис. 1. Классификация источников угроз

Угрозы, в свою очередь, классифицируются:

- по источнику;
- по аспекту ИБ (целостность, доступность, конфиденциальность);
- по целевому компоненту системы (АО, СПО, ППО).

Таким образом, угрозы можно свести в таблицу 1.

Таблица 1. Угрозы КИС

Источник	**Аспект**	**Цель**	**Угрозы**	**События риска**
Оператор	Целостность	СПО	Ошибочные действия в административном интерфейсе	Утрата данных

Источник	Аспект	Цель	Угрозы	События риска
Гость	Доступность	СПО	Неисполняемые запросы	Недоступность управления КТ для других пользователей
Нелегитимный пользователь	Целостность	ППО	Инъекция (SQL)	Утрата или модификация данных
	Доступность	ППО	Инъекция (XSS)	Недоступность административного интерфейса
	Доступность	АО, СПО, ППО (в зависимости от типа (D)DoS)	DoS, DDoS	Недоступность интерфейсов для загрузки данных
	Конфиденциальность	ППО	Эксплуатация уязвимостей в аутентификации (недостаточная аутентификация, индексирование директорий, и т.п.)	Кража идентификационных данных
Системное ПО	Доступность	ППО	Отказ	Невозможность работы сервиса
ПО сервиса	Доступность	ППО	Дефект	Некорректная работа сервиса
Нелегитимное ПО	Доступность	ППО, СПО, АО	Исчерпание программных или аппаратных ресурсов	Недоступность интерфейсов или сервиса в целом
	Целостность	ППО, СПО, АО	Несанкциони-рованный доступ	Утрата данных
	Конфиденциальность	ППО	Несанкциони-рованный доступ	Кража идентификационных данных
	Доступность, целостность, конфиденциальность	ППО	Организация каналов обмена информацией	Утрата, кража данных
АО	Доступность, целостность	ППО	Сбой электропитания	Невозможность работы сервиса, утрата данных
Сетевое АО	Доступность	ППО	Отказ	Недоступность интерфейсов
	Конфиденциальность	ППО	Перехват трафика	Кража идентификационных данных
АО хранения данных	Доступность	ППО	Отказ	Невозможность работы сервиса
	Целостность	ППО	Отказ	Утрата данных
АО обработки данных	Доступность	ППО	Отказ	Невозможность работы сервиса

Следует отметить, что в значительном количестве случаев угрозы затрагивают сразу несколько компонентов системы и аспектов

информационной безопасности. Такие угрозы назовём комплексными. При защите следует приоритетно рассматривать именно такие угрозы, так как они получают всё большее распространение в связи с ростом сложности защищаемых систем и являются более общим классом по отношению к частным угрозам.

1.3. Известные системы защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий

В целом существует значительное количество систем, позволяющих выполнять оценку свойств поступающей информации [12-15]. Для анализа таких систем используем критерии:

- архитектурные:
  - расширяемость;
  - наличие открытого кода;
  - наличие зависимости от других систем.
- функциональные:
  - тип обрабатываемой информации;
  - тип обнаруживаемых угроз;
  - работа с распределёнными системами;
  - используемые методы;
  - возможности учёта контекста.

К системам, выполняющим обнаружение аномалий во входящем потоке информации, относятся Snort.AD и Cerberus. Рассмотрим эти системы подробнее.

На рис. 2 приведена структура системы Snort.AD [12]:

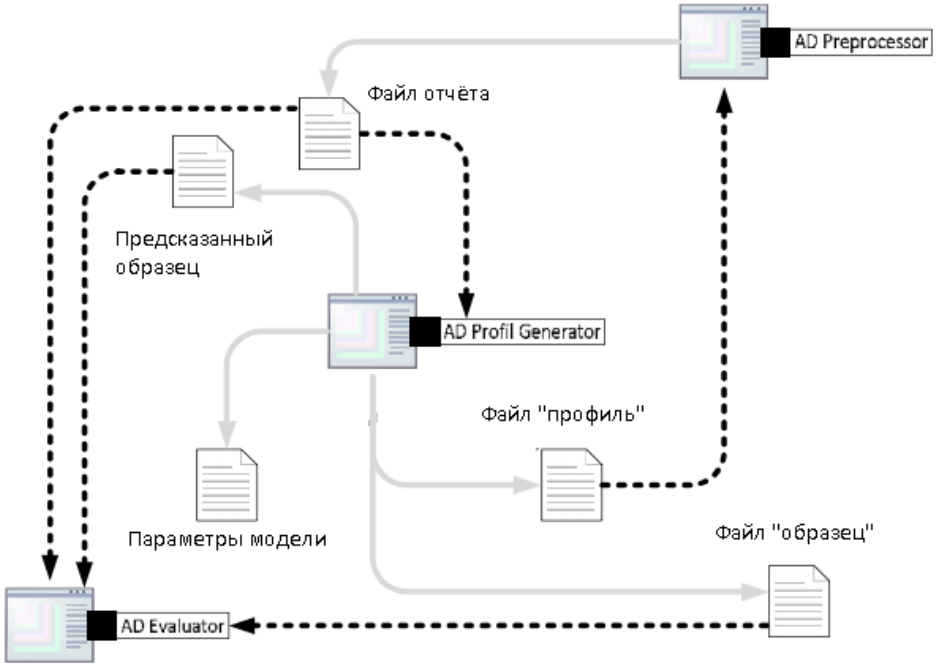


Рис. 2. Схема системы Snort.AD

(Серая стрелка означает, что модуль записывает данные в файл, пунктирная – что модуль читает из файла)

Система состоит из препроцессора (AD Preprocessor – сбор данных о трафике и выдача предупреждений), генератора профилей (AD Profile Generator – прогнозирование трафика) и модуля оценки профиля (AD Evaluator – сравнение предсказанных данных с реальными). Препроцессор читает образец (предсказанные величины трафика) из файла «профиль» и генерирует тревогу, если текущее значение выходит за рамки допустимого (т. е. не лежит в пределах от минимума до максимума). Выполняется сбор следующих данных: число TCP-, UDP-, ICMP-пакетов (как общее число, так и число входящих и исходящих), число этих же пакетов из своей подсети, количество TCP-пакетов с флагами SYN/ACK, количество входящих и исходящих WWW-пакетов (под ними подразумеваются TCP-пакеты на стандартный порт 80), число входящих/исходящих DNS-пакетов (UDP на 53), количество ARP-запросов и ответов, количество не-TCP/IP пакетов, скорости трафика по всем этим составляющим трафика.

Основными ограничениями Snort.AD является то, что он не учитывает значимые компоненты контекста информации (пространство, идентификатор пользователя), а также анализирует исключительно сигнальную информацию в формате временных рядов и только информацию о сетевом трафике. Если вторая проблема может быть устранена с помощью разработки дополнительных модулей сбора и анализа информации, то первая порождает архитектурные проблемы в области интеграции данных с разных узлов КИП.

Система Cerberus [13], напротив, оптимизирован для распределённых систем и позволяет максимально учитывать контекст поступающей информации. Например, оценка достоверности аутентификации пользователя может быть разной в зависимости от контекста. Однако в Cerberus рассматривается только аутентификационная информация. Кроме того, Cerberus может разрешать или запрещать доступ к ресурсам в зависимости от статуса аутентификации, но не учитывает возможность конфликтов доступа.

Фреймворк ConSec [14] также рассматривает контекст в КИП, но защищает только коммуникационный процесс между компонентами системы.

В работе [15] рассматриваются вопросы защиты интеллектуальных пространств на базе платформы Smart-M3, но рассматривается только аспект аутентификации и предоставления доступа к данным.

Сведём рассмотренные системы в таблицу 2. В целом анализ существующих систем и фреймворков показывает, что целью их разработки является защита конфиденциальности и обеспечение высокой точности при аутентификации пользователей. При этом вопросы обеспечения доступности при большом количестве пользователей, которые легитимны, но пользуются разной степенью доверия, рассматриваются только в Snort в контексте противодействия DDoS атакам. Однако Snort имеет очень ограниченные возможности учёта контекста и работы в многопользовательских системах.

Таблица 2. Системы обеспечения ИБ КИС

Критерии	Системы			
	Snort.AD	Cerberus	ConSec	Semantic security framework
Функциональные:				
тип информации	только временные ряды	аутентификационные данные и контекст	аутентификационные данные и контекст	аутентификационные данные и контекст
методы обработки	математическая статистика	логический вывод	?	онтологии, логический вывод
тип угроз	DoS, DDoS	НСД	НСД	НСД
распределённость	нет	да	да	да
контекст	не полностью	да	да	да
Архитектурные:				
открытый код	да	?		
расширяемость	да	?		
зависимости	нет	Gaia [71]		Smart-M3

Таким образом, систем и фреймворков, полностью соответствующих требованиям, не разработано. Тем не менее, значительное количество методов, используемых в этих системах и опубликованных в научной литературе, применимы для решения поставленных задач. Ряд таких методов рассматривается далее.

1.4. Известные методы защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий

Вследствие наличия в КИС гетерогенных программных и аппаратных компонентов, многомодальных интерфейсов поступающая от пользователей информация разнородна. Методы анализа свойств этой информации различаются, и их применение зависит прежде всего от типа информации. Тип информации в значительной мере определяется не ей самой, а способом её восприятия. Следовательно, одна и та же информация может относиться к разным типам. В КИП используются следующие типы информации:

- сигнальная – информация представляется как одиночная команда от одного компонента к другому;
- структурная – информация представлена как множество организованных элементов (например, в виде JSON- или XML-структур);
- текстовая – информация как последовательность текстовых символов;
- медиа – информация представляет собой аудио, видео или изображение;
- комбинированная – информация содержит несколько логически связанных компонентов, возможно разного типа.

Известные методы [16-28, 30-41, 73-75, 78] можно рассмотреть в виде классификации, приведённой на рис. 3.

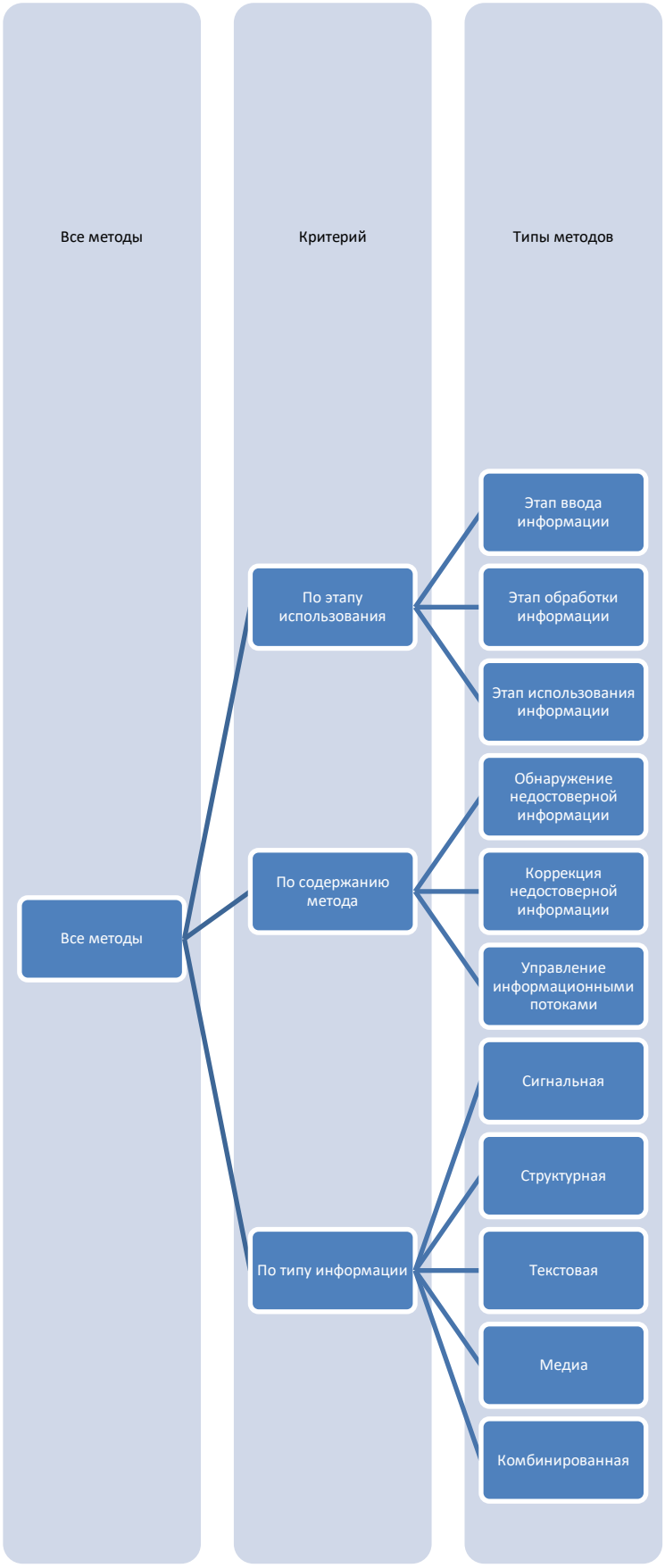


Рис. 3. Классификация методов анализа информации

Рассмотрим подробнее методы обработки информации для обеспечения информационной безопасности КИП в зависимости от типа поступающей информации.

Некоторые методы обработки сигнальной информации приведены в таблице 3.

Таблица 3. Методы анализа сигнальной информации

Метод	**Вычислительная сложность**	**Другие особенности**	**Используемые метрики**
На основе распределений			
пороговый анализ [16]	низкая	необходимость обоснования выбора значений порога	Количество пакетов или байт
вычисление коэффициентов расстояния и подобия между распределениями [17]	высокая; применяются параллельные вычисления	рассматривается отличие атак от массового легального трафика	Количество пакетов с общим свойством (например, адрес источника, размер)
модель гауссовских смесей [18]	высокая	выполняется расчёт распределения трафика и разложение его на гауссовские компоненты; нераскладывающийся трафик считается недостоверным	Отношение входящего трафика к исходящему
модель на базе Simple Network Management Protocol [19]	низкая	Метод позволяет учитывать сессии и потоки. Отмечается, что учёт потоков ведётся роутерами, что сильно облегчает сбор данных.	Отношение SYN/FIN; i/o отношения для UDP и ICMP
Модели на основе частотности протоколов и флагов [74, 78]	низкая		Частотности флагов и протоколов, их соотношения
На основе энтропии			
вычисление разности энтропий [20]	высокая; обработка данных должна быть распределённая и многопоточная	необходимо обоснование выбора порогов	Вероятности пакетов с заданным адресом источника, назначения или размером
вычисление разности энтропий	средняя, осложняется	выполняется анализ отдельных сессий;	Скорость исполнения

Метод	Вычислительная сложность	Другие особенности	Используемые метрики
[21]	необходимостью сортировать пакеты по сессиям	используется шаблон; необходимо обоснование выбора порогов	запроса, время просмотра страницы (для каждой сессии)
энтропия рассчитывается для пакетов, которые имеют отношение к TCP-рукопожатию (SYN, ACK, RST) [22]	простая		Количество TCP пакетов с флагами SYN, ACK, RST, FIN для каждой сессии
На основе машинного обучения			
метод опорных (поворотных) точек [23]	высокая	выполняется многоуровневое извлечение параметров трафика	Частота пакетов, скорость данных, частоты флагов SYN, FIN, RST
расчёт частот различных флагов, допустимые границы частот определяются методом машинного обучения [24]	простая при условии, что выполнено обучение	используются FIN, ACK и SYN флаги во входящих и исходящих пакетах; рассматривается возможность изучения всех остальных флагов	Отношение частот флагов FIN и SYN; частот SYN и ACK
На основе вейвлет-анализа			
Обнаружение вторжений на основе вейвлет-анализа сетевого трафика [25, 26]	средняя		Скорость передачи данных (в байтах и пакетах), уровень загрузки процессора
На основе нечёткой логики			
Модель обнаружения DDoS-атак [73, 75]	средняя		Частоты протоколов и TCP-флагов

Можно видеть, что эти методы ориентированы на обработку сетевого трафика, но при этом многие из них используют закономерности, характерные для потоков событий. Поэтому методы, не привязанные жёстко к структуре сетевых протоколов, можно адаптировать для фильтрации сигнальной информации. Таким образом, методы [16-18, 20-21, 25, 81] могут быть использованы для анализа сигнальной информации.

В последние годы разработано также достаточно много методов анализа достоверности мультимедиа-информации. Такая информация поступает в КИП через многомодальные интерфейсы и камеры и может применяться злоумышленником для введения системы в заблуждение. Кроме того, такая информация подвержена помехам, так как требует более существенных сетевых и вычислительных ресурсов для передачи и обработки по сравнению с сигнальной информацией. Рассмотрим известные методы более подробно.

В работе [5] рассматривается метод обнаружения приёмов копирования и вставки в изображениях. Этот метод основан на артефактах, возникающих в вейвлет-разложении изображения при нарушении его целостности. Метод позволяет выявить факт вмешательства, а также устанавливать модифицированные области. Известные методы пассивного выявления модифицированных видеозаписей рассмотрены в обзорной статье [6]. Авторы анализируют методы, основанные на обнаружении таких признаков, как многократная компрессия видеопотока, выявление модифицированных областей и обнаружение межкадровой подделки (inter-frame forgery). Например, к последнему классу относится метод [7], в котором в качестве признаков вмешательства выступают значения ошибок квантования.

Так как формально видеозапись состоит из изображений (кадров) и аудиопотока, то в ряде случаев задачу анализа видео можно свести к двум отдельным задачам. Однако такой подход не учитывает динамику видеозаписи – связей движущихся образов между собой и со звуковым потоком, которые могут предоставлять дополнительную информацию. С учетом этого, в [30] для повышения точности распознавания образов применяется анализ последовательных серий кадров. В работе [11] предложен способ машинного обучения, позволяющий распознавать выражения лица. В этом способе обрабатываются одновременно аудио-, и видеопотоки. Более того, глубокое обучение позволяет выявлять эмоции

человека по его лицу, свойственные ложным высказываниям, страху, радости, гневу [31].

В большей части работ, посвящённых анализу достоверности текстовой информации, используются:

– фактологический метод, основанный на семантическом анализе контента, извлечении из него элементарных фактов и сопоставлением их с эталонными образцами (проверка на противоречивость);

– стилистический анализ и методы, ориентированные не на выявление фактов, а на анализ формы их выражения, позволяющий делать выводы об объективности, достоверности и компетентности представления информации;

– подход, основанный на анализе метаданных, позволяющий привлекать дополнительную информацию о контенте (его происхождение, связь с другими образцами, форму представления).

К фактологическому подходу можно отнести работу [32]. В ней предложена оценка достоверности веб-ресурсов на основе проверки корректности фактов, содержащихся в ресурсе. Факты автоматически извлекаются из ресурса методами, используемыми для создания баз знаний. Установление ложности фактов на веб-ресурсах предусматривается с помощью совместного логического вывода и многоуровневой вероятностной модели. Источники, содержащие меньшее количество ложных фактов, признаются заслуживающими доверия.

В работе [33] рассмотрен вопрос использования контекстно-зависимых рекомендующих систем для анализа документов на основе сходства. Особенностью предложенного подхода является применение гибридного метода фильтрации и метрик сходства, определяющих взаимоотношения в парах документов. Это позволило учесть как содержательный аспект документов, так и особенности стороны, выполняющей запрос. Использован аппарат онтологического моделирования, позволяющий выявлять

противоречия в документах и на их основе обнаруживать недостоверную информацию.

В [34] изучаются эвристические принципы, используемые человеком для определения достоверности информации, получаемой из сети. Авторы рассматривают факторы репутации ресурса, его поддержки другими пользователями, согласованности с другими ресурсами, а также субъективные аспекты, связанные с априорной информацией. Эти факторы влияют на восприятие ресурса человеком, но позволяют только косвенно судить о достоверности ресурса.

В [35] рассмотрены вопросы доверия к текстовой информации. Особенностью этой работы является то, что выделяются факторы, влияющие на восприятие человеком информации как достоверной.

В статье [36] рассматриваются тематика ресурса, дизайн и технологии, язык и стиль и другие факторы, которые могут учитываться в автоматизированной системе оценки достоверности ресурса.

В работах [37-39] раскрыты методы решения задач поиска текстов по запросу, вопросно-ответного поиска, классификации, кластеризации текстов, выявления заимствований и похожих по смыслу текстов. Эти методы учитывают, помимо лексем, семантические значения текстов. Они также могут быть применены для выявления в компьютерных сетях недостоверной информации.

В [40] обсуждаются подходы к обработке естественного языка, основанные на машинном обучении. Большинство методов предусматривают распределение документов по классам на основе признаков этих документов. Одним из широко практикуемых способов классификации является классификация сообщений на позитивные, негативные и нейтральные по тону, а также определение эмоций (печаль, ненависть, позор), тематики и направленности сообщений.

Анализ метаданных и сопутствующего контента ресурса основан на применении приведённых выше методов и позволяет уточнить оценки. В

качестве входных данных используются мета-теги документа: заголовок, ключевые слова и описание (исследуется соответствие содержанию и наличие маркеров), доменное имя и хостинг (учитывается уровень домена и репутация хостинга), характер и объём рекламных блоков, дата публикации [41]. Подобные подходы эффективны для анализа структурной или частично структурированной информации, представленной в таких форматах, как XML, JSON, HTML и т.п.

1.5. Выводы

Анализ процесса защиты корпоративных информационных систем от комплексных деструктивных воздействий показал, что возможности такой защиты не в полной мере удовлетворяют потребностям практики. Идет непрерывное совершенствование злоумышленниками комплексных деструктивных информационных воздействий на КИС. Это существенно сказывается на их эффективности и прикладных процессов. Известные методы и системы защиты КИС в некоторой мере отстают от развития таких угроз. Одним из существенных недостатков известных методов и систем защиты выступает их невысокая адаптивность к быстро меняющимся условиям обстановки. В большом ряде случаев управляющие решения по противодействию угрозам не оптимальны и существенно запаздывают по времени. В интересах повышения эффективности защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий необходимо сформулировать и решить научную задачу, которая предусматривает разработку новых методов и моделей адаптивной защиты КИС от комплексных деструктивных информационных воздействий.

2. Метод оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий

2.1. Формальная постановка задачи разработки средств защиты корпоративных информационных систем от комплексных деструктивных воздействий

Анализ целей, задач и возможностей обеспечения информационной безопасности корпоративных информационных систем в условиях комплексных деструктивных информационных воздействий показал, что существующие системы защиты КИС во многом не удовлетворяют потребностям практики. В частности, не учитываются быстро меняющиеся условия обеспечения такой защиты. Появляются новые более изощренные комплексные деструктивные воздействия на КИС, учитывающие специфику применяемых методов и средств защиты. Известные системы обеспечения информационной безопасности КИС и лежащие в их основе методы обладают не высокой адаптивностью к изменяющимся условиям обстановки. Все это отрицательным образом сказывается на эффективности защищаемых КИС.

В связи с вышеуказанными проблемами имеет место актуальная научная задача разработки новых методов и моделей адаптивной защиты КИС от комплексных деструктивных информационных воздействий.

В интересах разработки таких методов и моделей, направленных на повышение эффективности информационной защиты КИС в работе предусматривается:

1. Разработка метода оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий.

2. Разработка метода адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий.

3. Обоснование рекомендаций по повышению эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий.

В интересах разработки метода оценивания эффективности исследуемой защиты КИС исследованы показатели, модели и алгоритмы их расчета.

При разработке метода адаптивной защиты КИС раскрыта архитектура перспективной адаптивной системы и лежащие в ее основе алгоритмы и оптимизационные решения.

Рассмотрение вопросов моделирования с применением этих методов ориентировано на обоснование рекомендаций по повышению эффективности КИС в условиях комплексных деструктивных информационных воздействий [46].

С формальной точки зрения решаемая научная задача сводится к поиску оптимальной программы PRG_k мероприятий защиты от комплексных деструктивных воздействий, при котором достигается максимум эффективности защиты $L_{opt}(PRG_{opt})$ на интервале времени *[0; T]* при ограничениях на временные и технические условия реализации данного комплекса:

$$L_{opt}(PRG_{opt}) = \max_{k} \int_{0}^{T} L(PRG_k, t)dt$$

Ограничения:

$$t_k(PRG_k) \le t_D$$

$$PRG_k \in R$$

$$k = \overline{1, K}$$

Здесь:

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

K – количество формируетмых альтернативных программ в множестве R;

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.

Предлагаемый в данной главе метод оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий основан на использовании показателей эффективности и защищённости системы (п. 2.2) и включает модели её функционирования в пространстве угроз (пп. 2.3 и 2.4) и алгоритм оценивания эффективности защиты (п. 2.5). Рассмотрим эти компоненты подробнее.

2.2. Показатели эффективности защиты КИС от КДВ

Для поиска обоснованных способов и средств защиты корпоративных информационных систем (КИС) от комплексных деструктивных информационных воздействий (КДВ) необходимо наличие соответствующих методов оценивания эффективности такой защиты.

Исходя из общих положений по оценке защищенности подобных систем, эта эффективность может рассматриваться на различных уровнях иерархии. На самом высоком уровне эффективность защиты КИС от КДВ

осуществима по приращениям основных показателей корпорации. В качестве таких показателей могут выступать приросты получаемой прибыли, количества выпускаемой продукции корпорацией, сокращения суммарных расходов людских, материальных и других ресурсов за счет использования защищенных КИС по сравнению с незащищенными системами.

Чуть ниже эффективность защиты КИС осуществима по приращениям показателей успешности функционирования административных и производящих продукцию структур. Применительно к административным структурам эффект от использования соответствующих КИС может выражаться в оперативности и точности принимаемых управленческих решений, снижении затрат временных ресурсов на административную деятельность. Для структур непосредственно производящих отдельные виды продукции, в том числе новых знаний и технологий, эффективность использования защищаемых КИС может оцениваться по следующим показателям. Это приросты основных показателей этих подразделений (вероятностей и времени выполнения планов, получаемых конкретных результатов).

Если учесть, что КИС обеспечивает на различных уровнях иерархии некоторые сервисы стимулирующие деятельность корпорации, то в ряде случаев эффективность защиты ее от комплексных деструктивных воздействий можно оценивать по приращениям показателей этих сервисов за счет реализуемых мероприятий защиты. Например, эффективность каждого отдельного сервиса КИС можно оценить вероятностью соответствия его заданным требованиям. К таким требованиям могут относиться различные условия по обеспечению функциональности, качеству предоставляемой информации, по задержкам в удовлетворении заявок и другие.

Для оценивания выполнения сценариев многомодального взаимодействия пользователей с обеспечивающими устройствами окружающего киберфизического пространства можно выделить также показатели качества обслуживания, уникальные для каждого сервиса. Каждая

пользовательская заявка требует обслуживания (выполнения), которое предполагает загрузку определенных аппаратных и программных ресурсов (дисплей, звук, пользовательская сессия) в течение некоторого времени [53]. Некоторые детализированные показатели эффективности предоставления сервисов КИС приведены в таблице 4, где использованы следующие обозначения:

t_{UI} - максимальное время реакции пользовательского интерфейса, которое пользователь считает комфортным. В [45, 68] описаны виды пределов для времени отклика интерфейса пользователя. В частности, при времени реакции до 0,1 с пользователь воспринимает взаимодействие без задержек. При времени реакции до 1 с пользователь воспринимает процесс взаимодействия как хорошо контролируемый. При достижении 10 с задержки пользователь с высокой вероятностью отвлечётся на другие задачи;

p_D - максимально допустимая вероятность отказа в выполнении пользовательской задачи, которую можно выбирать, руководствуясь стандартом [54].

Таблица 4. Показатели эффективности реализации сервисов, не привязанные к видам

Показатель	**Единица измерения**	**Обозначение**	**Возможные значения**	**Допустимые значения**
Время загрузки приложения	с	t_l^{App}	$[0; \infty)$	$[0;\ t_{UI}]$
Время инициализации приложения	с	t_i^{App}	$[0; \infty)$	$[0;\ t_{UI}]$
Время актуализации данных в приложении	с	t_a^{App}	$[0; \infty)$	$[0;\ t_{UI}]$
Относительная доля выполненных заявок (относительная пропускная способность)	-	$f_{np}^{Success}$	[0; 1]	$[1 - p_D;\ 1]$
Относительная доля выполненных заявок, взвешенная по приоритету	-	$f_p^{Success}$	[0; 1]	$[1 - p_D;\ 1]$

Показатель	**Единица измерения**	**Обозначение**	**Возможные значения**	**Допустимые значения**
Относительная доля отказов в выполнении пользовательских заданий при отсутствии конкурирующих заданий	-	f_{norm}^{Denial}	[0; 1]	$[0; p_{D}]$
Относительная доля отказов в выполнении пользовательских заданий при наличии конкурирующих заданий	-	f_{stress}^{Denial}	[0; 1]	$[0; p_{D}]$
Время задержки в выполнении пользовательских заданий при отсутствии конкурирующих заданий	с	$t_{norm}^{Request}$	[0; ∞)	$[0; t_{UI}]$
Время задержки в выполнении пользовательских заданий при наличии конкурирующих заданий	с	$t_{stress}^{Request}$	[0; ∞)	$[0; t_{UI}]$

Исследования [55] показывают, что наибольшее влияние на восприятие пользователем веб-сервисов, в отличие от мультимедийных аудио- и видеосервисов, оказывает время ожидания конечного пользователя. Таким образом, время обработки запроса является ключевым фактором в КИС. Помимо вышеперечисленных параметров, на качество восприятия сервисов существенно влияет модальность интерфейса, посредством которого пользователь взаимодействует с системой. В частности эффективность сервиса может зависеть от точности используемых алгоритмов распознавания речи и алгоритмов распознавания лиц, удобства графического интерфейса.

Что касается специфических показателей эффективности предоставляемых КИС сервисов, по которым также может оцениваться защищенность этой системы, поясним их на примере сервиса интерактивного корпоративного телевидения МИНОС. Сервис интерактивного корпоративного телевидения взаимодействует с пользователями с помощью стационарных камер и экранов, расположенных в

разных местах организации. Кроме того, пользователи могут управлять сервисом с помощью мобильных устройств. В функции сервиса входит трансляция на стационарные экраны информации для сотрудников и посетителей (сведения об институте и его деятельности, демонстрация разработок, объявления, приветствия, поздравления) по их запросу и/или в соответствии с расписанием. Показатели этого сервиса связаны с задержками, отказами и потерями, возникающими при трансляции медиаконтента [53].

Для оценивания показателей сервиса интерактивного корпоративного телевидения могут использоваться параметры, приведенные в таблице 5. В таблице используются следующие обозначения: $t_{distraction}$ - время, по истечении которого пользователь с большой вероятностью отвлечётся на другие задачи (10 секунд по оценке в работе [45]); I - количество информации в медиафайле, бит; I_{max} - норма максимально допустимого количества информации в медиафайле, бит; R_{min}, R_{max} - оценки минимальной и максимальной скорости восприятия информации пользователем, бит/с.

Помимо этих показателей для оценивания эффективности защиты КИС от КДУ могут быть использованы и другие. Во всех случаях для расчета подобных показателей необходимо иметь модели анализируемых процессов, протекающих в КИС.

Таблица 5. Показатели качества обслуживания для сервиса интерактивного корпоративного телевидения

Показатель	**Единица измерения**	**Обозначение**	**Возможные значения**	**Допустимые значения**
Задержка между планируемым и фактическим временем трансляции медиа	с	t_{delay}^{CT}	[0; ∞)	[0; $t_{distraction}$]
Относительное время простоя	-	f_{down}^{CT}	[0; 1]	[0; $t_{distraction}$]

Показатель	**Единица измерения**	**Обозначение**	**Возможные значения**	**Допустимые значения**
Соотношение времени трансляции и объёма транслируемой информации,	бит/с	$r_{perception}^{CT}$	$[0; \infty)$	$[R_{min};\ R_{max}]$
Время смены медиафайлов	с	t_{load}^{CT}	$[0; \infty)$	$[0;\ t_{UI}]$
Относительная доля неуспешных загрузок контента	-	f_d^{CT}	[0; 1]	$[0;\ p_D]$
Относительная доля потерь по времени	-	f_t^{CT}	[0; 1]	$[0;\ 1 - I/I_{max}]$
Относительная доля потерь по области отображения	-	f_i^{CT}	[0; 1]	$[0;\ 1 - I/I_{max}]$
Коэффициент искажения	-	k_d^{CT}	[0; 1]	$[0;\ 1 - I/I_{max}]$

Метод комплексного оценивания защищенности КИС от КДУ по множеству основных показателей должен предусматривать анализ их систем или различных сверток. В самом простом случае метод заключается в расчёте приращения 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. Принимая во внимание рассмотренные выше положения, в интересах оценивания защищенности КИС от КДУ раскроем ниже перспективную модель этой системы в пространстве базовых состояний.

2.3. Модель функционирования защищаемой корпоративной информационной системы

Определить исходные данные для предлагаемого метода можно с помощью математической модели, описывающей функционирование объекта

защиты. Для большинства практических случаев, процесс функционирования корпоративной информационной системы в условиях, когда возможно наличие некоторой заданной угрозы и реализован некоторый способ её обнаружения и противодействия, может быть формализован в виде графа на рис. 4.

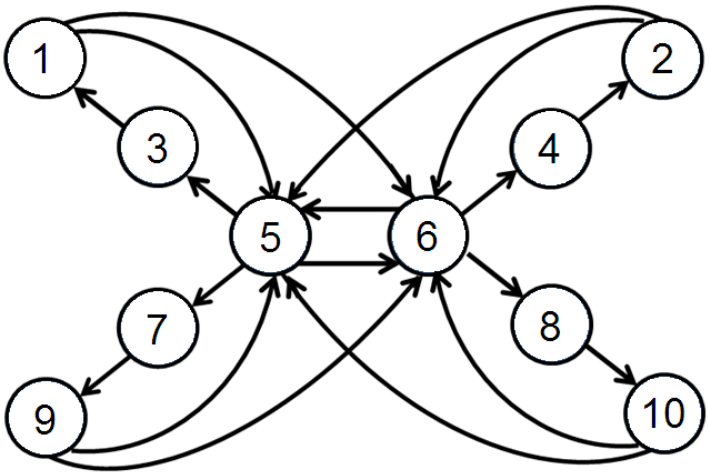


Рис. 4. Модель функционирования защищаемой КИС

Вершины графа обозначают состояния процесса, дуги – переходы из одних состояний в другие. Можно выделить 10 состояний (S_1-S_{10}) рассматриваемого процесса, которые перечислены в таблице 6. Отличия этих состояний заключаются в условиях, в которых функционирует система в заданный момент времени. Приведённое множество состояний является полной группой событий. Переходы между состояниями, показанные на рис. 4, определяются на основе характера анализируемого процесса.

Переходы $S_5 \rightarrow S_6$, $S_6 \rightarrow S_5$ 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 6. 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

Переходы $S_5 \rightarrow S_3$, $S_5 \rightarrow S_7$ возможны, когда система использует средства защиты для обнаружения угроз. Переход $S_5 \rightarrow S_3$ означает успешное обнаружение угрозы, тогда как переход $S_5 \rightarrow S_7$ характеризует пропуск угрозы, несмотря на использование средств защиты.

Переход $S_3 \rightarrow S_1$ выполняется, если выявленная угроза устраняется, $S_7 \rightarrow S_9$ – если ложная информация об угрозе принимается за истинную.

Переходы $S_6 \rightarrow S_4$, $S_6 \rightarrow S_8$, $S_4 \rightarrow S_2$, $S_8 \rightarrow S_{10}$ соответствуют случаям, когда рассматриваемая угроза отсутствует. Несмотря на отсутствие угрозы, средства защиты могут генерировать сигналы ложной тревоги. Эти сигналы могут приводить к реализации неадекватных мер защиты, что отражено в переходе $S_8 \rightarrow S_{10}$. Переход $S_4 \rightarrow S_2$ происходит, когда системы защиты определили отсутствие угрозы корректно, и никаких дополнительных защитных мер не принимается.

При разработке вышеописанной модели использовалась следующая логика. На самом высоком уровне система может быть описана только двумя состояниями (рис. 5, А), которые означают, что заданная угрозы отсутствует (2, 4, 6, 8, 10) или присутствует (1, 3, 5, 7, 9). Каждое из этих состояний

может быть разделено на два других состояния на основе использования средств обнаружения угрозы. В результате получается 4 состояния (рис. 5, B). Два из них соответствуют наличию угрозы при использовании (1, 3, 7, 9) и без использования средств обнаружения угрозы. Другие состояния характеризуют функционирование системы при отсутствии угрозы и при использовании (2, 4, 8, 10) и без использования (6) средств обнаружения угрозы.

Каждое состояние, характеризующее работу системы с использованием средств обнаружения угрозы, разделяется на два состояния по критерию результативности обнаружения (рис. 5, C). Таким образом, состояния 3 и 7 означают обнаружение и пропуск угрозы, соответственно. Состояния 4 и 8 аналогично означают корректную оценку ситуации при отсутствии угрозы и ложную тревогу. Состояния 3, 7, 4 и 8 сменяются состояниями 1, 9, 2 и 10, которые подразумевают принятие защитных мер согласно результатам обнаружения угрозы.

Таким образом, в результате получается модель на рис. 7. Корректность этой модели основана на её соответствии общим закономерностям функционирования защищаемых систем.

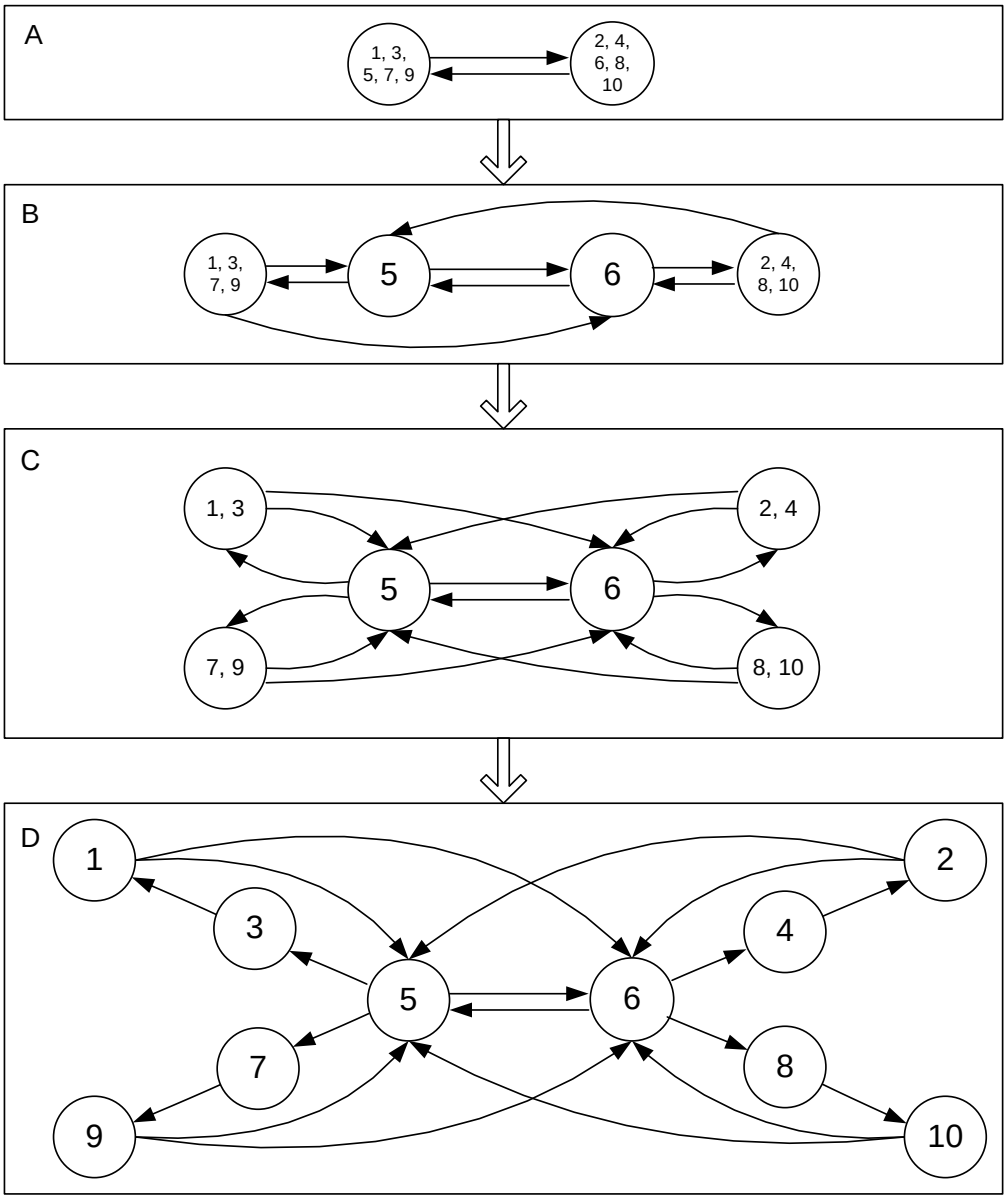


Рис. 5. Процесс построения модели функционирования системы

Классификация состояний по критериям, описанным выше, приведена в таблице 7. С учётом центральной предельной теоремы в теории вероятности для потоков событий, граф на рис. 4 может быть описан с использованием математического аппарата Марковских процессов [70]. Этот аппарат позволяет представить модель анализируемого процесса в форме системы линейных дифференциальных уравнений [42].

Таблица 7. Классификация состояний

Номер состояния	**Наличие угрозы**	**Наличие информации**	**Наличие мер защиты**	**Адекватность мер защиты**
6	–	–	–	N/A
4	–	+	–	N/A
8	–	+	–	N/A
2	–	+	+	+
10	–	+	+	–
5	+	–	–	N/A
3	+	+	–	N/A
7	+	+	–	N/A
1	+	+	+	+
9	+	+	+	–

Рассмотренному выше графу соответствует система из 10 линейных дифференциальных уравнений, каждое из которых описывает зависимость вероятностей нахождения системы в соответствующем состоянии $S_1 \ldots S_{10}$ от времени:

$$\frac{dP_1(t)}{dt} = \lambda_{31}P_3(t) - (\lambda_{15} + \lambda_{16})P_1(t)$$
$$\frac{dP_2(t)}{dt} = \lambda_{42}P_4(t) - (\lambda_{25} + \lambda_{26})P_2(t)$$
$$\frac{dP_3(t)}{dt} = \lambda_{53}P_5(t) - \lambda_{31}P_3(t)$$
$$\frac{dP_4(t)}{dt} = \lambda_{64}P_6(t) - \lambda_{42}P_4(t)$$
$$\frac{dP_5(t)}{dt} = \lambda_{15}P_1(t) + \lambda_{25}P_2(t) + \lambda_{65}P_6(t) + \lambda_{95}P_9(t) + \lambda_{10,5}P_{10}(t) - (\lambda_{53} + \lambda_{56} + \lambda_{57})P_5(t)$$
$$\frac{dP_6(t)}{dt} = \lambda_{16}P_1(t) + \lambda_{26}P_2(t) + \lambda_{56}P_5(t) + \lambda_{96}P_9(t) + \lambda_{10,6}P_{10}(t) - (\lambda_{64} + \lambda_{65} + \lambda_{68})P_6(t)$$
$$\frac{dP_7(t)}{dt} = \lambda_{57}P_5(t) - \lambda_{79}P_7(t)$$
$$\frac{dP_8(t)}{dt} = \lambda_{68}P_6(t) - \lambda_{8,10}P_8(t)$$
$$\frac{dP_9(t)}{dt} = \lambda_{79}P_7(t) - (\lambda_{95} + \lambda_{96})P_9(t)$$
$$\frac{dP_{10}(t)}{dt} = \lambda_{8,10}P_8(t) - (\lambda_{10,5} + \lambda_{10,6})P_{10}(t)$$

В рассмотренной системе уравнений $P_1(t),..., P_{10}(t)$ представляют собой вероятности нахождения системы в состояниях 1…10 в момент времени t; λ_{ij} - интенсивности переходов между состояниями i и j. Значения λ_{ij} зависят от выбора реализуемой защитной программы PRG_k.

Необходимо отметить, что решение конкретной системы уравнений даёт вероятности, описывающие поведение системы при защите от конкретной угрозы с помощью конкретной программы защиты PRG_k. Однако в этом примере для упрощения формы представления зависимость вероятностей и коэффициентов уравнений от PRG_k без потери общности опущена.

Также следует пояснить, что интенсивности λ_{ij} переходов между состояниями могут быть определены как

$$\lambda_{ij} = g_{ij} / \bar{t}_{ij},$$

где $\bar{t}_{ij}$ - среднее время перехода между состояниями i и j в идеальных условиях; g_{ij} - вероятность такого перехода.

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 выполняется модулем анализа эффектов системы защиты, которая рассматривается в главе 4. Кроме того, для каждого типа угроз и программ защиты, модель должна иметь свои начальные значения и параметры. При наличии возможности распознавания актуального состояния системы и известных λ_{ij}, появление угроз может быть предсказано.

Следует отметить, что каждое состояние в рассмотренной модели может быть «развёрнуто» во вспомогательную модель в случае необходимости более детального изучения этого состояния. При этом можно

использовать как марковские модели, так и альтернативные модели, описывающие поведение систем с точки зрения информационной безопасности. Одна из таких моделей основана на использовании автоматных объектов и приведена в работе [77].

2.4. Модель КИС в расширенном пространстве угроз

Рассмотренная выше модель описывает поведение защищаемой системы при возможном наличии единственной угрозы. Тем не менее, реальные ситуации в области защиты информации связаны с наличием комплекса взаимосвязанных угроз. В этом случае модель на рис. 4 должна быть расширена.

В частности, состояния, связанные с наличием угрозы (5), а также её корректной или ложной идентификацией (3, 9) разделяются на несколько состояний, описывающих возможные комбинации угроз. Состояния, соответствующие реализации мер защиты (1, 10), также разделяются на состояния, соответствующие мерам защиты, предусмотренным программой PRG_k при реализации тех или иных угроз.

Таким образом, граф состояний защищаемой системы при наличии двух угроз для случая, когда угрозы присутствуют, выглядит, как на рис. 6.

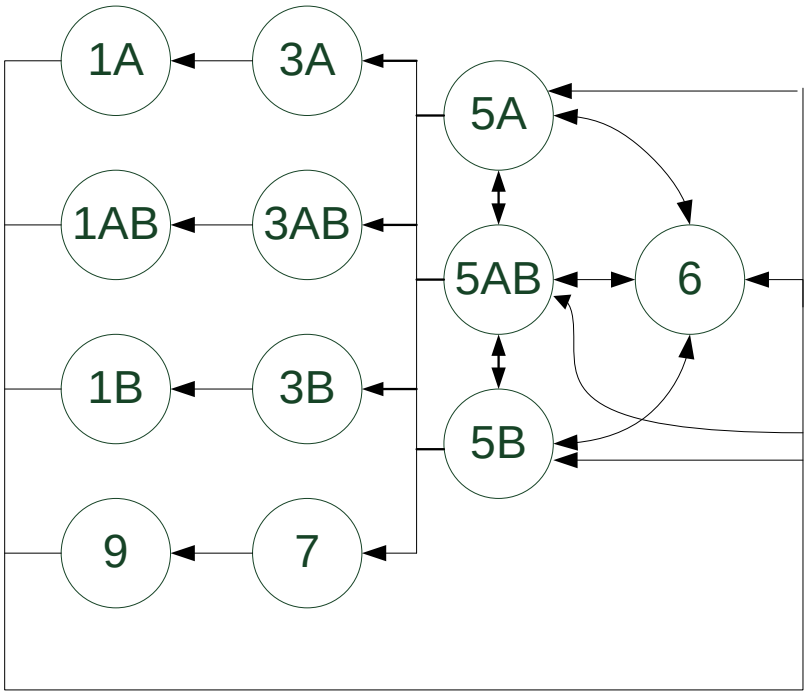


Рис. 6. Граф состояний КИС при наличии угроз

В случае, если угрозы отсутствуют, соответствующие состояния системы показаны на рис. 7.

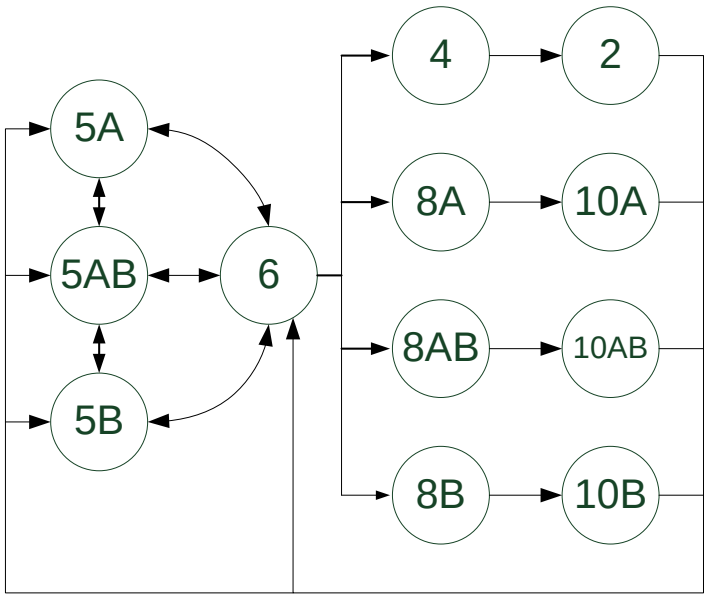


Рис. 7. Граф состояний КИС при отсутствии угроз

Рассмотренные графы при известных начальных условиях и интенсивностях перехода позволяют рассчитывать вероятности нахождения

защищаемой системы в том или ином состоянии. В случае, если этим состояниям сопоставлены оценки экономического или иного эффекта, то модель позволяет оценить эффект и его зависимость от условий функционирования защищаемой системы. Алгоритм, предлагаемый для реализации метода оценивания, рассматривается в п. 2.5.

2.5. Алгоритм оценивания эффективности защиты корпоративных информационных систем с применением марковских моделей

Рассмотрим особенности использования предложенных выше марковских моделей анализируемых процессов для оценивания эффективности защиты КИС.

Эти особенности включают в себя следующие шаги:

Ш1. Расчет вероятностей $P_z^*(t)$, $P_{zk}(PRG_k, t)$ нахождения КИС в выделенных состояниях без применения мер защиты с этими мерами на заданный момент времени.

Ш2. Оценка 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:

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

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

Ш3. Каждому состоянию z ставится в соответствие величина эффекта V_z, связанная с показателями качества обслуживания, доставляемого пользователю в единицу времени.

Ш4. Рассчитываются совокупные эффекты L^*, $L(PRG_k)$ КИС без мероприятий защиты и с ними,

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

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

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

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

Ш5. Оценка прироста $\Delta L = L_z(PRG_k) - L_z^*$ эффективности КИС за счет реализуемых мероприятий защиты.

Рассмотрим для примера показатели QoS для сервиса интерактивного корпоративного телевидения, связанные с искажением, задержкой и отменой выполнения заданий. Для оценки эффекта $V_z(t)$ эти показатели необходимо свернуть в единый показатель.

Рассмотрим для начала коэффициент искажения k_d, который определяется как среднее значение искажения элементов медиафайла:

$$k_d = \frac{1}{N} \sum_{i=1}^{N} \Delta E(P_i, P_i^*),$$

где N – количество элементов медиафайла (пикселов), ΔE – функция цветовой разницы между пикселами P_i (фактическим) и P_i* (идеальным) [56]. В более простом случае, при использовании бинарной функции цветовой разницы коэффициент можно представить как отношение площади искажённой области к общей площади изображения. В идеальном случае зависимость k_d от времени для сигнала длительностью l выражается через функцию Хевисайда:

$$k_d{}^*(t) = \theta(t) - \theta(t - l)$$

Для учёта времени задержки t_{delay} введём вспомогательную функцию задержки (рис. 8), характеризующую своевременность выполнения пользовательского задания:

$$d(t) = \begin{cases} 1, & t \le l \\ e^{-\alpha(t-l)}, & t > l \end{cases},$$

где α – коэффициент, характеризующий скорость потери актуальности задания при его задержке.

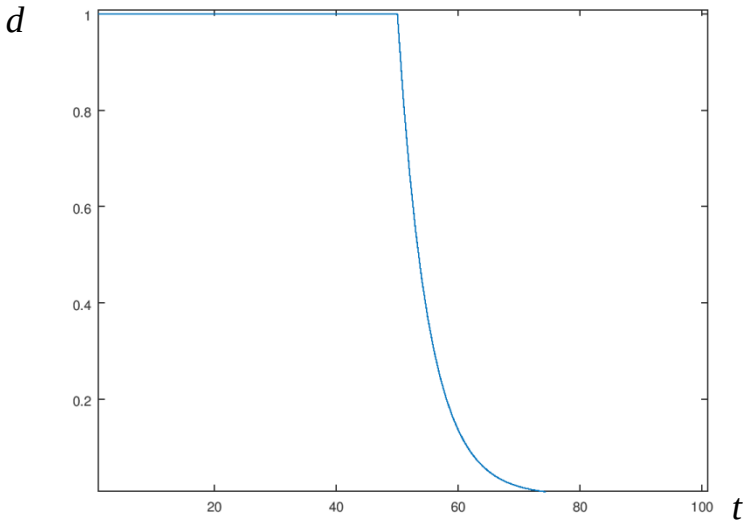


Рис. 8. Функция *d(t)*

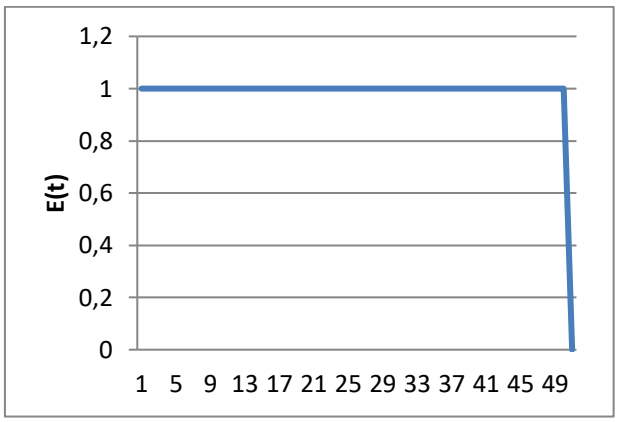
В этом случае величина

$$E(t) = k_d(t)d(t)$$

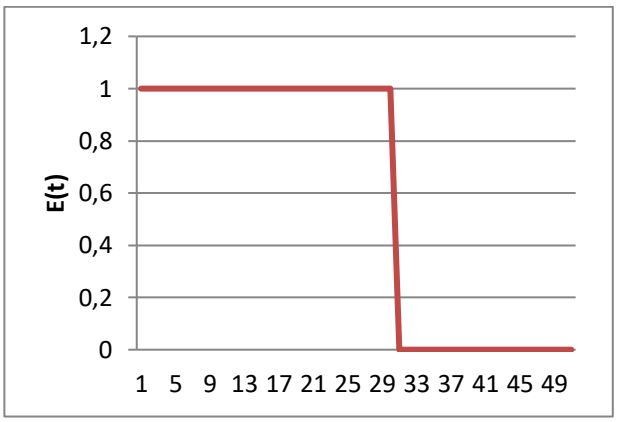
характеризует как возможные искажения, так и задержки. Для учёта отказа системы пользователю в выполнении задания в этом случае можно принять $t_{delay} = \infty$.

На графиках на рис. 9 отражено поведение величины при отсутствии потерь данных и при наличии потерь данных разного рода. В частности, представлены примеры зависимостей при $l = 50$ для идеального случая (а), случая преждевременного завершения задания в момент $t = 30$ с (б), случая

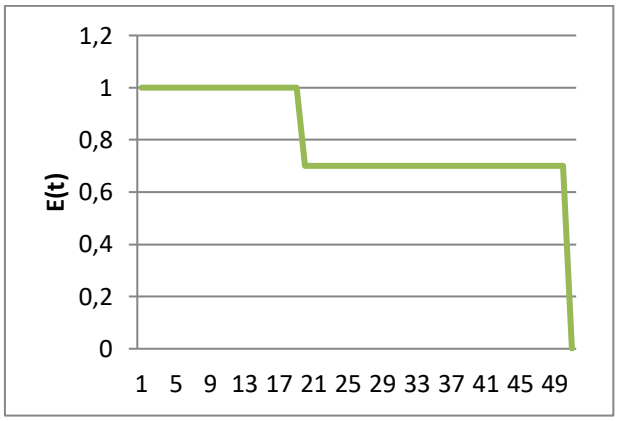
возникновения искажения в момент $t = 20$ с (в) и случая задержки выполнения на 28 с (г).



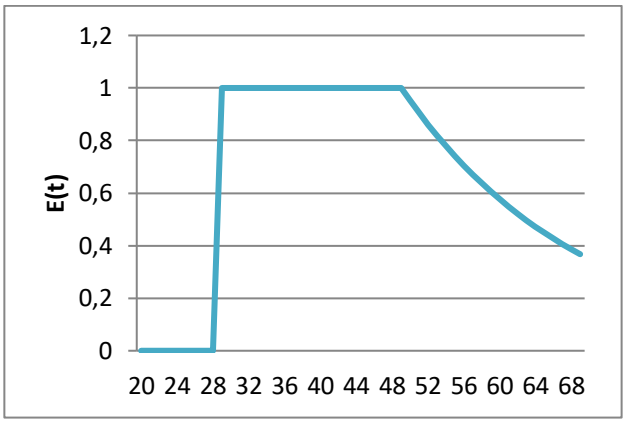
а) Отсутствие искажений



б) Отмена задания при $t = 30$ *с*



в) Потеря данных при $t = 20$ *с*



г) Задержка на 28 с

Рис. 9. Зависимости функции эффекта от возможных искажений

2.6. Выводы

Разработан новый метод оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий. В основу этого метода положено использование предложенной новой марковской модели функционирования защищаемой КИС в условиях комплексных деструктивных информационных угроз. Формализация процесса согласно этой модели осуществляется в ранее не исследуемом пространстве состояний КИС. Оценку эффективности защиты предлагается осуществлять с использованием этой модели по интегральному показателю

эффективности функционирования КИС с учетом времени нахождения ее в каждом состоянии и достигаемого частного эффекта в нем.

3. Метод адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий

3.1. Архитектура системы адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий

Для раскрытия предлагаемого метода рассмотрим модель системы адаптивной защиты КИС от комплексных деструктивных воздействий. Структура этой системы приведена на рис. 10. 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.

Цель данной системы – адаптивная защита от гетерогенных деструктивных информационных воздействий на компьютерные сети. Для этого используются различные методы. Например, для защиты от комплексных сетевых воздействий можно использовать способ обнаружения атак, предложенный в п. 4.4. Адаптация системы к актуальным условиям функционирования выполняется с помощью её реконфигурирования. Реконфигурирование подразумевает подстройку блоков системы к текущей ситуации, а также выбор подходящих методов защиты.

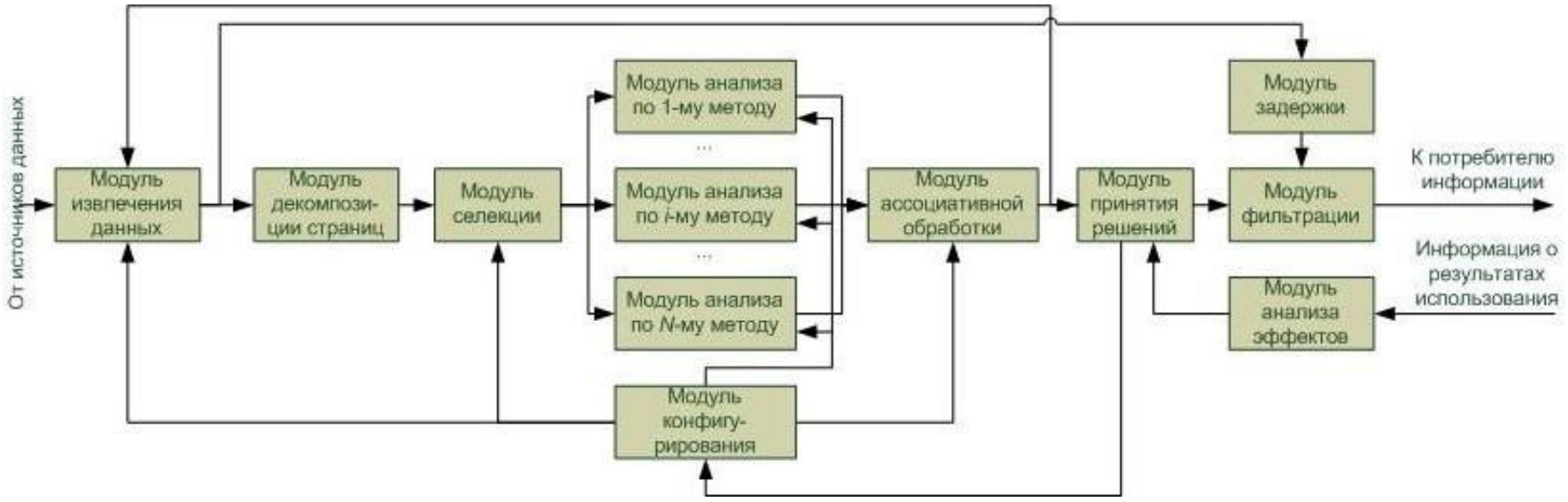


Рис. 10. Структура системы адаптивной защиты

Согласно рис. 10, процесс защиты начинается со сбора данных от источников. В качестве данных система может принимать интернет-трафик в форме дампов, контент в статистической, структурной, текстовой или мультимедийной форме. Поставщиками данных могут быть узлы локальной или глобальной сети, аппаратное и программное обеспечение. В зависимости от количества и определённости источников данных могут применяться три подхода:

1. Постоянный мониторинг конкретных источников информации с анализом информации, поступающей от них. Этот подход применим для небольшого количества чётко заданных источников, так как вычислительный ресурс анализатора ограничен. Примером такого наблюдения может быть постоянный перехват трафика с сетевого узла интерфейсом, работающим в неразборчивом режиме.

2. Периодический мониторинг источников информации с частичным анализом информации, поступающей от них. Этот подход используется при ограниченных возможностях в области наблюдения и анализа в ситуациях, когда необходимо контролировать значительное количество источников. Примером такого мониторинга является использование контрольных сумм (хэшей) и регулярных выражений для определения изменений и выявления необходимых элементов данных в большом объёме информации.

3. Поиск источников информации, представляющей интерес. Этот подход используется, если множество источников не определено. Подход применим как для поиска новой информации, так и для валидации существующей. Примером является рассылка широковещательных сообщений в компьютерной сети для поиска узлов, поддерживающих тот или иной протокол обмена информацией.

В общем случае входные данные включают как информацию для анализа, так и информацию обратной связи от пользователя. Рассмотрим пример, когда система анализирует данные, представленные в Web-формате. После извлечения данных из внешнего источника, система подгружает

связанные компоненты (фреймы с другими документами, медиафайлы, стили, сценарии, и т. д.) Затем система декомпозирует данные, т.е. строит их структурную модель. Так, при обработке HTML-страниц парсер преобразует простой текст в иерархическую структуру тегов DOM (Document Object Model). После определения структуры данных выполняется выбор компонентов для анализа: система идентифицирует составляющие документа (текст, изображение, видео) как отдельные информационные объекты. Для HTML-документов идентификация выполняется на базе видов тегов и их содержания, например: теги <title>, <h1>…<h6> означают текстовые блоки, содержащие заголовки документа и его секций; <p>, , <article> - блоки текста; <img>, <canvas>, <figure> - изображения; <video>, <object>, <embed> - видеофайлы или вложенные объекты; <audio> - звуковые файлы, <a> - гиперссылки.

Идентифицированные информационные объекты можно анализировать различными методами в зависимости от типа и характеристик объектов. Помимо контента объектов, необходимо принимать во внимание следующие факторы:

- целостную структуру документа (отношения следования и композиции между отдельными объектами), которая определяется иерархией HTML-тегов;
- связи с другими документами, которые могут быть реализованы в виде гиперссылок и фреймов;
- пространственное соотношение компонентов документов, которое может быть статическим, определённым набором стилей или, реже, атрибутами HTML-тегов; или динамическим, формируемым сценариями документа после того, как документ загружен.

Информацию о классах информационных объектов, методах их анализа и их параметрах предоставляем модуль конфигурации. Ряд подобных методов был перечислен в п. 1.5.

На базе проведённого анализа информационных объектов, каждому из них назначаются свойства, которые отражают присущие ему характеристики. К важным свойствам информационных объектов, прежде всего, следует отнести их структурные, частотные и содержательные особенности отдельных конструкций и объектов в целом.

В результате мы имеем дело с многоуровневой структурой свойств информационных объектов и правил их оценки, позволяющих перейти от оценки характеристик информационного объекта, вычисляемых непосредственно, к оценке существенных свойств объекта как носителя информации, а от них – к определению класса информационного объекта в целом [73]. Схему оценки информационных объектов можно представить в виде рис. 11, где вершинами обозначены реализуемые функции, а дугам ставятся в соответствие весовые коэффициенты.

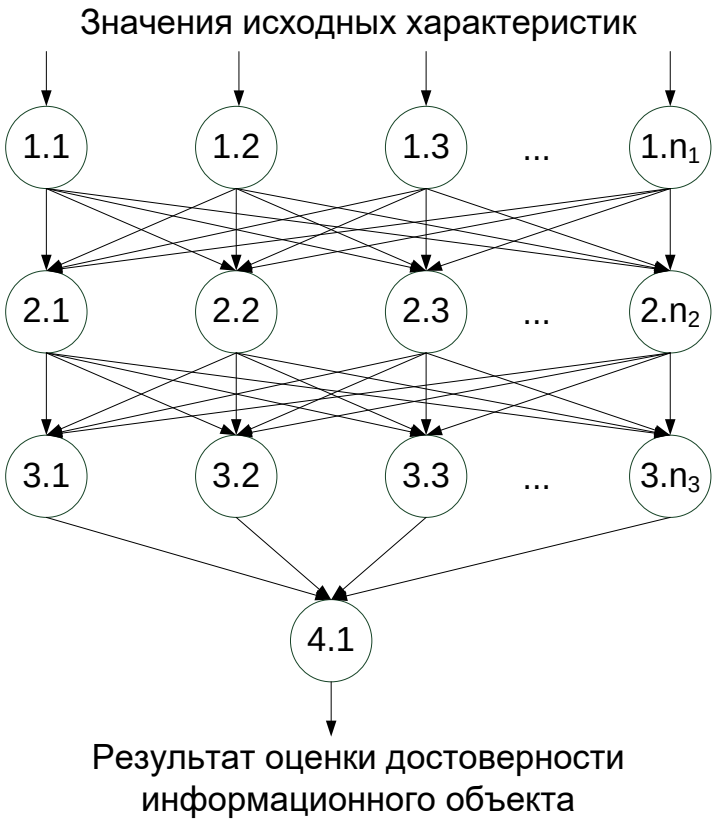


Рис. 11. Схема оценки достоверности информационных объектов

В некотором смысле такую схему оценки можно трактовать как классификатор информационных объектов по уровням легитимности. Поясним такой подход.

Каждому информационному объекту можно поставить в соответствие многоуровневую систему его характеристик (свойств). Отнесение таких объектов к вредоносной информации в общем случае предусматривает анализ его характеристик на различных уровнях иерархии с учетом их взаимосвязей. Для случаев, когда известна многомерная плотность $f(y_1,..., y_n)$ распределения характеристик $y_1,..., y_n$ информационного объекта, вероятность $P_{ди}$ отнесения его к легитимной информации можно рассчитать по формуле:

$$P_{ди} = P_a \int_{Y_1} ... \int_{Y_n} f(y_1,...,y_n) dy_1 .. dy_n,$$

где P_a — априорная вероятность наличия легитимной информации; $Y_1,..., Y_n$ — области значений для истинных характеристик информационного объекта.

Если считать независимыми друг от друга характеристики $y_1,..., y_n$, то:

$$P_{ди} = P_a \int_{Y_1} f_1(y_1) dy_1 ... \int_{Y_n} f(y_n) dy_n,$$

где $f_1(y_1)$, …, $f_n(y_n)$ — одномерные плотности распределения характеристик $y_1,..., y_n$. Согласно этим выражениям информационный объект может быть отнесен к вредоносной информации при низкой априорной вероятности P_a или при низкой вероятности достоверности хотя бы одной из его характеристик.

На практике необходимо учитывать неравнозначность вклада каждой характеристики в $P_{ди}$. Для определения достоверности множества одноуровневых, но не равнозначных характеристик информационного

объекта, отражающих некоторое его свойство, можно использовать выражение:

$$P_{\partial u}^{*} = \sum_{i \in \Omega} a_i P_{\partial u_i},$$

где $P_{\partial u_i}$ — вероятность достоверности i-й характеристики объекта; — относительный вес этой характеристики, $P_{\partial u}^{*} \le 1$.

С учетом этого интегральный показатель W оценки информационного объекта можно рассчитать по правилу: $W = W_{zi}$ при $z = Z$ и $i = 1$:

$$W_{zi} = \sum_{j=1}^{n_{z-1}} a_{zij} W_{z-1,j} \; ; \; i = \overline{1, n_z} \; ; \; z = \overline{1, Z},$$

где z — номер уровня обработки характеристик; Z — число уровней; n_z — число различных характеристик, влияющих на достоверность свойств информационного объекта, на $z+1$ уровне; a_{zij} — относительный вклад показателя $W_{z-1,i}$ в W_{zj}. На уровне $z = 1$ в качестве показателей W_{zi} могут выступать вероятности достоверности исходных характеристик информационного объекта.

Физический смысл такого интегрального показателя – взвешенная сумма частных нормированных показателей.

Для классификации объектов на базе этих свойств может использоваться ассоциативная обработка. Она позволяет устанавливать связи (в том числе неявные) между свойствами информационных объектов и их классами (например, достоверная информация, ошибочная, ложная, деструктивная, и т.п.).

Результаты ассоциативной обработки используется, чтобы сделать выводы о типе анализируемой информации и о мерах защиты, которые следует применять в актуальных условиях. После этого, информация при необходимости корректируется и передаётся её потребителю. Процедура фильтрации может включать такие действия, как удаление вредоносной

информации, коррекция ошибок, внедрение дополнительной разметки в информационный объект.

С учётом возможности оценить получаемый совокупный эффект в разных условиях функционирования системы, можно построить метод реконфигурирования системы защиты. В частности, реконфигурирование может включать в себя коррекцию процедур обработки данных в информационных объектах, удовлетворяющих ряду условий (например, принадлежность к определённому классу, происхождение от некоторого источника данных). Коррекция может включать добавление и удаление методов обработки информационных объектов, изменение параметров этих методов для повышения точности обработки информации, что, в свою очередь, приводит к повышению эффекта.

Принимая во внимания особенности приведённого примера системы адаптивной защиты, перейдём к рассмотрению метода, на базе которого подобная система может функционировать.

3.2. Алгоритм адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий

Опираясь на рассмотренную выше модель, раскроем алгоритм, лежащий в основе предлагаемого метода адаптивной защиты КИС. Этот алгоритм учитывает изменяющиеся условия при функционировании защищаемой системы. Блок-схема этого алгоритма приведена на рис. 12. Конечной целью работы этого алгоритма выступает поиск и реализация целесообразной конфигурации системы защиты, обеспечивающей максимальные возможности защиты в сложившихся условиях.

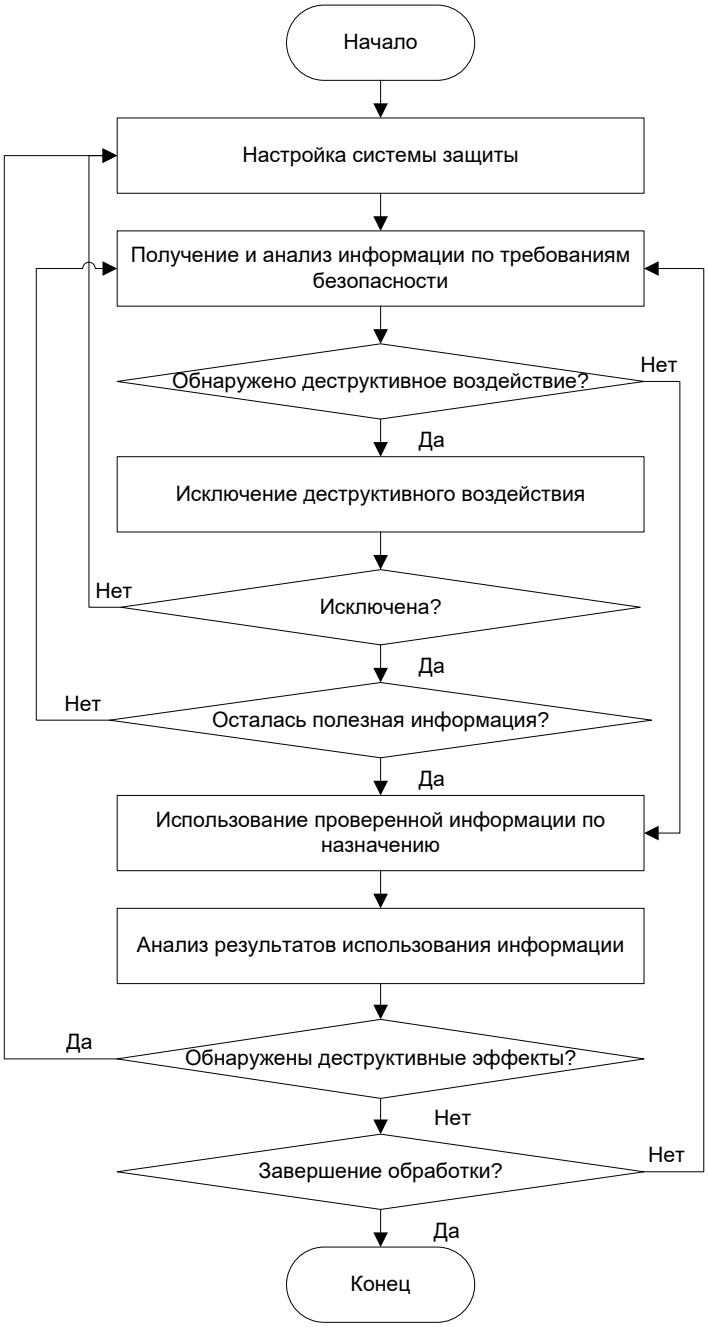


Рис. 12. Алгоритм адаптивной защиты от комплексных информационных угроз

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. Подобные модели были построены в главе 2.

Процессы получения блоков информации и их анализа по требованиям безопасности имеют свои особенности в зависимости от конфигурации системы. Так, информация может происходить из разных источников. Она может быть разных типов и качества, обладать противоречивостью. Желательно, чтобы априорные данные, включая результаты прогноза, а также комплексные методы оперативного выявления деструктивных воздействий использовались настолько широко, насколько возможно. Чтобы повысить полноту и достоверность полученной информации, источники данных могут быть распределены по вычислительным ресурсам. Если в рассматриваемом образце данных обнаружена угроза, алгоритм предусматривает защитные меры, как на уровне системы, так и на уровне конкретного образца данных (коррекция, удаление). Только затем образец данных передаётся компонентам защищаемой системы.

Тем не менее, риск пропуска угрозы остаётся в связи с несовершенством защитных методов. Это может вызвать негативные эффекты в функционировании защищаемой системы. Чтобы выявить эти эффекты, следует анализировать результаты функционирования защищаемой системы. Если негативные эффекты выявлены, система защиты должна быть реконфигурирована для исключения таких эффектов в будущем.

При реконфигурации необходимо учитывать не только текущее состояние системы, но и результаты прогнозов, построенных с помощью соответствующих моделей. Такие модели должны предсказывать как сами угрозы, так и их последствия. Модели, рассмотренные в главе 2, удовлетворяют этим требованиям.

3.3. Метод оптимизации конфигурации системы защиты

В рамках рассмотренного в п. 3.2 алгоритма должна осуществляться оптимизация конфигурации системы защиты КИС от комплексных 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]*:

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

при следующих ограничениях:

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

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

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

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 значений переменных: $k = 0$, $L_{opt} = 0$.
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 шагу 8.

14. Если $L_{opt} < L_k$, то $L_{opt} = L_k$, $PRG_{opt} = PRG_k$.

15. Перейти к шагу 2.

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.

Возможный способ определения $t_k(PRG_k)$ для программ конфигурирования рассмотрен в п. 3.3.

Для большого количества альтернативных программ полный поиск может быть заменён известными методами оптимизации, например, методом ветвей и границ [44], и т. п.

Рассмотренный метод оптимизации конфигурации системы защиты КИС отличается от других известных решений новым набором правил, позволяющих реализовывать адаптивную защиту от комплексных 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 в п. 3.1, решение оптимизационной задачи (1) - (4) можно реализовать в модуле конфигурирования на рис. 12.

3.4. Оценка вспомогательных параметров процесса конфигурирования системы защиты КИС

Рассмотрим факторы, влияющие на решение задачи в п. 3.3. Все факторы, оказывающие влияние на интегральный показатель эффекта, можно разделить на группы:

1. Внешние факторы, которые в незначительной степени зависят от объекта защиты и слабо поддаются корректировке: например, ситуация в зоне расположения защищаемой системы, знания злоумышленников о новых технологиях и возможных уязвимостей в системах защиты. Эти факторы выражаются в интенсивностях возникновения и исчезновения угроз λ_{56} и λ_{65} в модели из п. 2.1.

2. Факторы, связанные с программами конфигурирования системы защиты:

- множество программ конфигурирования систем защиты $\{PRG_k\}$, множество результативных программ R и время реализации каждой программы $t_k(PRG_k)$;

- максимально допустимое время исполнения программы конфигурирования t_D;

- факторы, отражающие способность объекта и системы защиты адекватно воспринимать и использовать информацию, поступающую из среды. Они зависят от методов получения информации и отнесения её к классам (истинная, ложная, вредоносная, полезная, незначительная и т.п.) Эти факторы выражаются интенсивностями λ_{53}, λ_{57}, λ_{64}, λ_{68};

- факторы, отражающие способность объекта и системы защиты предпринимать своевременные эффективные шаги для устранения угроз и, в случае необходимости, их последствий. Эти факторы выражаются интенсивностями λ_{31}, λ_{79}, λ_{42}, $\lambda_{8,10}$.

3. Факторы, связанные со спецификой защищаемого объекта:

- факторы, выражающие способность защищаемого объекта получать эффект в различных условиях функционирования, соответствующих состояниям в модели из п. 2.1. Эти факторы определяются функциями плотностей эффекта $V_z(t)$;

- начальные условия функционирования (вероятности нахождения защищаемой системы в каждом состоянии в момент времени $t = 0$).

Рассмотрим более подробно процедуры определения начальных значений этих параметров.

Множество программ конфигурации $\{PRG_k\}$ строится на основе методов защиты, рассмотренных в п. 1.3 и 1.4. Каждая такая программа включает в себя действия по выбору (1), загрузке (2), инициализации (3), настройке (4) и вводу в эксплуатацию (5) программных средств, реализующих те или иные защитные меры.

Процесс реализации каждой конфигурационной программы можно представить в виде цепи Маркова, в которой выделены, помимо вышеперечисленных состояний, начальное (S) и конечное (F) состояния (рис. 13).

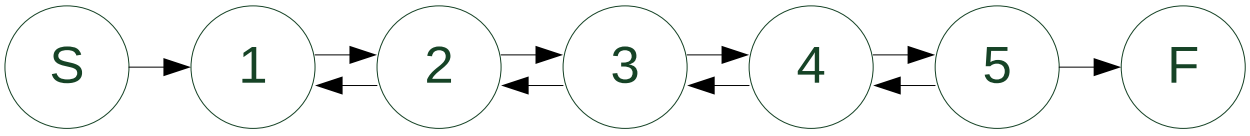


Рис. 13. Модель процесса конфигурации

Подобная модель позволяет оценить соответствие программы PRG_k ограничениям (2) и (3). Так, программа является реализуемой (входит в множество R), если в установившемся режиме соответствующий процесс приходит в конечное состояние:

$$\lim_{t\to\infty} P_{Fk}(t) = 1$$

Использование модели позволяет также определить значение $t_k(PRG_k)$. Значение $P_{Pk}(t)$ характеризует вероятность того, что в момент времени t программа завершена. Выбрав допустимое значение p_0 вероятности того, что выполнение программы не завершено, можно найти такое наименьшее значение момента времени t_0, что для всех $t > t_0$ будет выполняться следующее условие: $P_{Fk}(t) \geq 1 - \alpha$. В этом случае можно принять $t_k(PRG_k) = t_0$. Допустимое время исполнения программы t_D можно определить следующим образом.

Рассмотрим мгновенное значение эффекта функционирования системы в момент времени t при текущих условиях (выполнена программа PRG_k):

$$l_k(t) = \sum_{z=1}^{Z} V_z(t) P_{zk}(PRG_k, t),$$

где PRG_k – выполненная программа конфигурирования защитной системы. В случае, если в момент $t = 0$ выбирается и исполняется другая программа PRG_m с длительностью исполнения $t_m(PRG_m)$, то значение эффекта l_m будет определяться как:

$$l_m(t) = \begin{cases} \sum_{z=1}^{Z} V_z(t) P_{zk}(PRG_k, t), t \leq t_m(PRG_m) \\ \sum_{z=1}^{Z} V_z(t) P_{zm}(PRG_m, t), t > t_m(PRG_m) \end{cases}$$

Значение интегрального эффекта на отрезке времени *[0; T]* можно представить как функцию от $t_m(PRG_m)$ и рассчитать как

$$L_m(t_m(PRG_m)) = \int_0^{t_m(PRG_m)} l_k(t)dt + \int_{t_m(PRG_m)}^{T} l_m(t)dt$$

Используя модели, разработанные в п. 2.1 и п.2.2, и метод определения эффективности, представленный в п. 2.4, можно определить вид функции $L_m(t_m)$ и сравнить её с интегральным значением эффекта без учёта выполнения программы PRG_m:

$$L_k = \int_0^T l_k(t)dt$$

Для этого определяется значение прироста эффекта:

$$\Delta L(t_m(PRG_m)) = L_m(t_m(PRG_m)) - L_k$$

Тогда в качестве t_D можно взять наименьшее значение t_0, для которого будет выполняться:

$$\Delta L(t_0) < 0$$

Рассмотрим далее факторы, связанные со спецификой защищаемого объекта. Множество функций эффекта $\{V_z(t)\}$ определяется на основе метода в п. 2.4 с использованием моделирования функционирования КИС при различных условиях. Для определения начальных условий $\{P_{zk}(t=0)\}$ используются известные методы распознавания состояний защищаемой системы, ряд из которых рассмотрен в главе 1.

Проясним процесс определения начальных условий анализируемого процесса на примере простых случаев защиты сервера от DDoS-атак. Такие атаки основаны на деструктивном информационном воздействии, заключающемся в передаче серверу ложной информации о намерениях клиентских компьютеров подключиться к защищаемому серверу и/или выполнить на нём некоторые легитимные операции. С использованием

накопленной статистики можно оценить наличие и отсутствие такого воздействия в информационном потоке на входе защищаемой системы. В данном случае эти вероятности будут выражаться значениями $P_5(0)$ и $P_6(0)$ в контексте модели, представленной в п. 2.1. В случае, если угроза DDoS-атаки достоверно определена с помощью известных методов [12], то можно установить, что $P_3(0) = 1$. В других случаях эти вероятности также можно определить, наблюдая и распознавая состояние системы.

3.5. Выводы

Предложен новый метод адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий.

Этот метод ориентирован на новую архитектуру системы защиты КИС от комплексных деструктивных воздействий, которая отличается новым множеством функциональных блоков и связей между ними.

Метод отличается тем, что основан на разработанном алгоритме адаптивной защиты, а также методе оптимизации конфигурации системы такой защиты. Алгоритм отличается тем, что предусматривает как исключение деструктивного воздействия, так и реконфигурацию системы защиты в случае, если применение этой системы не даёт достаточного эффекта. В таком случае применяется метод оптимизации конфигурации системы защиты, который отличается тем, что использует предложенную в гл. 2 модель функционирования системы при выборе оптимальной конфигурационной программы.

Предложенный метод позволяет расширить возможности систем защиты по обнаружению и устранению комплексных деструктивных воздействий.

4. Результаты моделирования и рекомендации по повышению эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий

4.1. Условия защиты корпоративных информационных систем от комплексных деструктивных воздействий

Поясним возможные условия обеспечения информационной безопасности КИС на примере корпоративной многомодальной информационно-навигационной облачной системы (МИНОС), разрабатываемой в СПИИРАН [76]. МИНОС строится на основе сервис-ориентированной архитектуры (СОА) и состоит из слабосвязанных сервисов, взаимодействующих по унифицированным протоколам с использованием веб-сокетов. В сравнении с подходом REST применение веб-сокетов позволяет на протяжении длительного времени поддерживать соединение в активном состоянии и не выполнять его открытие и закрытие при каждой передаче данных. Это особенно важно при использовании безопасного соединения (в протоколах TLS, HTTPS и др.), когда создание логического канала требует генерации ключей. Эта операция длится дольше, чем передача среднестатистического JSON-сообщения, и использование традиционного REST-подхода приведёт к существенным накладным расходам и снижению времени отклика сервисов. Кроме того, веб-сокеты позволяют контролировать статус соединений и оперативно определять и восстанавливать сервисы, по каким-либо причинам отключившиеся от системы.

Все сервисы разделяются на две категории: системные, которые обеспечивают выполнение задач, необходимых для функционирования системы в целом, и прикладные, реализующие цели системы. Перечень сервисов и их краткое описание приведены в таблице 8. Структура сервиса

отражена на рис. 14. Каждый сервис определяется контрактом (детализацией формата взаимодействия с другими сервисами), интерфейсом и реализацией.

Сервисы предоставляют пользователям разделённый доступ к информации посредством своих интерфейсов.

Таблица 8. Сервисы МИНОС

Сервис	Описание
Системные сервисы	
Сервис доступа к данным	предоставляет доступ к информации, которая может быть использована разными сервисами (например, сведения об учётных записях, пользователях и т.д.), и контролирует правомерность доступа
Репозиторий сервисов	предоставляет информацию о зарегистрированных в системе сервисах, их статусе и методам доступа к сервисам
Интерфейс администратора	позволяет управлять системой в режиме онлайн
Управление аккаунтами	позволяет запрашивать и изменять список учётных записей, их ролей и привилегий
Классная доска	позволяет сервисам публиковать информацию о своих событиях для обработки другими сервисами
Прикладные сервисы	
Сервис корпоративного телевидения	транслирует медиаконтент (видеоролики, объявления, информационные сообщения) на клиентские устройства (стационарные экраны)
Сервис корпоративного портала	позволяет использовать информацию от сервисов МИНОС на сайте организации
Сервис коммуникации	позволяет пользователям управлять информационным пространством с помощью многомодальных технологий (речь, жесты)
Сервис навигации	предоставляет клиентским устройствам информацию об их физическом расположении в корпоративном пространстве, о расположении подразделений организации и маршрутах их достижения
Сервис видеоконференцсвязи	организует видеоконференцсвязь между клиентскими устройствами в корпоративном пространстве
Сервис идентификации	позволяет идентифицировать посетителей различными методами (с помощью электронных ключей, биометрических признаков)

В качестве примера рассмотрим процесс взаимодействия пользователей с сервисами интерактивного корпоративного телевидения, локализации и навигации МИНОС [61]. Эти сервисы реализуются в виде комплекса веб-камер, стационарных экранов и неттопов с целью упростить получение пользователями сведений об организации, новостей, информации о

местонахождении пользователей. Веб-камеры используются в процессе регистрации, идентификации и распознавания лиц пользователей и позволяют автоматизировать их аутентификацию. Использование многомодальных интерфейсов упрощает процесс получения информации пользователями.

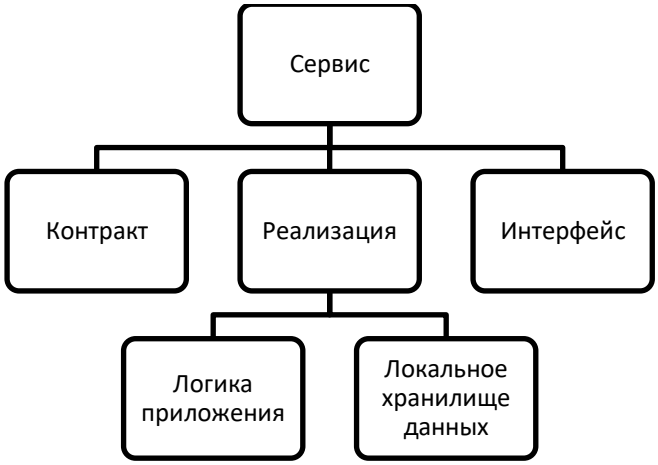


Рис. 14. Структура сервиса

Одной из особенностей разрабатываемого модуля корпоративного телевидения является его интерактивность. Интерактивное взаимодействие может быть обеспечено с помощью многомодальных интерфейсов. Пользователи создают запросы к сервисам, используя различные интерфейсы (речевые, жестовые) или посредством веб-приложений. С их помощью можно реализовать управление модулем с помощью голоса и жестов. Также модулем КТ можно управлять с помощью портативных устройств пользователей.

Администраторы также могут контролировать сервисы с помощью специального веб-интерфейса.

В общем виде взаимодействие между пользователем и модулем выполняется по следующему алгоритму:

1. Модуль КТ генерирует одноразовые токены для доступа к управлению и выводит их на стационарные экраны в виде QR-кодов.

2. Пользователь сканирует QR-код с помощью мобильного приложения и получает токен.

3. Мобильное приложение подключается к API КТ с помощью полученного токена и предоставляет пользователю графический интерфейс.

4. Пользователь использует графический интерфейс для получения данных о контенте и управления корпоративным телевидением.

Схема управления приведена на рис. 15.

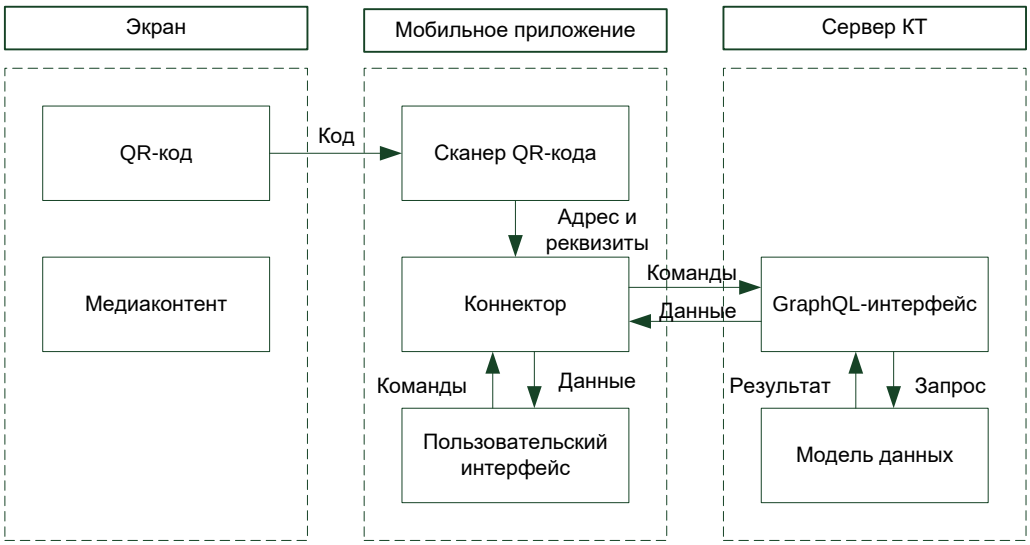


Рис. 15. Схема управление модулем КТ через мобильное приложение

В качестве API КТ используется интерфейс на базе GraphQL. GraphQL представляет собой язык запросов, позволяющий запрашивать и обновлять данные, находящиеся на сторонних источниках. GraphQL позволяет унифицировать представление структур данных у взаимодействующих сторон и создать промежуточный уровень, обеспечивающий корректную передачу, маршрутизацию и трансформацию данных, обработку триггеров, независимость от конкретных источников и получателей информации.

Модуль КТ предоставляет два типа GraphQL-запросов: query для получения актуального состояния сервиса и mutation для изменения состояния (отправки управляющих команд).

Запрос query имеет вид:

```
query {
```

```
monitor(id: <ID >, key: <key>) {
     currentMedia,
     status,
     medias {
          id,
          name
     }
}
}
```

В запросе <ID> означает уникальный идентификатор экрана КТ, <key> – авторизационный токен, обязательный при отправке первого запроса в сессии. Поля currentMedia, status, id, name являются необязательными и определяют состав запрашиваемых данных. Состав полей приведён в таблице 9.

Таблица 9. Поля запроса

Поле		Описание
currentMedia		ID активного медиафайла
status		Флаги состояния экрана: 1 – ошибка 2 – режим отладки включён 4 – кэширование включено 8 – пауза 16 – блокировка
medias.	id	ID очередного медиафайла
medias.	name	Название очередного медиафайла

Запрос mutation имеет вид:

```
mutation {
     sendMessage(id: <ID>, commands: <commands>) {
          status
     }
}
```

Поле <ID> означает идентификатор экрана, поле <commands> содержит одну или более управляющих команд, разделённых знаков «;». Запрос возвращает состояние дисплея после выполнения команды. Список команд приведён в таблице 10:

Таблица 10. Управляющие команды КТ

Команда	**Описание**
next	Переключение на следующий файл
prev	Переключение на предыдущий файл
load <ID>	Загрузка файла с заданным ID
pause [on | off]	Остановка/возобновление
lock [on | off]	Блокировка/разблокировка экрана
debug [on | off]	Включить/отключить режим отладки
reload	Перезагрузка приложения

Каждый пользовательский запрос должен быть обработан, т.е. для него создаётся отдельная задача, требующая выделения объёма ресурсов (аудио- и видеоканалы, память, процессор, пользовательские сессии) в течение некоторого времени. Недостаток ресурсов хотя бы одного типа при выполнении этих задач может привести к снижению доступности сервиса. Например, в случае единственного пользователя, работающего с сервисом корпоративного телевидение, поступление каждого следующего запроса подразумевает приостановку предыдущего, если эти запросы конфликтуют за ресурс. В таком случае угрозы доступности не создаётся. Однако при наличии нескольких пользователей выделить требуемый ресурс для всех задач может оказаться невозможным. В этом случае используются стратегии управления пользовательскими запросами [8], которые должны максимизировать метрики доступности сервиса. Выбор стратегий управления запросами и их параметров зависит от структуры и характера возникновения запросов. Таким образом, оптимальная стратегия может меняться в зависимости от условий функционирования сервиса. В этом случае для

обеспечения доступности необходимо использовать адаптивные методы выбора управляющих конфигураций.

4.2. Исходные данные и результаты моделирования

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 сеть массового обслуживания [43], построенная средствами языка Python (рис. 16).

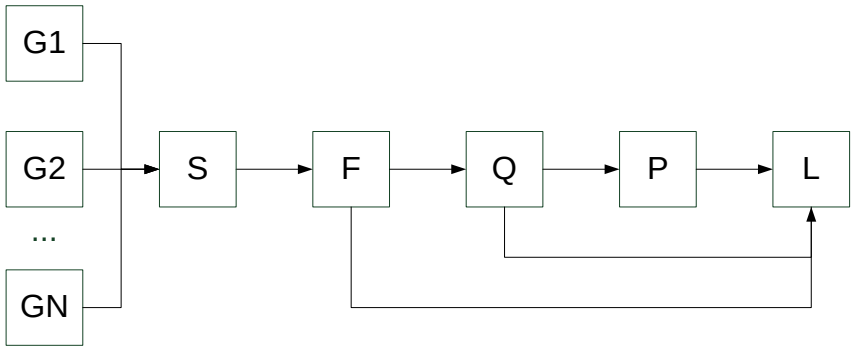


Рис. 16. Сеть массового обслуживания

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

Генераторы потоков создают объекты класса «Поток», которые моделируют пользовательские сессии. Они характеризуются паттернами трафика и его распределениями. Паттерны трафика используются для симуляции потока заявок от легитимных пользователей, распределения – для автоматической генерации потоков. Кроме того, для каждого потока задаётся его длительность.

Диспетчер сессий сохраняет объекты потоков и генерирует запросы для каждого активного потока в соответствии с его параметрами. При генерации

потоков согласно пуассоновскому распределению эта система массового обслуживания имеет классификацию M/D/1 согласно символике Кендалла.

Фильтр реализует меры защиты, которые зависят от конфигурации системы защиты и выбираются из списка, приведённого в главе 1.

Контроллер очереди передаёт запросы обработчику, используя данные об очерёдности, приоритете запросов и стратегий управления. В данном эксперименте использована оптимальная стратегия, определённая в работе [53] для условий работы сервиса интерактивного корпоративного телевидения. Она подразумевает использование очереди для низкоприоритетных заданий и вытеснение в остальных случаях. При моделировании контроллер очереди имеет два варианта реализации – с задержками (M/D/1) и отказами (M/D/1/1).

Обработчик запросов эмулирует дисплей корпоративного телевидения.

Логгер принимает сведения обо всех запросах и их статусе по окончании их обработки и сохраняет эти сведения в базу данных.

При низкой интенсивности запросов вероятность конфликта между запросами низка, и оценка эффекта близка 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, оценка эффекта будет падать. На рис. 17 представлена зависимость значения эффекта от средней интенсивности возникновения запросов λ_R и потоков λ_S при условии, что потоки легитимны:

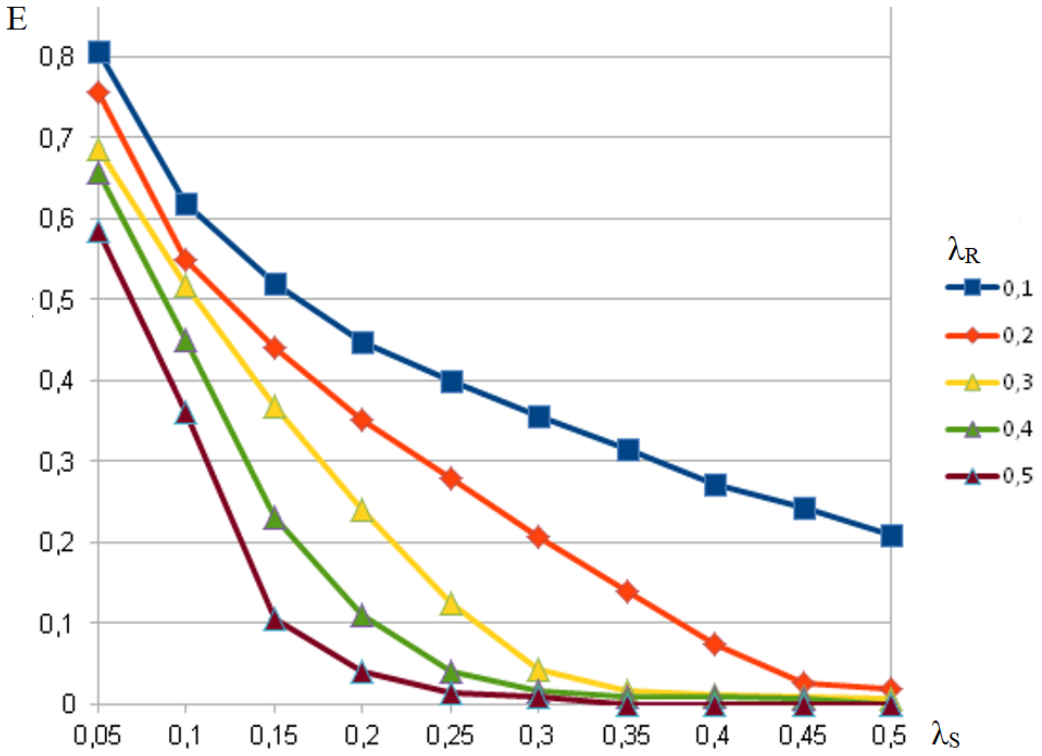


Рис. 17. Зависимость эффекта *E* от λ_R и λ_S

Значение эффекта также значительно снижается при появлении паттернов нелегитимных запросов с интенсивностями λ_M (рис. 18):

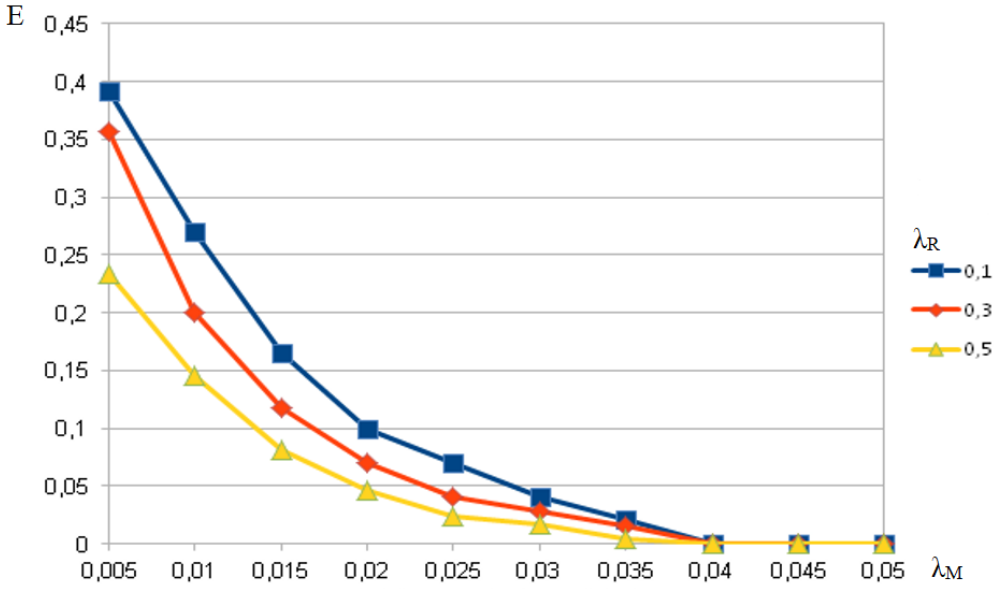


Рис. 18. Зависимость эффекта *E* от λ_R и λ_M (λ_S = 0,1)

Фильтрация позволяет частично устранить нелегитимные запросы и увеличить значения эффекта. Было проведено моделирование для оценки

значений эффекта с использованием фильтрации по разным пороговым значениям статистических моментов и энтропии. Рис. 19 иллюстрирует изменение эффекта при изменении порога оценки математического ожидания для частоты появления запросов. Рис. 20 характеризует ту же величину в зависимости от порога среднеквадратического отклонения. Рис. 21 отражает зависимость эффекта от допустимого нижнего порога энтропии.

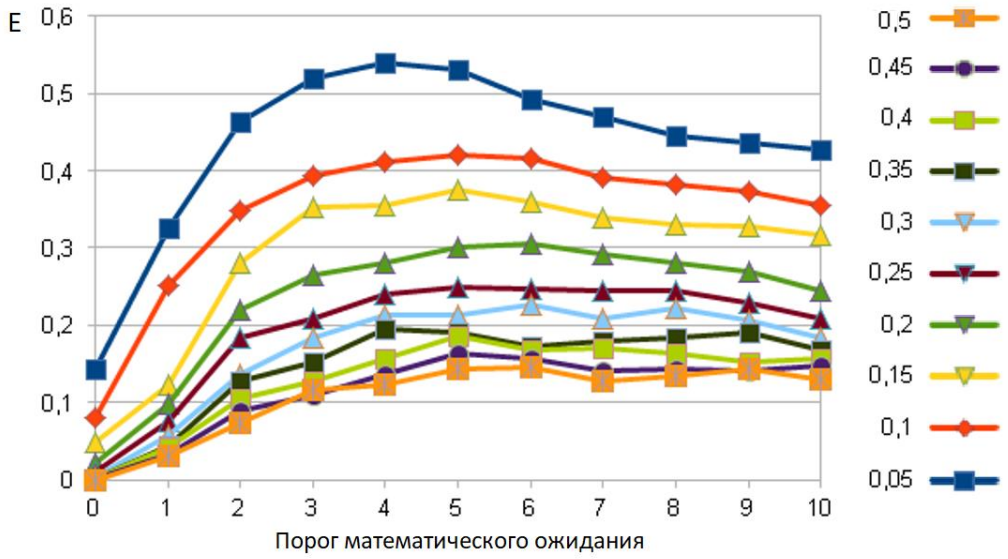


Рис. 19. Зависимость эффекта E от интенсивности запросов λ_R и допустимого порога среднего значения

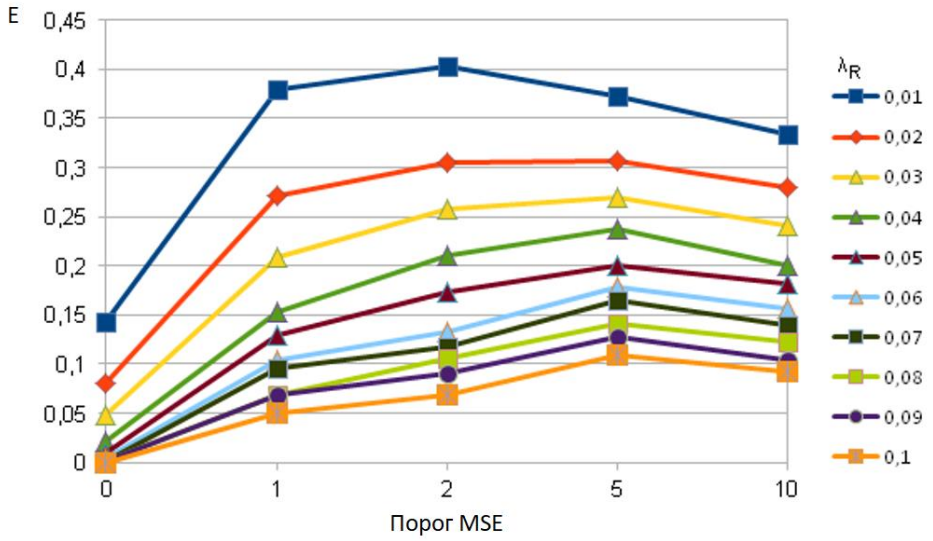


Рис. 20. Зависимость эффекта E от интенсивности запросов λ_R и допустимого порога среднеквадратического отклонения

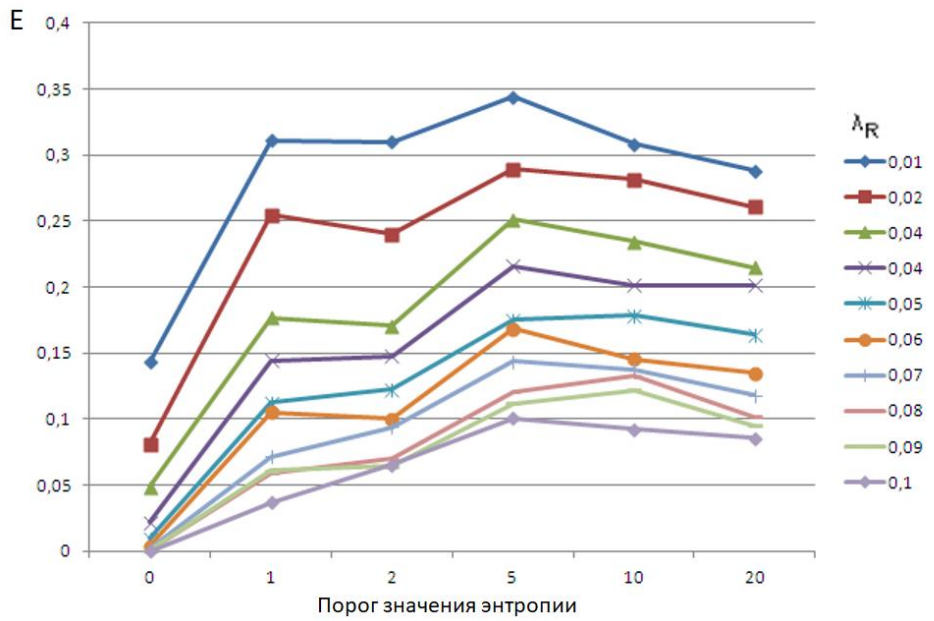


Рис. 21. Зависимость эффекта E от интенсивности запросов λ_R и допустимого порога энтропии

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 $V_z(t)$ для различных состояний ИБ защищаемой системы. Методы, рассмотренные в п. 1.5, позволяют оценить вероятности перехода между состояниями. Таким образом, для изучения поведения системы можно применить модель из п. 2.1.

Рассмотрим более подробно влияние факторов на процессы, протекающие в защищаемой системе. Рис. 22 показывает, каким образом эффект функционирования КИС зависит от внешних факторов, связанных с интенсивностями возникновения угроз в математической модели. В данном случае на начальном этапе функционирования КИС эффект положительный, но в зависимости от значения λ_{65} он может приобрести как восходящий, так и нисходящий тренд.

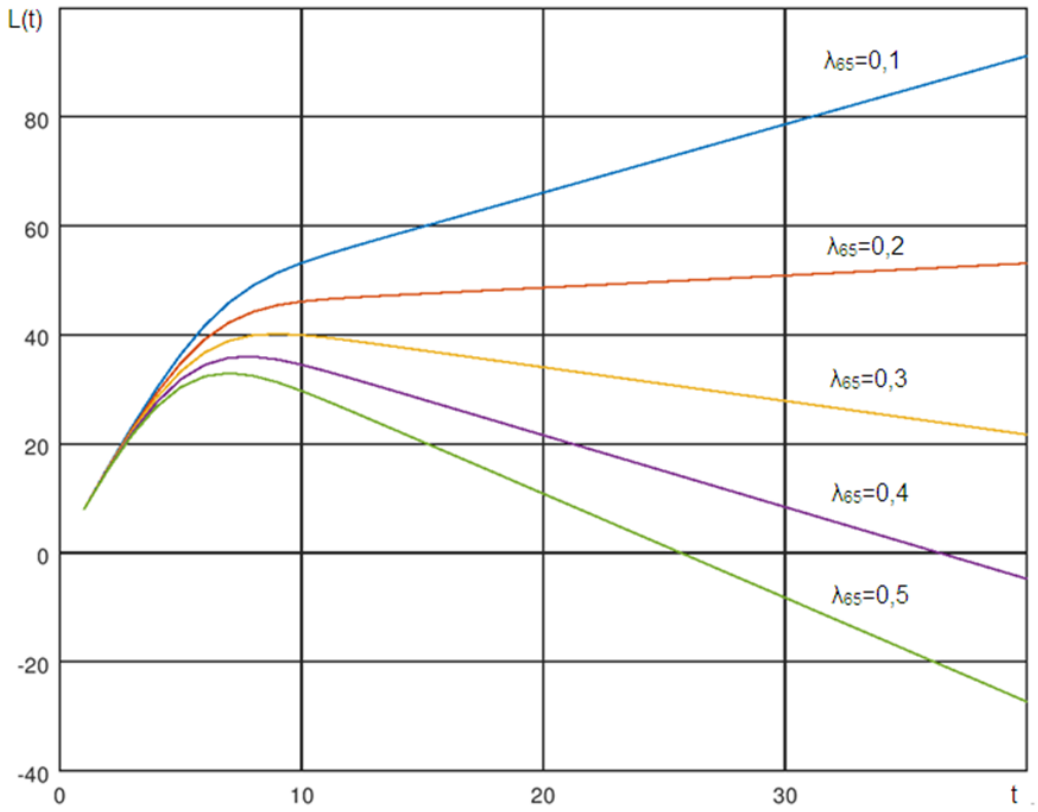


Рис. 22. Зависимость эффекта функционирования КИС от интенсивности возникновения угроз (λ_{65}= 0,1…0.5)

В случае, если на рассматриваемом временном интервале значение совокупного эффекта функционирования КИС не удовлетворяет требованиям предприятия, подходы к обеспечению безопасности должны быть пересмотрены.

Начальные условия функционирования КИС оказывают значительное влияние на динамику эффекта до тех пор, пока система не достигнет установившегося режима. Так, на рис. 23 изображена зависимость эффекта от времени при следующих начальных условиях: $P_5(0)$ = 0,1; 0,3; 0,5; 0,7; $P_6(0)$ = = 1 – $P_5(0)$, т.е. при различных вероятностях наличиня (отсутствия) угрозы в начальный момент времени.

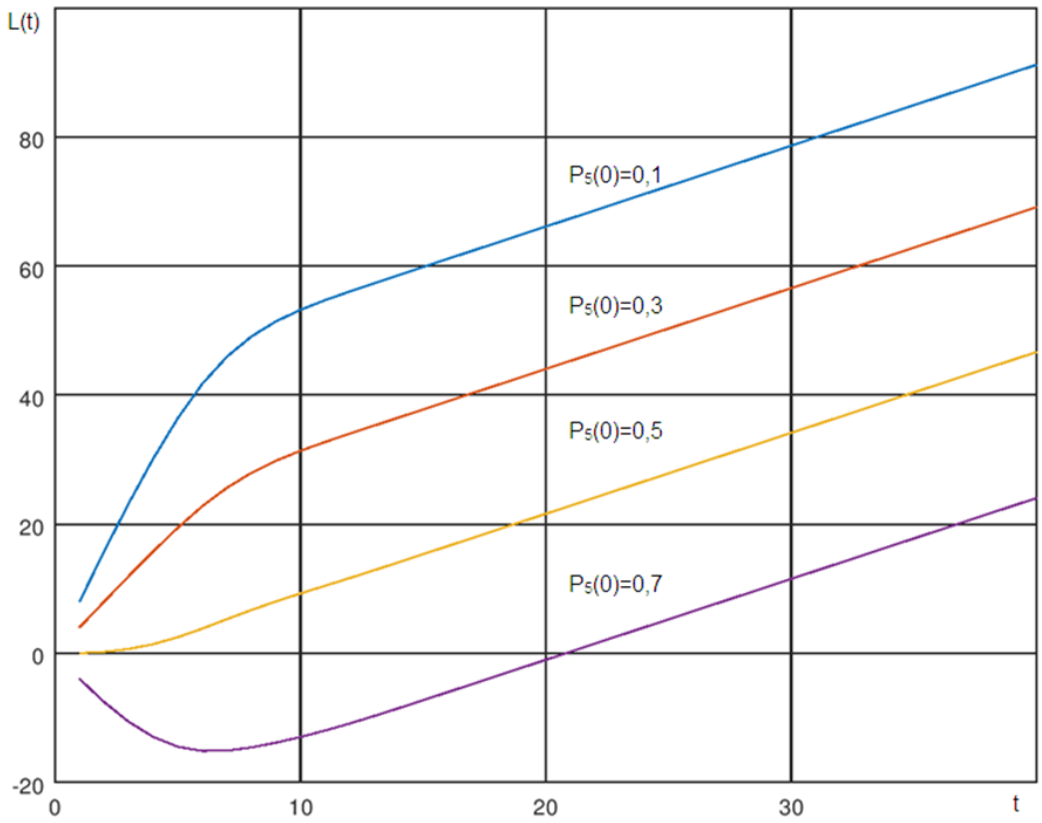


Рис. 23. Эффект функционирования КИС при начальных условиях:

$P_5(0) = 0,1; 0,3; 0,5; 0,7; P_6(0) = 1 – P_5(0)$

Рис. 24 отражает изменение вероятности нахождения в состоянии 6 (остутствие угрозы).

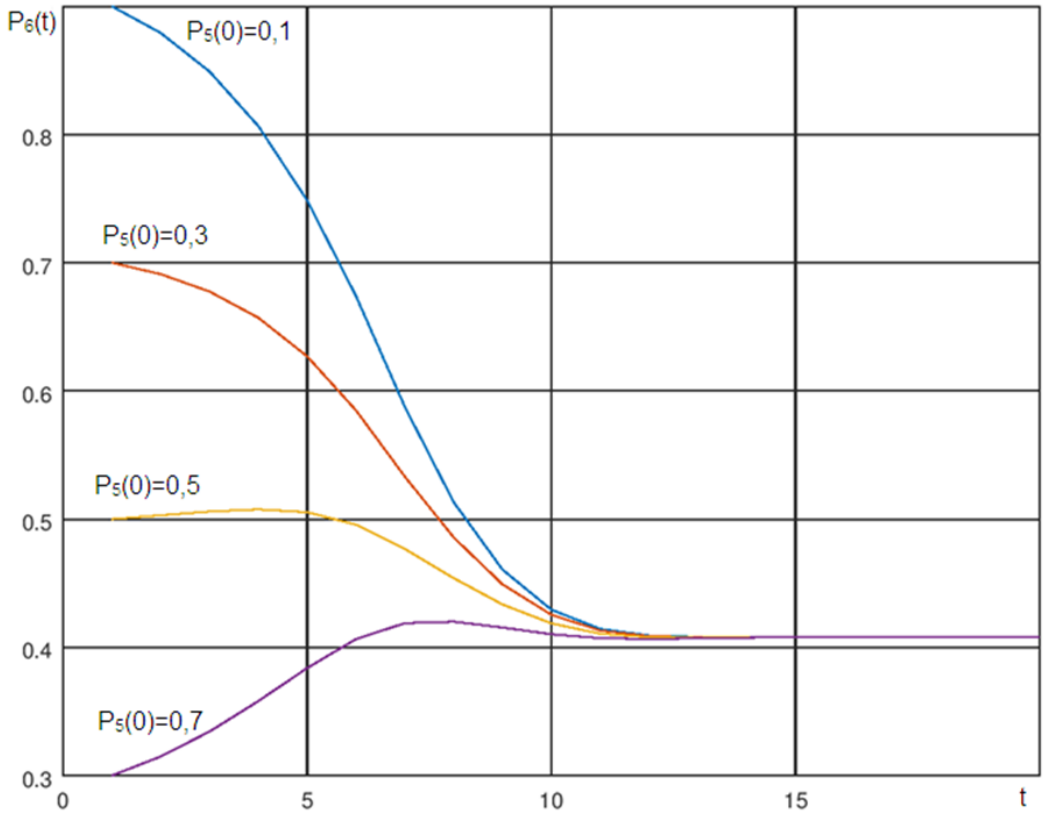


Рис. 24. Зависимость $P_6(t)$ при начальных условиях

$P_5(0) = 0,1; 0,3; 0,5; 0,7; P_6(0) = 1 – P_5(0)$

Рис. 25 отражает изменение эффекта при различных способностях средств защиты КИС обнаруживать деструктивные воздействия.

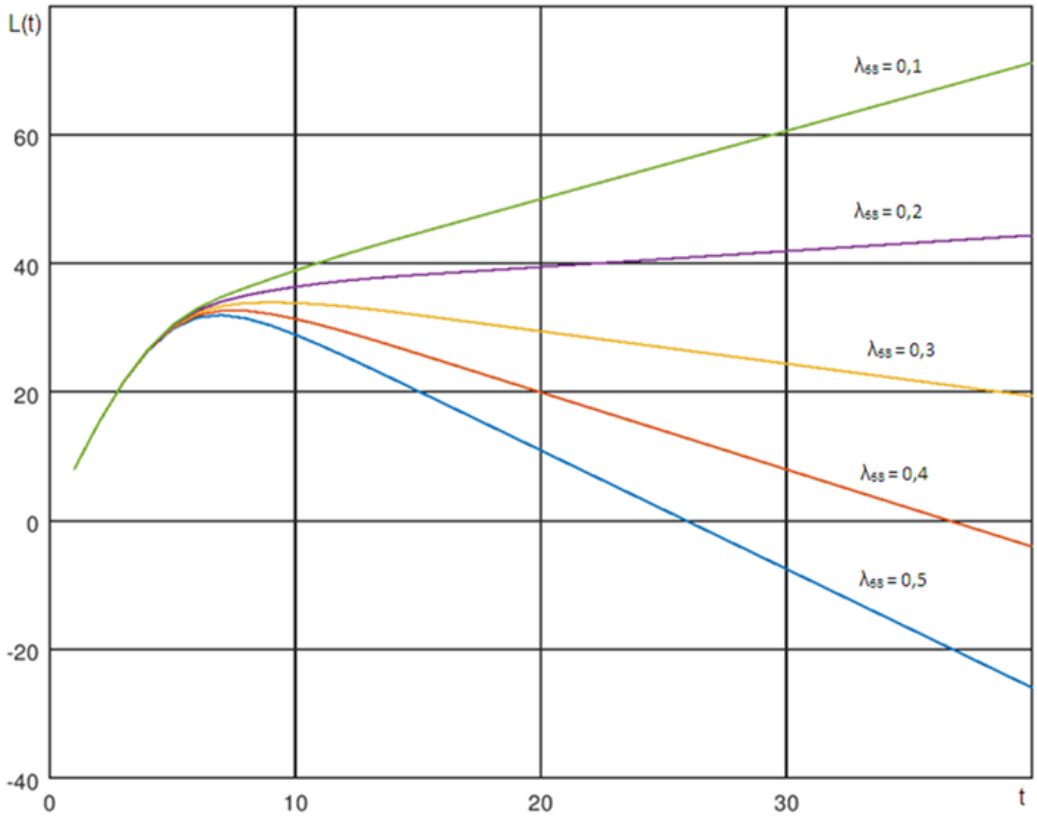


Рис. 25. Кривая эффекта функционирования КИС при $\lambda_{68} = 0,1; 0,2; 0,3; 0,4; 0,5$.

В этом случае вероятность нахождения системы в состоянии активной угрозы зависит от времени, как показано на рис. 26.

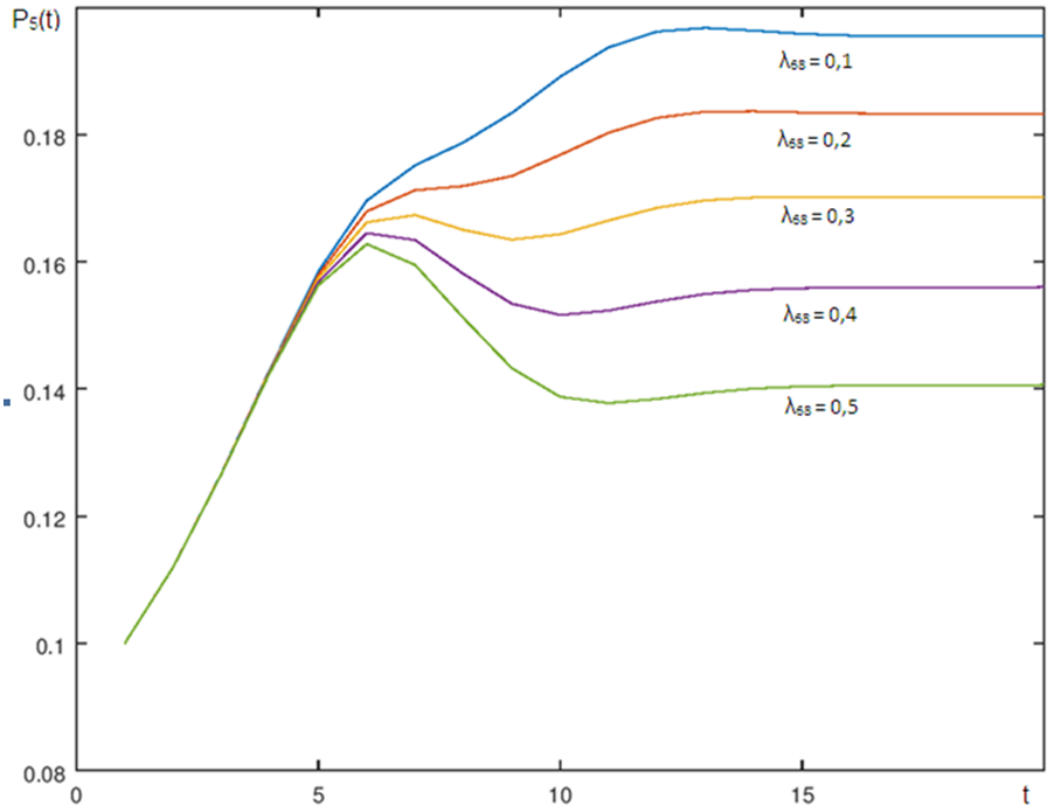


Рис. 26. Зависимость вероятности $P_5(t)$ от времени при $\lambda_{68} = 0,1; 0,2; 0,3; 0,4; 0,5$

График изменения вероятности $P_8(t)$ восприятия деструктивного воздействия показан на рис. 27.

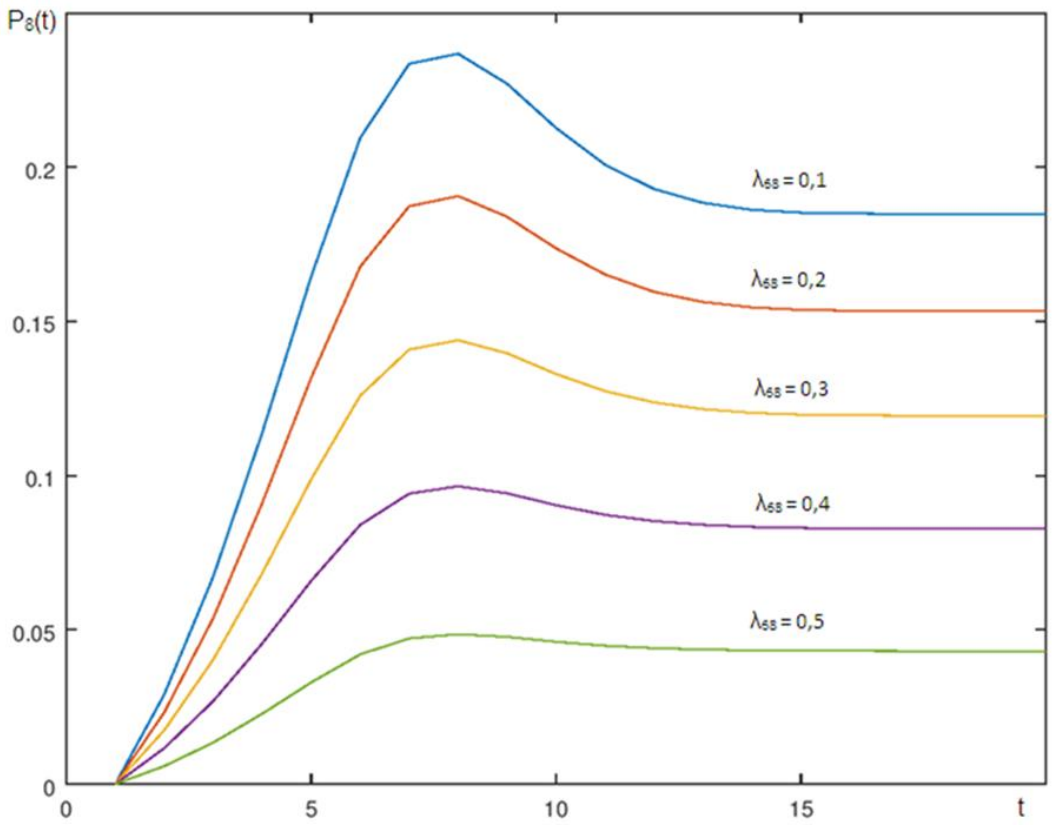


Рис. 27. Зависимость вероятности $P_8(t)$ от времени при условиях λ_{68} = *0,1; 0,2; 0,3; 0,4; 0,5*

Рис. 28 показывает зависимости эффекта от времени на примере двух защитных конфигураций, предполагающих соответственно быстрый и углублённый анализ данных. Если рассмотреть для примера задачу защиты компьютерной сети от DDoS-атак, то к первому типу конфигурации можно отнести методы, основанные на выявлении сетевых аномалий с помощью сигнатур или статистических моментов невысокого порядка. Ко второму типу можно отнести методы, основанные на машинном обучении.

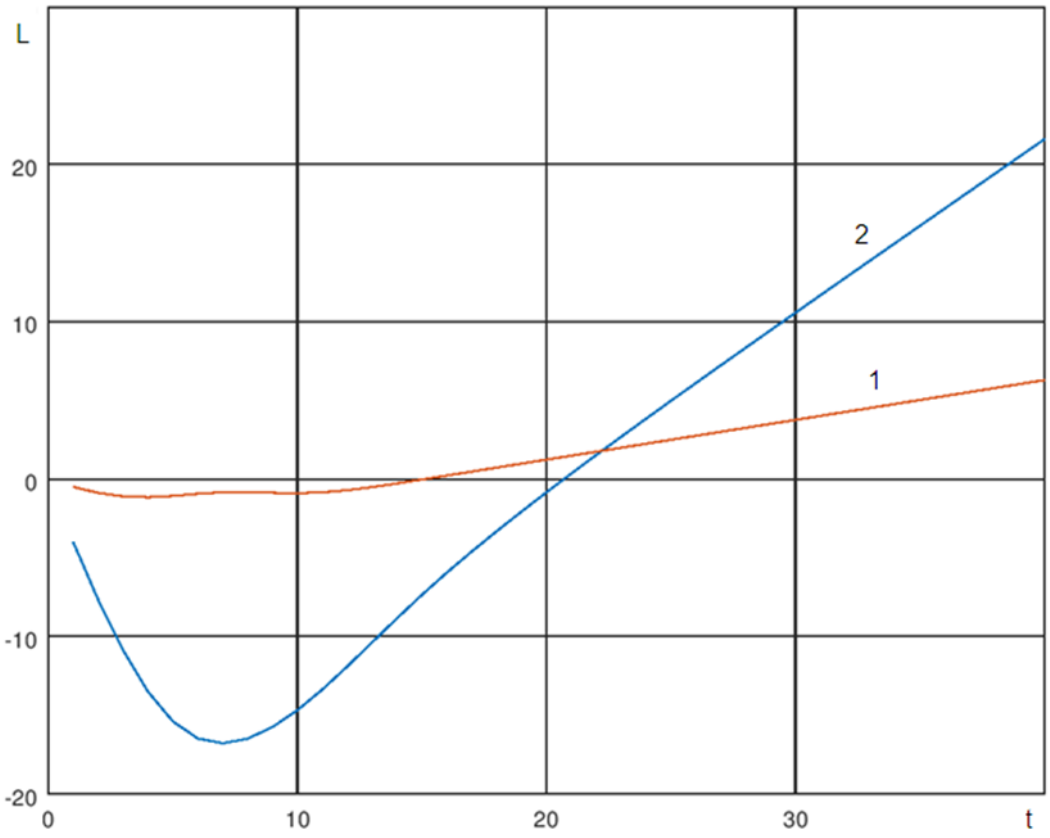


Рис. 28. Величина эффекта при двух защитных конфигурациях: 1 – быстрый анализ входных данных; 2 – углублённый анализ входных данных

Согласно рис. 28, 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. Следует отметить, что моделирование не привязано к

конкретным типам угроз и может применяться для анализа поведения защищаемой системы и при одиночных, и при комплексных деструктивных воздействиях. При этом предложенные модели позволяют также оценить возможное поведение системы при различных сценариях защиты и воздействия.

4.3. Предложения по составу, структуре, математическому и программному обеспечению системы адаптивной защиты КИС

Приведём схему потоков данных, возникающих при выполнении алгоритма выбора оптимальной программы защиты. На рис. 29 модуль конфигурации хранит и предоставляет множество начальных данных. Диспетчер программ хранит и предоставляет доступ к набору $\{PRG_k\}$ реализуемых программ защиты. Фильтр программ тестирует эти программы на соответствие ограничениям, приведённым в п. 3.2. Компонент моделирования и прогнозирования оценивает вероятности нахождения КИС в заданных состояниях в зависимости от времени и позволяет спрогнозировать дальнейшее поведение системы. Компонент оценки эффекта используется, чтобы рассчитать эффект, достигаемый при функционировании КИС в актуальных условиях. Значение этого эффекта используется в качестве целевой функции для выбора оптимальной программы защиты.

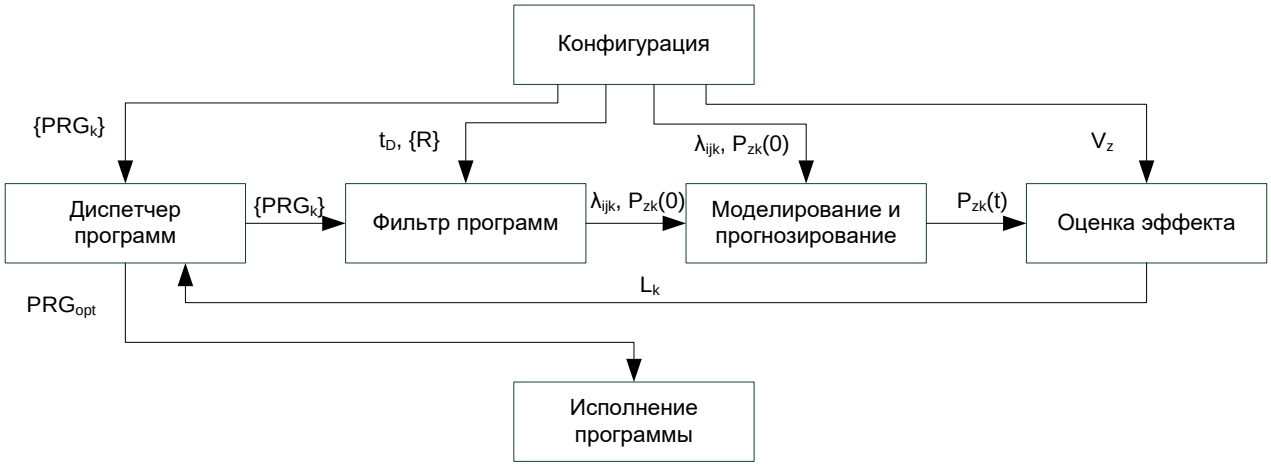


Рис. 29. Диаграмма потоков данных для модуля адаптации

Цикл исполнения выбранной программы защиты проиллюстрирован на рис. 30. Цикл состоит из построения множества заданий по мониторингу данных (диспетчер задач), определения множества источников данных для мониторинга (диспетчер источников), получения данных (коннектор), структуризации данных (парсер), анализа данных с использованием методов,

определённых выбранной программой защиты (анализатор), фильтрации данных (процессор) и передачи данных прикладной системе (КИС) для дальнейшего использования. Цикл содержит обратную связь, данные в которой могут передаваться вручную оператором или автоматически через диспетчер обратной связи.

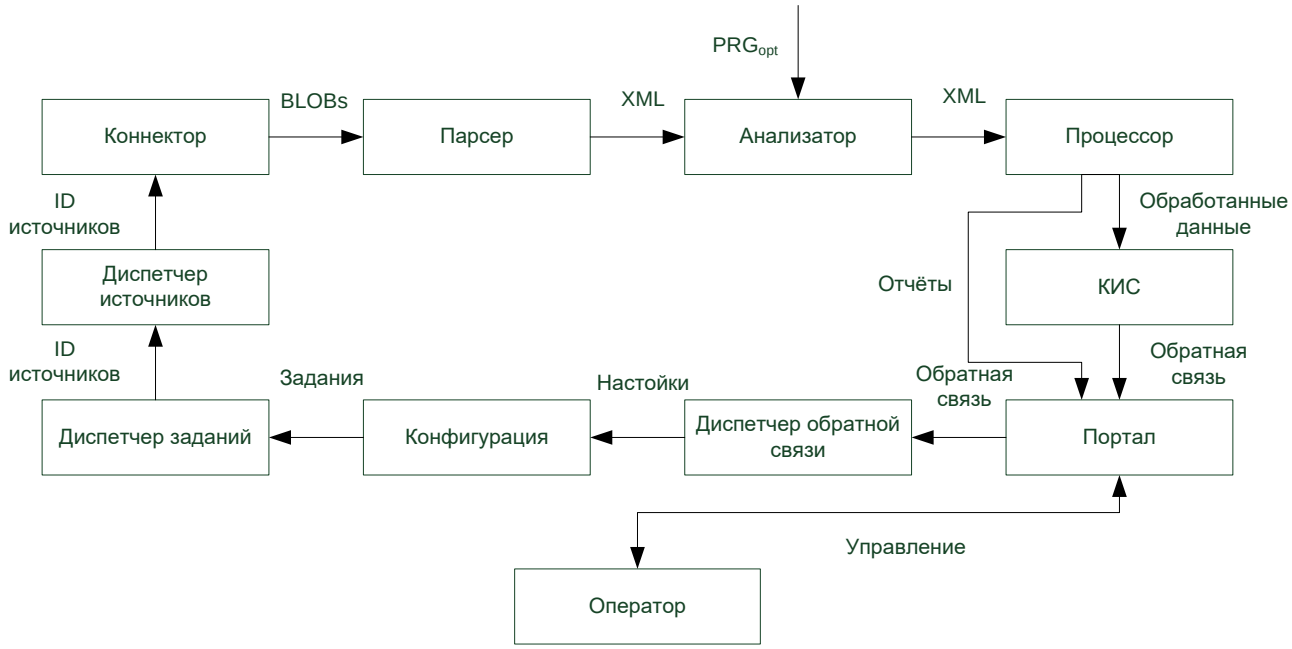


Рис. 30. Диаграмма потоков данных для модуля реализации

Диаграммы на приведённых выше рис. можно использовать для построения иерархии компонентов адаптивной системы защиты КИС. Эта иерархия показана на рис. 31.

Рис. 31. Иерархия компонентов системы защиты

Согласно рис. 31, система защиты состоит из следующих компонентов: модуль конфигурации, который хранит активное состояние системы защиты, модуль адаптации, который корректирует состояние системы для достижения оптимальных значений эффекта, модуль реализации, который исполняет программы конфигурирования системы защиты, и административный интерфейс.

Рассмотрим диаграммы классов, характеризующие структуру отдельных компонентов приложения, построенные с помощью UML [83-84].

На рис. 32 изображена UML-диаграмма, характеризующая структуру классов для компонента «Диспетчер заданий», определяющая его связи с другими компонентами.

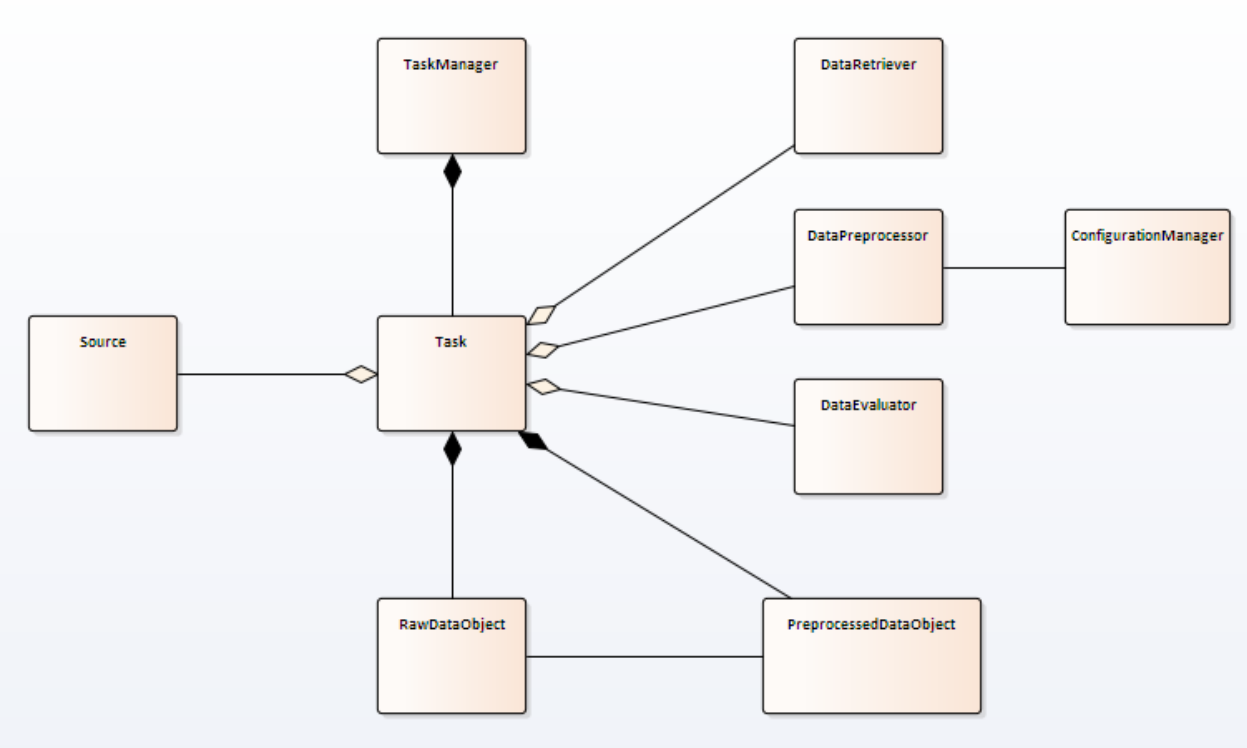


Рис. 32. Диаграмма классов для диспетчера заданий

На рис. 33 изображена аналогичная структура для диспетчера источников данных.

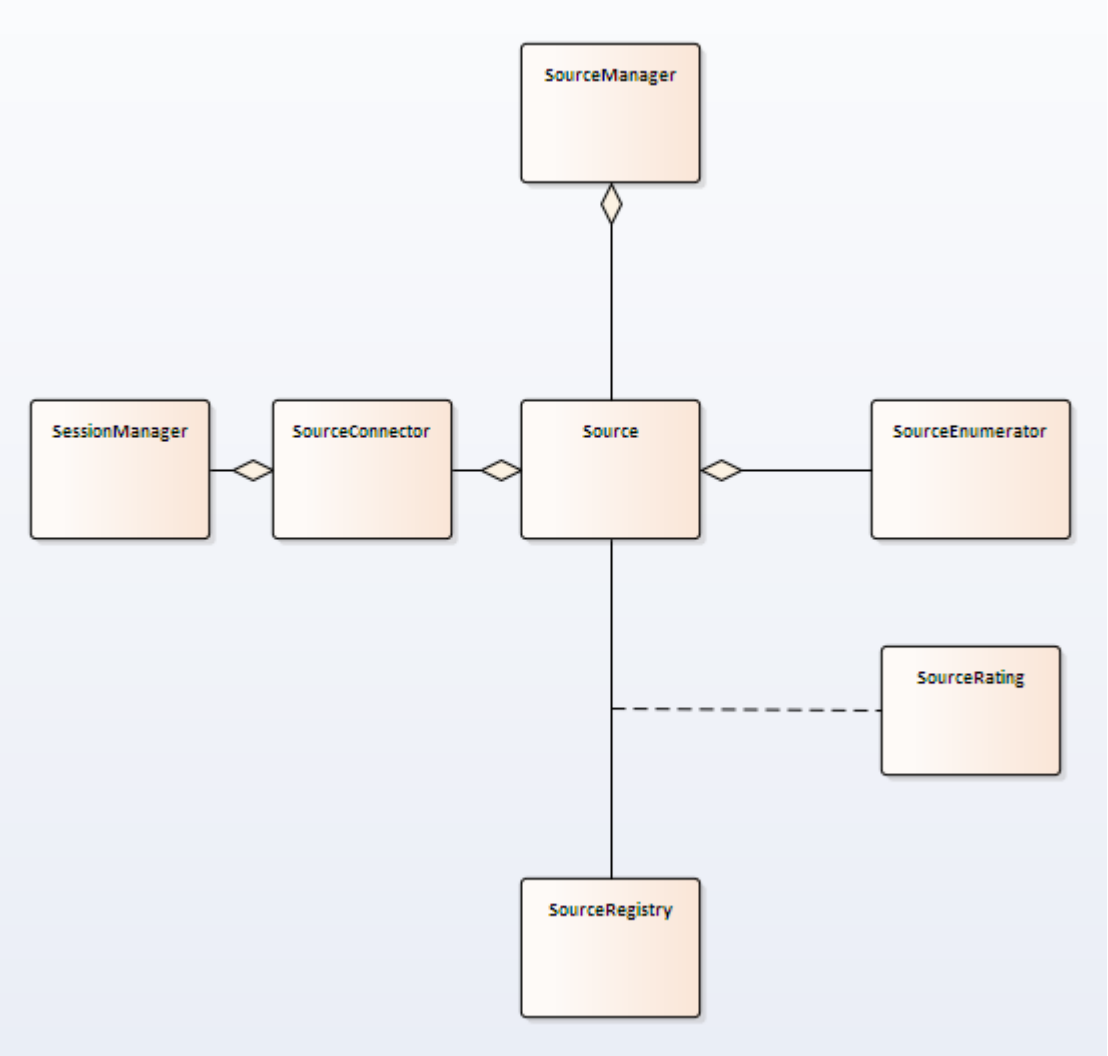


Рис. 33. Диаграмма классов для диспетчера источников данных

4.4. Способ обнаружения компьютерных атак на КИС

Корпоративные информационные системы подвержены компьютерным атакам со стороны злоумышленников. Среди наиболее распространённых типов атак в Интернете – атаки типа “отказ в обслуживании” (Distributed Denial of Service, DDoS), в ходе которых создаются такие условия работы атакуемой системы (например, веб-сервера), при которых обычные, легитимные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен, что выражается в возникновении задержек, сбоев и, как следствие, снижении доступности, падении показателей QoS, QoE.

Приведём некоторые распространённые типы DDoS-атак, описанные в литературе [85-88]:

HTTP-flood [85] – атака, которая заключается в отправке множества HTTP-пакетов, на которые сервер отвечает пакетами, размер которых во много раз больше полученных, для исчерпания вычислительных ресурсов сервера.

SYN-flood [85] – атака, которая заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок.

UDP-flood [86] – атака, которая заключается в отправке большого количества UDP-пакетов на случайные порты атакуемого компьютера (жертвы), в результате чего атакуемый компьютер генерирует ответные ICMP-сообщения.

ICMP-flood [87] – атака, при которой отправляется множество эхо-запросов, требующих от атакуемого компьютера принятия пакета, его обработки и формирования/отправки пакета с ответом на запрос. Объем выполняемых действий при этом многократно превышает объем работы по маршрутизации обычного пакета. В результате, при формальном сохранении небольшого трафика возникает перегрузка по количеству пакетов.

TCP-flood [88] – атака, предусматривающая отправку на конкретный адрес большого количества TCP пакетов, что в результате приводит к “связыванию” ресурсов атакуемого компьютера.

Среди способов защиты информационно-вычислительных сетей от компьютерных атак [90], заключающийся в том, что принимают i-й, где i=1, 2, 3, пакет сообщения из канала связи, запоминают его, принимают (i+1)-й пакет сообщения, запоминают его, выделяют из запомненных пакетов сообщений характеризующие их параметры, сравнивают их и по результатам

сравнения принимают решение о факте наличия или отсутствия компьютерной атаки. При этом при обнаружении фрагментированных пакетов сообщений запоминают их в предварительно созданном массиве и определяют правильность сборки выявленных фрагментированных пакетов сообщений. В случае невозможности правильной сборки фрагментированных пакетов сообщений принимают решение о наличии компьютерной атаки (атака вида “Teardrop”) и запрещают передачу выявленных пакетов сообщений в защищаемую компьютерную сеть.

Недостатком этого способа является специализация только на одном виде атак и, соответственно, невозможность обнаружения атак других видов.

Известен также способ защиты информационно-вычислительных сетей от компьютерных атак [91], заключающийся в том, что

- формируют массив для запоминания фрагментированных пакетов сообщения и массивы для запоминания параметров, выделенных из запомненных пакетов сообщений;
- в качестве выделенных полей из запомненных пакетов сообщений используют поля данных: “Время жизни пакета” {T}, “Опции” {O}, “IP адрес назначения” {D}, “IP адрес источника” {I}, которые запоминают в сформированных для них массивах;
- дополнительно формируют список доверенных адресов получателя и отправителя пакетов сообщений, которые запоминают в массивах эталонных параметров значений полей данных: “IP адрес назначения” {$D_{эт}$} и “IP адрес источника” {$I_{эт}$}, затем
- адаптируют информационно-вычислительную сеть, для чего
    - в тестовом режиме измеряют значения полей данных пакета “Время жизни пакета” и “Опции” для всех

маршрутов между доверенными получателями и отправителем пакетов сообщений;

- запоминают измеренные значения параметров в соответствующих массивах эталонных параметров значений полей данных: “Время жизни пакета” $T_{эт}$, “Опции” $O_{эт}$, после запоминания принятого пакета сообщения, для обнаружения факта атаки или ее отсутствия;

- принимают очередной пакет сообщения из канала связи, запоминают его,
- выделяют из заголовка данного пакета значения полей данных: “Время жизни пакета” T, “Опции” O, “IP адрес назначения” D и “IP адрес источника” I и запоминают их в соответствующих массивах {T}, {O}, {D} и {I};
- сравнивают эталонные значения полей данных “Время жизни пакета”, “Опции”, “IP адрес назначения” и “IP адрес источника” со значениями полей данных из полученного пакета;
- анализируют запомненный пакет на обнаружение факта наличия или отсутствия компьютерной атаки;
- устанавливают факт отсутствия атаки, если эталонные значения полей данных: “Время жизни пакета”, “Опции”, “IP адрес назначения” и “IP адрес источника” совпадают со значениями полей данных из полученного пакета;
- устанавливают факт наличия атаки, если эталонные значения полей данных: “Время жизни пакета”, “Опции”, “IP адрес назначения” и “IP адрес источника” не совпадают со значениями полей данных из полученного пакета;
- при отсутствии компьютерной атаки передают очередной пакет сообщения в информационно-вычислительную сеть;

- а в случае обнаружения компьютерной атаки принимают решение о запрете передачи пакета в информационно-вычислительную сеть;
- удаляют ранее запомненные значения пакетов сообщения из массивов.

В известном способе используется анализ ряда параметров пакетов и сравнение этих параметров с эталонными значениями, полученными в ходе адаптации сетевой компьютерной системы.

Недостатками известного способа являются невозможность обнаружения атак разных видов, а также невозможность обнаружения комбинированных одновременных атак и определения вида атак.

Предложенный способ [78] обеспечивает возможность обнаружения компьютерных атак разных видов, комбинированных одновременных атак разных видов и определения видов атак.

Для этого предлагается способ, в котором для анализа получаемых из сети пакетов выбираются определенные параметры и вычисляются их значения, которые затем сравниваются с эталонными значениями, а факт наличия одиночной или комбинированной одновременной атаки и определение видов атак определяется по сочетанию установленных условий для параметров.

Для обработки получаемых из сети пакетов данных используется система анализа трафика, входящая в состав компьютерной системы и позволяющая вычислять параметры трафика в реальном масштабе времени.

Для использования в предлагаемом способе выбираются параметры трафика, инвариантные к изменению величины легального трафика, но чувствительные к появлению DDoS-атак. Все параметры вычисляются за единицу времени.

Исследования [89] показали, что в качестве таких параметров целесообразно выбрать следующие.

Отношение входящего и исходящего трафика

$$R_{IP} = V_{IN} / V_{OUT},$$

где V_{IN}- объем входящего трафика, принятого по протоколу IP;

V_{OUT}- объем исходящего трафика, отправленного по протоколу IP.

Повышение скорости входящего трафика без соразмерного повышения скорости исходящего трафика ведет к росту величины R_{IP}, что означает более высокую вероятность наличия атаки. Как правило, входящий трафик Web-сервера представляет собой набор кратких HTTP-запросов, а исходящий – большое количество Web-страниц и мультимедийных данных. Поэтому величина R_{IP} в нормальном режиме должна быть меньше единицы, а продолжительное превышение входящего трафика над исходящим в 2 и более раз может рассматриваться как один из признаков атаки.

Количество потоков критических приложений N_{CR} используется для обнаружения атак прикладного уровня.

Наиболее частой задачей сетевой информационной системы является обработка поступающих по сети запросов пользователей, для чего в компьютере используются соответствующие критически важные программы (приложения). Такие приложения обычно выполняются в несколько потоков, общее количество которых для компьютера конкретной конфигурации может быть велико, но, тем не менее, ограничено некоторым максимальным значением. При возникновении атаки величина N_{CR} возрастает, соответственно, признаком наличия атаки может быть нахождение величины N_{CR} в районе своего максимума.

Так, для сетевой информационной системы в виде Web-сервера характерной задачей является обработка HTTP-запросов, выполняемая серверными процессами (например, httpd, nginx), поэтому целесообразно измерять число их потоков N_{CR} . Если Web-сервер обращается к другим приложениям (например, к базе данных или системе инженерных вычислений), следует измерить количество потоков и этих приложений. Стандартная конфигурация сервера, например, для широко распространенного серверного ПО Apache v.2.2.22, ограничивает количество потоков до 150, поэтому опасность представляет близость N_{CR} к этому значению.

Разность

$$d_{ACK} = N_{OUT} - N_{IN},$$

где N_{OUT} - количество исходящих ACK-флагов в TCP-трафике;

N_{IN} - количество входящих ACK-флагов в TCP-трафике.

Этот параметр характеризует, как часто сервер отказывает клиенту из-за перегрузки. Эта величина имеет ценность для различных видов атак, в особенности для SYN-flood и HTTP-flood. Результаты экспериментов показывают, что при наличии атаки SYN-flood отклонение d_{ACK} от нуля превышает 100. Значительное отклонение модуля d_{ACK} от нуля

$$D_{ACK} = | d_{ACK} |,$$

является признаком дисбаланса трафика и может свидетельствовать о DDoS-атаке.

Отношение

$$R_{UDP} = V_{UDP} / V_{TCP},$$

где V_{UDP} - объем входящего UDP-трафика;

V_{TCP} - объем входящего TCP-трафика.

Этот параметр может характеризовать наличие атаки класса UDP-flood. Хотя в трафике Web-сервера присутствует небольшое количество пакетов, принадлежащих этому протоколу, в целом UDP-трафик для HTTP-соединений является нехарактерным, поэтому превышение UDP-трафика над TCP-трафиком, выражающееся в увеличении R_{UDP}, позволяет выявить UDP-flood. Порог для R_{UDP} может варьироваться, так как это значение определяется потенциальной мощностью атаки, которую система должна обнаруживать, и его выбор представляет собой компромисс, минимизирующий вероятность, как ложной тревоги, так и пропуска атаки. Величина порога должна быть больше 1, так как в ином случае система может принять за атаку легальный трафик, и иметь некоторый запас, чтобы не реагировать на случайные отклонения. В силу этих причин порог для R_{UDP} устанавливается равный 10.

Отношение

$$R_{NUD} = N_{UDP} / N_{TCP,}$$

где N_{UDP} – количество входящих UDP-пакетов;

N_{TCP} – количество входящих TCP-пакетов.

Этот параметр отражает уровень загрузки канала трафиком, полученным по протоколу UDP.

Отношение

$$R_{ICM} = V_{ICM} / V_{IN},$$

где V_{ICM} - объем входящего трафика, полученного по протоколу ICMP.

Этот параметр отражает загруженность трафика служебными пакетами. Если величина служебного трафика сравнима по величине с другими видами трафика (что означает, что ICMP-трафик представляет собой половину всего трафика и что $R_{ICM} \approx 0,5$) или превышает их (т. е. $R_{ICM} \geq 0,5$), то этот факт может рассматриваться как признак ICMP-flood.

Относительные доли флагов SYN и PSH во входящих пакетах позволяют определить эффективность передачи данных:

$$R_{SYN} = N_{SYN} / N_{TCP},$$

$$R_{PSH} = N_{PSH} / N_{TCP},$$

где N_{SYN}- количество SYN-флагов во входящих пакетах, переданных по протоколу TCP;

N_{PSH}- количество PSH-флагов во входящих пакетах, переданных по протоколу TCP;

Пакеты с флагом SYN пересылаются между клиентом и сервером в ходе установления TCP-соединения, после чего начинается обмен данными с помощью пакетов без SYN-флага. Таким образом, количество SYN-флагов, пришедших на сервер, равно числу запросов на соединение, а относительная доля SYN-флагов определяет относительную долю служебных пакетов этого типа в TCP-трафике.

Установленный флаг PSH означает, что данные, содержащиеся в пакете, должны быть переданы программе прикладного уровня. В случае Web-сервера эти данные представляют собой HTTP-запросы и HTTP-ответы, содержащие Web-страницы. Поэтому относительная доля PSH-флагов, напротив, характеризует полезную загрузку канала.

При атаке класса SYN-flood субъект атаки не намерен передавать какие-либо данные серверу и пытается перегрузить его очередь соединений с

помощью служебных пакетов. Поэтому относительные доли флагов SYN и PSH изменяются.

Изменение эффективности использования сети с учетом обоих типов флагов отслеживается с помощью параметра

$$R_{SP} = R_{SYN} / R_{PSH} = N_{SYN} / N_{PSH}$$

Значение параметра увеличивается как при увеличении R_{SYN}, так и при уменьшении R_{PSH}, поэтому SYN-flood проще отследить с помощью R_{SP}. О наличии SYN-flood может говорить многократное превышение количества флагов SYN над PSH. Предельным для легального трафика значением R_{SP} является 1, что говорит в среднем об одной передаче данных на одно подключение к серверу. Значения R_{SP} большие 1, говорят о том, что к серверу производятся подключения без последующей передачи данных.

Отношение

$$R_{TCP} = N_{PSH} / (N_{TCP} - N_{PSH})$$

характеризует степень полезной загрузки канала данными прикладных программ, которая резко падает при SYN-flood и повышается при TCP-flood. Значения, близкие к нулю, означают, что при большом объеме TCP-трафика передача полезных данных минимальна (при R_{TCP} = 0,05 на 1 пакет с прикладными данными приходится 20 служебных). Это соотношение означает, что канал сервера перегружен служебными пакетами, что может быть следствием атаки.

Средняя длина принятого IP-пакета

$$L_{AVG} = V_{IN} / N_{IP},$$

где N_{IP} - количество входящих пакетов, передаваемых по протоколу IP.

Этот параметр позволяет выявить факт атаки в следующих случаях:

если L_{AVG} приближается к минимальному значению (около 65 байт - пакет с такой длиной не содержит данных, а состоит только из обязательных заголовочных структур), это говорит о перегрузке сервера служебными пакетами, что характерно для SYN-flood и ICMP-flood;

если L_{AVG} приближается к максимальному значению (около 1,5 Кбайт - это значение обусловливается ограничениями на размер кадра Ethernet для его надежной передачи по физическому каналу), это говорит о попытке перегрузить канал передачи данных сервера и может быть результатом UDP-flood, TCP-flood или HTTP-flood.

Средняя длина принятого TCP-пакета

$$L_{TCP} = V_{TCP} / N_{TCP}$$

Этот параметр позволяет выявить SYN flood. Если L_{TCP} приближается к минимальному значению (около 65 байт - пакет с такой длиной не содержит данных, а состоит только из обязательных заголовочных структур), это говорит о перегрузке сервера служебными пакетами, что характерно для SYN-flood.

Для снижения влияния отдельных случайных выбросов после вычисления значений параметров целесообразно проводить некоторое усреднение величин, снижая влияние шума. Для этого вполне пригодным является метод вычисления скользящего среднего (СС) для всех параметров. Расчет СС выполняется по известной формуле [7]

$$\overline{R}_{m+n} = \frac{\sum_{i=m}^{m+n} R_i}{n},$$

где m – начальный момент вычисления скользящего среднего,

n – длина окна (т. е. временной промежуток, на котором производится вычисление).

Важным является определение пороговых (эталонных) значений для рассмотренных параметров. Такое определение может быть проведено несколькими методами. Так, в известном способе, принятом за прототип, пороговые значения определяются в результате адаптации системы, т.е. путем первоначальной работы системы в обычном режиме эксплуатации, но при заведомом отсутствии атак.

В предлагаемом способе возможен и использовался другой метод, предусматривающий исходное логико-аналитическое определение значений параметров с последующей экспериментальной проверкой. Результаты определения пороговых значений параметров приведены в табл. 11.

Таблица 11. Пороговые значения параметров

Условие для параметра	Виды атак, при которых выполняется условие
$R_{IP} > 2$	Все
$R_{SP} > 10$	SYN
$R_{UDP} > 10$	UDP
$R_{NUD} > 5$	UDP
$R_{TCP} > 10$	TCP
$R_{TCP} < 0.05$	SYN
$D_{ACK} > 100$	SYN, TCP
$L_{AVG} < 65$	SYN, ICMP
$R_{ICM} > 0,5$	ICMP
$N_{CR} > 140$	HTTP
$L_{TCP} < 65$	SYN

Повышение вероятности обнаружения атаки достигается также рассмотрением приведенных выше параметров в совокупности. Так как характер влияния каждого вида атаки на параметры известен и отличается от

влияния других классов атак, представляется возможным не только определить факт атаки, но и определить ее вид.

Для обнаружения атак используются пороговые значения параметров путем сравнения текущего значения СС параметра с пороговым значением. Результаты выполнения условий для пороговых значений параметров в ходе одиночных атак различного вида приведены в табл. 12 (знак V указывает на выполнение соответствующего условия).

Таблица 12. Выполнение условий для пороговых значений параметров в ходе одиночных атак различного вида

Параметр	HTTP-flood	SYN-flood	TCP-flood	UDP-flood	ICMP-flood
$R_{IP} > 2$	V	V	V	V	V
$N_{CR} > 140$	V				
$D_{ACK} > 100$		V	V		
$R_{UDP} > 10$				V	
$R_{NUD} > 5$				V	
$R_{ICM} > 0,5$					V
$R_{SP} > 10$		V			
$R_{TCP} > 10$			V		
$R_{TCP} < 0,05$		V			
$L_{AVG} < 65$					V
$L_{TCP} < 65$		V			

Таким образом, предложенный набор параметров позволяет определить наличие одиночных атак разных видов и вид атаки.

Помимо этого, предложенный набор параметров и их пороговых значений позволяет также определить наличие одновременных комбинированных атак разных видов и виды применяемых атак. Результаты выполнения условий для пороговых значений параметров в ходе одновременных комбинированных атак различного вида приведены в табл. 13.

Таблица 13. Выполнение условий для пороговых значений параметров в ходе одновременных комбинированных атак различного вида

Параметр	HTTP+SYN flood	HTTP+TCP flood	HTTP+ICMP flood	SYN+ICMP flood	TCP+ICMP flood
$R_{IP} > 2$	V	V	V	V	V
$N_{CR} > 140$	V	V	V		
$D_{ACK} > 100$	V	V		V	V
$R_{ICM} > 0,5$			V	V	V
$R_{SP} > 10$	V			V	
$R_{TCP} > 10$		V			V
$R_{TCP} < 0,05$	V			V	
$L_{AVG} < 65$			V	V	V
$L_{TCP} < 65$	V			V	

Таким образом, предложенный набор параметров позволяет достичь при его использовании заявленный технический результат и обеспечить возможность обнаружения одиночных компьютерных атак разных видов, комбинированных одновременных атак разных видов и определения видов атак.

Можно непосредственно определить наличие и вид одиночной компьютерной атаки по сочетанию рассчитанных значений параметров на основе следующих условий:

если значения параметров R_{IP} и N_{CR} превысили пороговое значение, то определяется атака типа HTTP-flood (условие 1);

если значения параметров R_{IP}, D_{ACK} и R_{SP} превысили пороговое значение, а R_{TCP} и L_{TCP} меньше порогового значения, то определяется атака типа SYN-flood (условие 2);

если значения параметров R_{IP}, R_{TCP} и D_{ACK} превысили пороговое значение, то определяется атака типа TCP-flood (условие 3);

если значения параметров R_{IP}, R_{UDP} и R_{NUD} превысили пороговое значение, то определяется атака типа UDP-flood (условие 4);

если значения параметров R_{IP} и R_{ICM} превысили пороговое значение, а L_{AVG} меньше порогового значения, то определяется атака типа ICMP-flood (условие 5).

Наличие комбинированной компьютерной атаки и виды одновременно применяемых атак можно определить по сочетанию рассчитанных значений параметров на основе следующих условий:

если одновременно выполняется условие 1 и условие 2, то определяется комбинированная атака HTTP-flood и SYN-flood;

если одновременно выполняется условие 1 и условие 3, то определяется комбинированная атака HTTP-flood и TCP-flood;

если одновременно выполняется условие 1 и условие 5, то определяется комбинированная атака HTTP-flood и ICMP-flood;

если одновременно выполняется условие 2 и условие 5, то определяется комбинированная атака SYN-flood и ICMP-flood;

если одновременно выполняется условие 3 и условие 5, то определяется комбинированная атака TCP-flood и ICMP-flood.

4.5. Типовые ситуации и мероприятия защиты

Представим в таблице 14 типовые ситуации, в которых разработанные методы, модели и технические решения могут быть применены.

Табл. 14. Типовые задачи и ситуации

№	Задача	Пример ситуации	Источник угрозы	Используемые методы и модели
1	Противодействие целенаправленным деструктивным воздействиям на КИС	Атака «отказ в обслуживании» (DoS)	Пользователь, который может быть как легитимным, так и нелегитимным	Предложения по новым способам защиты (п. 3.2)
2	Противодействие	Исчерпание	Легитимный	Метод

№	Задача	Пример ситуации	Источник угрозы	Используемые методы и модели
	нецеленаправленным деструктивным воздействиям на КИС	пропускной способности канала передачи данных	пользователь	оценивания эффективности защиты
3	Противодействие ошибочному восприятию сервисами поступающих заявок	Обработка ошибочно воспринятых данных при использовании многомодальных средств человеко-машинного взаимодействия	Программное обеспечение	Метод оценивания эффективности защиты. Метод адаптивной защиты.

Для примера рассмотрим более подробно задачу №2, связанную с противодействием нецеленаправленным воздействиям на сервисы КИС, в результате которых может быть нарушена их доступность, на примере сервиса интерактивного корпоративного телевидения, выполняющего доставку контента по запросам пользователей на мобильные приложения и экраны. Используем модель, приведённую в п. 4.1, и показатель эффекта, рассмотренный в п. 2.4.

В качестве альтернативных программ защиты рассматривается множество стратегий управления заявками, которые можно представить в виде набора действий $<A_H, A_E, A_L>$, выполняющихся соответственно при

более высоком, равном или более низком приоритете конфликтующей заявки. При этом оптимальность той или иной стратегии зависит от характера потока запросов и передаваемых данных.

Для примера приведём оценку эффективности сервиса при разных стратегиях управления заявками. Рис. 34 иллюстрирует, что при низкой интенсивности возникновения пользовательских запросов предпочтительно использование очереди, а при более высоких значениях – стратегии с отказами. Т.е. оптимальная конфигурация сервиса может измениться со временем при изменении условий функционирования сервиса, в данном случае – интенсивности запросов.

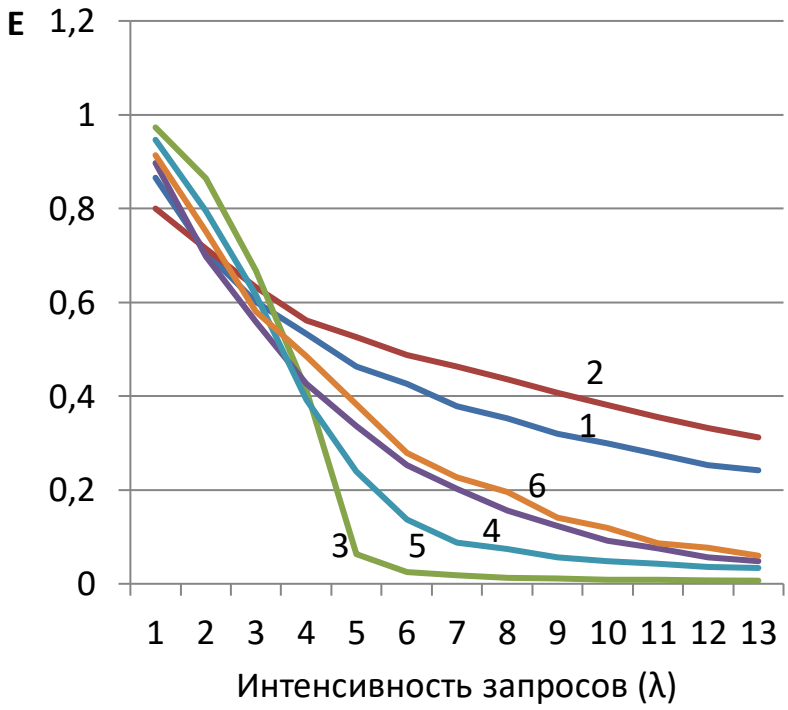


Рис. 34. Зависимость эффекта при различных стратегиях управления запросами

На рис. 34 используются следующие обозначения стратегий: 1 – отклонение новой заявки; 2 – отклонение конкурирующих заявок; 3 – очередь FIFO; 4 – очередь LIFO; 5 – очередь FIFO (максимальная задержка 1); 6 – очередь LIFO (максимальная задержка 1).

Для адаптивного управления конфигурацией сервиса используем метод, описанный в пп. 2.1-2.4. Графики полученного эффекта для трёх стратегий без применения предложенного метода и для применения этого метода приведены на рис. 35.

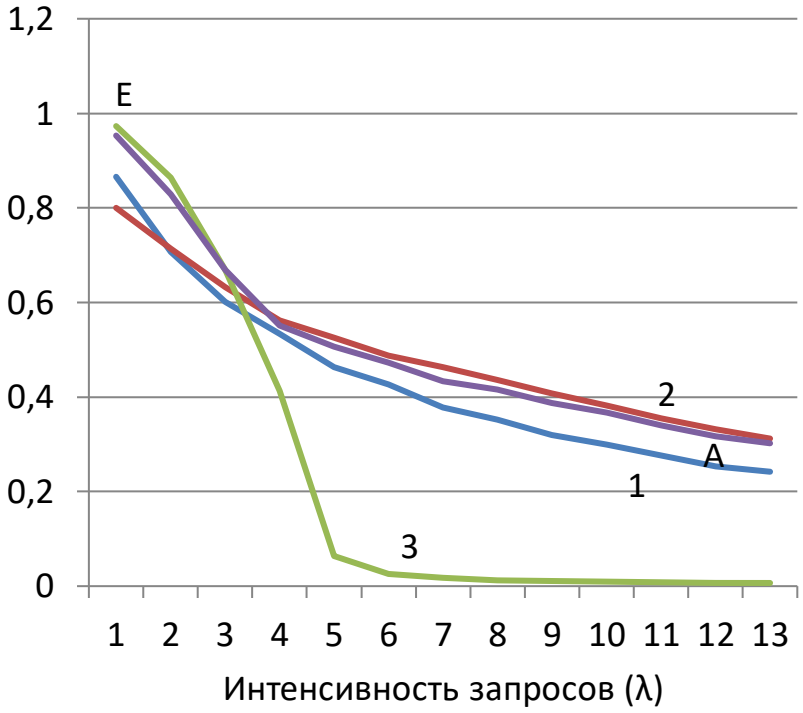


Рис. 35. Достигаемый эффект в зависимости от интенсивности запросов при использовании статических стратегий (1, 2, 3) и предложенного метода (A)

Рис. 36 демонстрирует отклонение ΔE, которое для *i*-го решения вычисляется как:

$$\Delta E_i = \max_i E_i - E_i$$

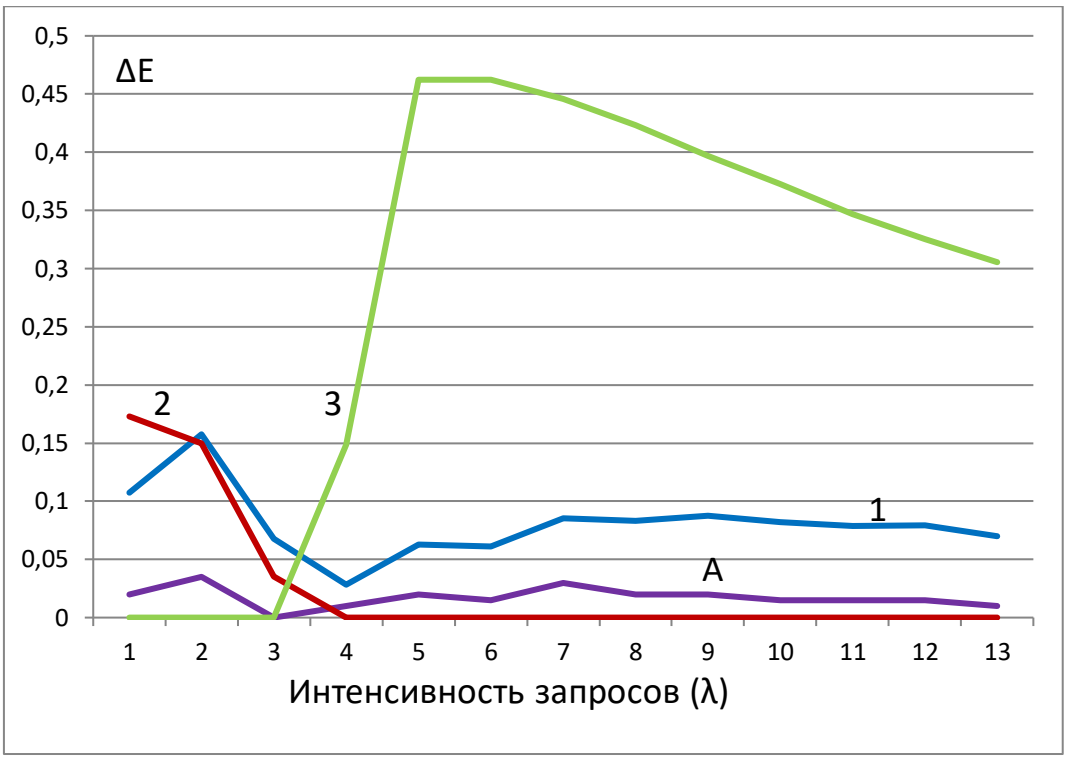


Рис. 36. Отклонение эффектов от максимальных значений

В табл. 15 показаны значения среднеквадратических отклонений полученного эффекта от максимально достижимого эффекта при использовании рассмотренных стратегий.

Табл. 15. Среднеквадратические отклонения эффекта от максимального значения

Используемая стратегия	**Среднеквадратическое отклонение**
1	0,31
2	0,23
3	1,20
A (Адаптивное управление)	0,07

Проведение экспериментов показывает, что хотя для каждого значения интенсивности возникновения запросов использование предложенного

метода показывает несколько меньший эффект по сравнению с методом, оптимальным в данных условиях, но в среднем использование предложенного метода позволяет достичь наименьшего отклонения от максимально возможного значения эффекта в разных условиях функционирования системы.

4.6. Выводы

Предложенная архитектура программной системы адаптивной защиты корпоративной информационной системы от комплексных информационных угроз отличается новой совокупностью функциональных блоков и их связей и может быть использована в перспективных системах защиты информации, реализующих предложенные методы и модели.

Также предложен способ обнаружения атак на компьютерные системы, особенность которого состоит в возможности противодействия комплексным атакам. Предложены типовые сценарии применения мероприятий защиты в различных ситуациях информационной безопасности – при наличии целенаправленных и нецеленаправленных деструктивных воздействий, технических ошибок. Проведено моделирование, показывающее работоспособность предложенных решений.

Предложенные решения позволяют качественно оценивать процессы, протекающие в защищаемых системах. Они позволяют обосновывать целесообразные мероприятия в области управления данными при защите прикладных систем от комплексных информационных угроз. Данные решения могут быть использованы как для планирования и осуществления противодействия вредоносным воздействиям, так и для оперативного управления информационной безопасностью систем. В частности, рассмотренные 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 защитных программ для противодействия угрозам в этих организациях. Эта возможность обоснована соответствием результатов моделирования общим закономерностям.

Заключение

Совокупность предложенных моделей, методов и средств, а также их практическая реализация представляют собой решение научной задачи повышения эффективности защиты корпоративных информационных систем от комплексных деструктивных информационных воздействий, имеющей важное значение для развития технологий в области информационной безопасности, в том числе были получены следующие 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.

Рекомендации, перспективы дальнейшей разработки темы. Построенные модели позволяют количественно оценивать процессы, протекающие в защищаемых КИС и выполнять высокоуровневую формализацию процессов их функционирования на производственных предприятиях, в социальных учреждениях, транспортных объектах. Предложенные методы и модели могут быть использованы в перспективных системах защиты информации в корпоративных информационных системах, предъявляющих высокие требования к доступности сервисов этих систем, адаптивности и комплексности подходов к обеспечению информационной безопасности. Кроме того, разработанные методы и модели могут использоваться при создании решений по обнаружению сетевых атак и защите от них на основе анализа сетевого трафика в информационно-телекоммуникационных системах. Эти возможности обоснованы корректностью исходных предпосылок, соответствием результатов моделирования общим закономерностям, апробацией основных результатов работы на конференциях и в научной печати, реализацией результатов работы в проектах.

Положения, выносимые на защиту, соотнесены с пунктами паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»: «3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса» (результаты 3-5), «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» (результаты 4-5), «7. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения» (результат 1), «8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем» (результат 1), «9. Модели и методы оценки защищенности информации и информационной безопасности объекта» (результаты 1–2), «10. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты» (результат 2), «14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности» (результат 2).

Список литературы

1. Михайлов С.А., Кашевник А.М. Организация интеллектуальных пространств на основе платформы Smart-M3 с использованием устройств на базе операционной системы DD-WRT // Труды СПИИРАН. 2017. Вып. 52. С. 180-203.
2. Sarwar G., Ullah F., Lee S. QoS and QoE Aware N-Screen Multicast Service // Journal of Sensors, 6. 2016. С 1-11.
3. Павельев С.В. Методы обеспечения доступности информационных ресурсов в территориально-распределенных автоматизированных системах обработки данных: диссертация на соискание учёной степени к.т.н., 2008. https://elibrary.ru/item.asp?id=19191212
4. Szmit M., Wężyk R., Skowroński M., Szmit A. Traffic Anomaly Detection with Snort // Information Systems and Computer Communication Networks. 2007.
5. Mahmood T. и др. Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images // Forensic Science International. 2017. Т. 279. С. 8-21.
6. Sitara K., Mehtre B.M. Digital video tampering detection: An overview of passive techniques // Digital Investigation. 2016. Т. 18. С. 8-22.
7. Aghamaleki J.A., Behrad A. Inter-frame video forgery detection and localization using intrinsic effects of double compression on quantization errors of video coding // Signal Processing: Image Communication. 2016. Т. 47. С. 289-302.
8. Penttinen A. Introduction to Teletraffic Theory. Helsinki University of Technology. 2003.
9. Langeheinrich M. Privacy by Design – Principles of Privacy Aware Ubiquitous System // Proceedings of UBICOMP Conference. 2001. С. 273-291.
10. Humayed A., Lin J., Li F., Luo B. Cyber-Physical Systems Security – A Survey. 2017.

11. Yan H. Collaborative discriminative multi-metric learning for facial expression recognition in video // Pattern Recognition. 2018. Т. 75. Вып. С. С. 2-31.
12. Szmit M., Szmit A., Adamus S., Bugała S. Usage of Holt-Winters Model and Multilayer Perceptron in Network Traffic Modelling and Anomaly Detection // Informatika. 2012. Т. 3. С. 359-368.
13. Al-Muhtadi J. и др. Cerberus: A Context-Aware, Security Scheme for Smart Spaces // Proceedings of the First IEEE International Conference on Conference: Pervasive Computing and Communications (PerCom 2003). 2003.
14. Al-Rabiaah S., Al-Muhtadi J. ConSec: Context-Aware Security Framework for Smart Spaces // Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). 2012.
15. Hosseinzadeh S. и др. A semantic security framework and context-aware role-based access control ontology for smart spaces // Proceedings of the International Workshop on Semantic Big Data. 2016.
16. Бабенко Г.В., Белов С.В. Анализ трафика TCP/IP на основе методики допустимого порога и отклонения как инструмент определения инцидентов информационной безопасности // Технологии техносферной безопасности. 2011. Т. 5. С. 273-279.
17. Li K. и др. Distinguishing DDoS attacks from flash crowds using probability metrics // Proceedings of the Third International Conference on Network and System Security. 2009. С. 9-17.
18. Lu W., Traore I. An unsupervised approach for detecting DDoS attacks based on traffic-based metrics // Proceedings ot the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing. 2005.
19. Siaterlis C., Mlaglaris B. Detecting DDoS attacks with passive measurement based heuristics // Proceedings of the Ninth International Symposium on Computers And Communications. 2004.

20. Syed Navaz A.S., Sangeetha V., Prabhadevi C. Entropy based anomaly detection system to prevent DDoS attacks in cloud // International Journal of Computer Applications. 2013. Т. 62. № 15. С. 42-47.
21. Renuka Devi S., Yogesh P. Detection of application layer DDoS attacks using information theory based metrics // Proceedings of the Second International Conference on Computer Science, Engineering and Applications. 2012.
22. Bellaïche M., Grégoire J.-C. SYN flooding attack detection based on entropy computing // Proceedings of the IEEE Global Telecommunications Conference. 2009.
23. Lu K. и др. Robust and efficient detection of DDoS attacks for large-scale Internet // Computer Networks. 2007. Т. 51. С. 5036-5056.
24. Noh S. и др. Detecting distributed denial of service (DDoS) attacks through inductive learning // Lecture Notes in Computer Science. 2003. Т. 2690. С. 286-295.
25. Домрачёв В.Г. и др. Статистический анализ сетевого трафика с использованием вейвлет-функций. М.: Информика, 2009.
26. Тишина Н. А., Дворовой И. Г, Соловьёв Н. А. Обнаружение вторжений на основе вейвлет-анализа сетевого трафика // Вестник Уфимского государственного авиационного технического университета. 2010. Т. 14. № 5 (40). С. 188-194.
27. Schwab K. The Fourth Industrial Revolution. Currency: 2016.
28. Hermann M., Pentek T., Otto B. Design Principles for Industrie 4.0 Scenarios: A Literature Review. Technische Universität Dortmund, Working Paper No. 01, 2015 [Электронный ресурс]: https://www.researchgate.net/publication/307864150_Design_Principles_for_Industrie_40_Scenarios_A_Literature_Review
29. Котенко И. В., Нестерук Ф. Г., Шоров, А. В. Концепция адаптивной защиты информационно-телекоммуникационных систем на основе парадигм нервных и нейронных сетей // Труды СПИИРАН. 2012. № 4(23). С. 101-116.

30. Nagendra S., Baskaran R., Abirami S. Video-Based Face Recognition and Face-Tracking using Sparse Representation Based Categorization // Procedia Computer Science. 2015. Т. 54. С. 746-755.
31. Kaya H., Gurpinar F., Salah A.A. Video-based emotion recognition in the wild using deep transfer learning and score fusion // Image and Vision Computing. 2017. Т. 65. С. 66-75.
32. Dong X.L. и др. Knowledge-Base Trust: Estimating the Truthworthiness of Web Sources [Электронный ресурс]. URL: arxiv.org/pdf/1502.03519v1.pdf
33. Воробьев В.И. и др. Исследование и выбор криптографических стандартов на основе интеллектуального анализа документов // Труды СПИИРАН. 2016. Т. 5(48). С. 69-87.
34. Metzger M.J., Flanagin A.J. Credibility and trust of information in online environments: The use of cognitive heuristics // Journal of Pragmatics. 2013. Т. 59B. С. 210-220.
35. Li R., Suh A. Factors Influencing Information credibility on Social Media Platforms: Evidence from Facebook Pages // Procedia Computer Science. 2015. Т. 72. С. 314-328.
36. Kakol M., Nielek R., Wierzbicki A. Understanding and predicting Web content credibility using the Content Credibility Corpus // Information Processing & Management. 2017. Т. 53. Вып. 5. С. 1043-1061.
37. Смирнов И.В., Шелманов А.О., Кузнецова Е.С., Храмоин И.В. Семантико-синтаксический анализ естественных языков. Часть II. Метод семантико-синтаксического анализа текстов // Искусственный интеллект и принятие решений. 2014. № 1. С. 11-24.
38. Осипов Г.С., Смирнов И.В., Тихомиров И.А. Реляционно-ситуационный метод поиска и анализа текстов и его приложения // Искусственный интеллект и принятие решений. 2008. №2. С. 3-10.
39. Смирнов И.В. Метод автоматического установления значений минимальных синтаксических единиц текста // Информационные технологии и вычислительные системы. 2008. №3. С. 30-45

40. Bartlett J., Reynolds L. The State of the Art 2015: a literature review of social media intelligence capabilities for counter-terrorism. Demos. 2015. 98 c.
41. Зубец В.В., Ильина И.В. Оценка достоверности сетевой информации // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2011. №1. URL: http://cyberleninka.ru/article/n/otsenka-dostovernosti-setevoy-informatsii
42. Колмогоров А.Н. Об аналитических методах в теории вероятностей // Успехи математических наук. 1938. №5. С 5-41.
43. Ивченко Г.И., Каштанов В.А., Коваленко И.Н. Теория массового обслуживания. Учебное пособие для вузов. М.: Высшая школа, 1982.
44. Land A. H., Doig A. G. An Automatic Method of Solving Discrete Programming Problems // Econometrica. 1960. Т. 3. С. 497-520.
45. Nielsen J. Response times: the three important limits [Электронный ресурс. URL: https://www.nngroup.com/articles/response-times-3-important-limits/
46. Осипов В.Ю., Носаль И.А. Обоснование мероприятий информационной безопасности // Информационно-управляющие системы. 2013. №2. С. 48-53.
47. Kwon A. и др. The design of a quality of experience model for providing high quality multimedia services // Proceedings of the IEEE International Workshop on Modelling Autonomic Communications Environments. 2010. С. 24-36.
48. Фаулер М. Архитектура корпоративных программных приложений.: Пер. с англ. М.: Издательский дом «Вильямс», 2006.
49. Cheong F., Lai R. QoS specification and mapping for distributed multimedia systems: A survey of issues // Journal of Systems and Software. 1999. Т. 45. №. 2. С. 127-139.
50. Nahrstedt K., Steinmetz R. Resource management in networked multimedia systems // IEEE Computer. 1995. Т. 28. №. 5. С. 52-63.
51. TM Forum GB923: Wireless service measurement Handbook [Электронный ресурс]. URL: https://www.tmforum.org/resources/best-practice/gb923-wireless-service-measurement-handbook/

52. 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.
53. Levonevskiy D., Vatamaniuk I., Saveliev A. Processing models for conflicting user requests in ubiquitous corporate smart spaces // MATEC Web of Conferences. 2018. Т. 161.
54. ГОСТ Р 27.403-2009 Надежность в технике (ССНТ). Планы испытаний для контроля вероятности безотказной работы. Национальный стандарт Российской Федерации. М.: Стандартинформ, 2010.
55. Egger S. и др. Waiting times in quality of experience for web based services // Proceedings of the Fourth International Workshop on Quality of Multimedia Experience (QoMEX). 2012. С. 86-96.
56. Sharma П. Digital Color Imaging Handbook. CRC Press, 2003.
57. Алексеева И.Ю. и др. Информационные вызовы национальной и международной безопасности. М.: ПИР-Центр, 2001. 328 с.
58. Сименко И. Одна из самых больших DDoS-атак в истории [Электронный ресурс]. URL: https://habrahabr.ru/post/174483/
59. Массино В. Мошенники тянутся к iCloud [Электронный ресурс]. URL: https://www.gazeta.ru/tech/2016/07/14/9687215/icloud_40mln.shtml
60. Иннополис – официальный сайт города [Электронный ресурс]. URL: http://www.innopolis.com/
61. Vatamaniuk I. и др. Scenarios of Multimodal Information Navigation Services for Users in Cyberphysical Environment // Lecture Notes on Artificial Intelligence. 2016. Т. 9811. С. 588-595.
62. Томас Т.Л. Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции. 2002.

63. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000. 452 с.
64. Девянин П.Н. и др. Теоретические основы компьютерной безопасности. Учебное пособие для вузов. М.: Радио и Связь, 2000, 192 стр.
65. Osipov V., Vodyaho A., Zhukova N. Multilevel Automatic Synthesis of Behavioral Programs for Smart Devices // Proceedings of the International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO). 2017. DOI: 10.1109/ICCAIRO.2017.68.
66. Тронин Ю.Н.. Информационные системы и технологии в бизнесе. М.: Альфа-Пресс, 2005.
67. Лисин Н. Лоскутная автоматизация, или как управлять «зоопарком» программ // Byte, 2009. URL: https://www.bytemag.ru/articles/detail.php?ID=14862
68. Henty S. UI Response Times [Электронный ресурс]. URL: https://medium.com/@slhenty/ui-response-times-acec744f3157
69. ГОСТ Р ИСО/МЭК 7498-1-99. Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. М.: Стандартинформ, 2006.
70. Марков А.А. Распространение закона больших чисел на величины, зависящие друг от друга // Известия физико-математического общества при Казанском университете. 1906. Т. 15. Сер. 2. С. 135-156.
71. Román M. и др. Gaia: A Middleware Infrastructure to Enable Active Spaces // IEEE Pervasive Computing. 2002. С. 74-83.
72. Осипов В.Ю., Воробьев В.И., Левоневский Д.К. Проблемы защиты от ложной информации в компьютерных сетях // Труды СПИИРАН. 2017. Вып. 53. С. 97-117.
73. Levonevskiy D.K., Fatkieva R.R., Ryzhkov S.R. Network attacks detection using fuzzy logic // Proceedings of the 18th International Conference on Soft Computing and Measurements (SCM). 2015. URL: https://ieeexplore.ieee.org/document/7190470

74. Vorobiev V. и др. Criteria and indices of computer network protection // Proceedings of the 9th International Conference on Security of Information and Networks. 2016. С. 176-177.
75. Fatkieva R.R., Vorobiev V.I., Levonevskiy D.K. Approach to information security control of complex computer networks // Proceedings of the 19th International Conference on Soft Computing and Measurements (SCM). 2016. URL: https://ieeexplore.ieee.org/document/7519687
76. Levonevskiy D., Vatamaniuk I., Saveliev A. Integration of corporate electronic services into a smart space using temporal logic of actions // Lecture Notes in Computer Science. Т. 10459. 2017. С. 134-143.
77. Novikov F. и др. Attribute-Based Approach of Defining the Secure Behavior of Automata Objects // ACM International Conference Proceeding Series: SIN-2017 Conference, Jaipur. 2017.
78. Патент РФ RU 2538292 C1. Способ обнаружения компьютерных атак на сетевую компьютерную систему // Патент России № RU 2538292 C1. 2015. / Фаткиева Р.Р., Атисков А.Ю., Левоневский Д.К.
79. Davis W.S., Yen D.C. The Information System Consultant's Handbook: Systems Analysis and Design. CRC Press, 1998. 800 с.
80. Saltzer J.H., Schroeder M.D. The Protection of Information in Computer Systems // Communications of the ACM. 1974, Т. 17.
81. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. 2017. Т. 23. С. 145-156.
82. Ernst J.B., Kremer S.C., Rodrigues J.J.P.C. A survey of QoS/QoE mechanisms in heterogeneous wireless networks // Physical Communication. 2014. Т. 13. С. 61-72.
83. Гамма Э. и др. Приемы объектно-ориентированного проектирования. Паттерны проектирования. СПб: Питер, 2010.

84. Ларман К. Применение UML 2.0 и шаблонов проектирования. Введение в объектно-ориентированный анализ, проектирование и итеративную разработку. Вильямс, 2013.
85. Zebari R. R., Zeebaree S. R. M., Jacksi K. Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers // *International Conference on Advanced Science and Engineering (ICOASE)*. 2018. С. 156-161.
86. Mujtiba S., Rasool B. G. Impact of DDoS attack (UDP Flooding) on queuing models // Proceedings - 4th IEEE International Conference on Computer and Communication Technology (ICCCT 2013). 2013. С. 210-216.
87. Han K.-L. ICMP Flooding Attacks and Countermeasures // Journal of Digital Convergence. 2014. Т. 12. С. 237-243.
88. Yoon S., Oh J., Kim I., Jang, J. Defense against TCP flooding attack. 2012. С. 416-420. URL: https://www.researchgate.net/publication/290795551_Defense_against_TCP_flooding_attack
89. Levonevskiy D.K., Fatkieva R.R. Statistical research of traffic-based metrics for the purpose of DDos attack detection // European Science and Technology: materials of the IV international research and practice conference. 2013. Т. 1. С. 259-268.
90. Патент РФ 2472211. Способ защиты информационно-вычислительных сетей от компьютерных атак // Патент России № 2472211. 2013. / Андрианов В.И. и др.
91. Патент РФ 2480937. Система и способ уменьшения ложных срабатываний при определении сетевой атаки // Патент России № 2480937. 2013. / Гудов Н.В., Левашов Д.А.
92. Zeng X., Pei H. Human-Computer Interaction in Ubiquitous Computing Environments // International Conference on Information Computing and Applications. 2012. Т. 308. С. 628-634.

93. Hossain M.A. и др. Performance analysis of smart digital signage system based on software-defined IoT and invisible image sensor communication // International Journal of Distributed Sensor Networks. 2016. Т. 7/12. С. 1-14.
94. Левоневский Д.К. Архитектура облачной системы распределения контента в киберфизических системах. Научный журнал «Моделирование, оптимизация и информационные технологии». 2019. Т. 7. № 4.
95. Александров В.В. и др. 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.
96. Ватаманюк И.В. и др. Модели и способы взаимодействия пользователя с киберфизическим интеллектуальным пространством. СПб: Лань, 2019. – 176 с. ISBN 978-5-8114-3877-8.
97. Jucker A.H. и др. Doing space in face-to-face interaction and on interactive multimodal platforms // Journal of Pragmatics. 2018. Т. 134. С. 85-101.
98. Kruys J.P. Security of open systems // Computers & Security. 1989. Т. 8. № 2. С. 139-147.
99. Котенко И. В., Коновалов А. М., Шоров А. В. Имитационное моделирование механизмов защиты от бот-сетей // Труды СПИИРАН. 2011. № 4(19). С. 7-33.
100. Pruteanu A., D’Acunto L., Dulman S. Distributed online flash-crowd detection in P2P swarming systems // Computer Communications. 2013. Т. 36. № 5. С. 533-541.
101. Микова С.Ю., Оладько В.С., Нестеренко М.А. Подход к классификации аномалий сетевого трафика // Инновационная наука. 2015. №11-2.

Приложение А. Список публикаций соискателя по теме диссертации

В рецензируемых журналах из списка ВАК:

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.

В зарубежных изданиях, индексируемых в WoS/Scopus:

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:

16. 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
17. 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.
18. 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.

Интеллектуальная собственность:

1. Патент на изобретение RU 2538292 C1. Способ обнаружения компьютерных атак на сетевую компьютерную систему. Фаткиева Р.Р., Атисков А.Ю., Левоневский Д.К. 2015.
2. Свидетельство о государственной регистрации программы для ЭВМ №2014614440. Левоневский Д.К., Фаткиева Р.Р. Программа обнаружения вредоносного трафика сетевых атак типа «отказ в обслуживании». 2014.
3. Свидетельство о государственной регистрации программы для ЭВМ №2016612251. Левоневский Д.К., Фаткиева Р.Р. Программа агрегации событий систем обнаружения вторжений. 2016.
4. Свидетельство о государственной регистрации программы для ЭВМ №2019660739. Левоневский Д.К., Осипов В.Ю., Фаткиева Р.Р. Программный комплекс решения задач мониторинга событий для прогнозирования террористических угроз. 2019.

Приложение Б. Акты внедрения результатов диссертационной работы

РАЗРАБОТКА И ПРОИЗВОДСТВО
ПРИБОРОВ ЭКСПРЕСС-АНАЛИЗА
ЛАБОРАТОРНОГО ОБОРУДОВАНИЯ

ООО «ЭКАН»

194021, г. Санкт-Петербург,
ул. Политехническая, д. 22

ИНН 7802850848 КПП 780201001
ОКПО 27520549 ОКАТО 40265562000
ОГРН 1147847046918
ОКВЭД 33.40.1

р/с 40702810155080003712
Северо-Западный банк ПАО «Сбербанк»
к/с 30101810500000000653
БИК 044030653

Телефон: (812) 649-77-69

№ 4 « 15 » января 2020 г.

АКТ РЕАЛИЗАЦИИ
результатов диссертационной работы
на соискание учёной степени кандидата технических наук
Левоневского Дмитрия Константиновича

Настоящий акт составлен о том, что результаты диссертационной работы Левоневского Д.К. на тему «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» использованы в ООО «ЭКАН» при выполнении составной части опытно-конструкторской работы «Разработка устройства сопряжения инфракрасного анализатора с локальной сетью предприятия» в рамках задач, посвящённых разработке прикладного программного обеспечения. В частности, были использованы результаты диссертационного исследования:

1. Математическая модель корпоративной информационной системы, функционирующей в условиях комплексных деструктивных информационных воздействий.
2. Метод оценивания эффективности функционирования корпоративной информационной системы с использованием предложенной математической модели.

Использование моделей, алгоритмов и методов, предложенных в работе, позволяет повысить доступность информационной системы и оценить её эффективность при различных сценариях функционирования системы.

Председатель комиссии
Генеральный директор — д.т.н., проф. Петров Г.П.

Общество с ограниченной ответственностью «ЭКАН» «EKAN» Санкт-Петербург

Члены комиссии:
Инженер-исследователь — Антонов Р.Ю.
Ведущий программист — Суриков А.Г.

УТВЕРЖДАЮ
Проректор по научной работе
Университета ИТМО
д.т.н., профессор
_____ В.О. Никифоров
« 17 » января 2020 г.

Акт

о внедрении результатов диссертационной работы
Левоневского Дмитрия Константиновича
на тему «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий»

Результаты диссертационного исследования Левоневского Д.К. на тему «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий», представленного на соискание учёной степени кандидата технических наук, использованы 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».

Декан фБИТ, к.т.н., доцент _____ Заколдаев Д.А.

Заведующая лабораторией фБИТ _____ Коваль Е.Н.

МИНОБРНАУКИ РОССИИ

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

14 линия, д. 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 » января 2020 г. № 060-01-01-077

На № _____

Левоневскому
Дмитрию Константиновичу

Акт

об использовании результатов кандидатской диссертационной работы
Левоневского Дмитрия Константиновича
«Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий»

Настоящий Акт составлен в том, что следующие результаты диссертационной работы Левоневского Дмитрия Константиновича были использованы в СПИИРАН при проведении исследований в рамках Соглашения с Минобрнауки России № 05.607.21.0322 (идентификатор RFMEFI60719X0322), а именно:

1 метод оценивания эффективности защиты корпоративных информационных систем от комплексных деструктивных воздействий использовался для оценки эффективности выбранных контрмер, направленных на обеспечение защиты от сетевых атак;

2 метод адаптивной защиты корпоративной информационной системы от комплексных деструктивных воздействий использовался для объединения различных подходов к обнаружению сетевых атак.

Руководитель проекта ,
проф., д.т.н. И.В. Котенко

Ответственный исполнитель проекта
проф., д.т.н. И.Б. Саенко

Директор СПИИРАН,
проф.РАН, д.т.н. А.Л. Ронжин

МИНОБРНАУКИ РОССИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕУЧРЕЖДЕНИЕ 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.spiiras.nw.ru
ОКПО 04683303, ОГРН 1027800514411, ИНН/КПП 7801003920/780101001

А К Т

об использовании результатов диссертационной работы Левоневского Дмитрия Константиновича «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» в НИР СПИИРАН по договору с федеральным государственным бюджетным учреждением "Российский научный фонд" (РНФ) № 16-19-00044 от 14.01.2016 г.

Комиссия в составе: председателя д.т.н., С.В. Кулешова, членов комиссии: к.т.н. А.И. Савельева и к.воен.н. Е.П. Силлы, рассмотрев представленные материалы:

1. Автореферат и диссертационную работу Левоневского Дмитрия Константиновича.
2. Отчетную документацию о выполнении проекта № 16-19-00044 «Принципы распределения задач между сервисными роботами и средствами киберфизического интеллектуального пространства при многомодальном обслуживании пользователей» в 2018 году

установила, что:

1. Положения диссертационной работы Левоневского Дмитрия Константиновича были использованы при проведении НИР, выполняемых 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».
2. Разработанная в диссертации Левоневского Д.К. модель функционирования защищаемой корпоративной информационной системы была апробирована при решении задачи обеспечения доступности сервисов корпоративного интеллектуального пространства в условиях намеренных и ненамеренных деструктивных воздействий.

Председатель комиссии
Заместитель директора по научной работе,
д.т.н. С.В. Кулешов

Члены комиссии:
Руководитель лаборатории
автономных робототехнических систем,
к.т.н. А.И. Савельев

Ученый секретарь,
к.воен.н. Е.П. Силла

Приложение В. Полученные свидетельства об интеллектуальной собственности

РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 538 292** (13) **C1**

(51) МПК
G06F 21/55 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2013134440/08, 24.07.2013**

(24) Дата начала отсчета срока действия патента:
24.07.2013

Приоритет(ы):
(22) Дата подачи заявки: **24.07.2013**

(45) Опубликовано: **10.01.2015** Бюл. № 1

(56) Список документов, цитированных в отчете о поиске: **US 8423645 B2, 16.04.2013. RU 2483348 C1, 27.05.2013. US 2012/0117646 A1, 10.05.2012. RU 2381550 C2, 10.02.2010. US 2012/0151583 A1, 14.06.2012. RU 2480937 C2, 27.04.2013**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, ОАО "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Фаткиева Роза Равильевна (RU),
Атисков Алексей Юрьевич (RU),
Левоневский Дмитрий Константинович (RU)

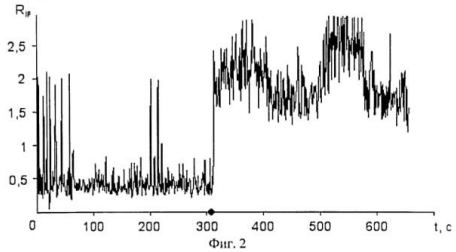
(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

RU 2538292 C1

(54) СПОСОБ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА СЕТЕВУЮ КОМПЬЮТЕРНУЮ СИСТЕМУ

(57) Реферат:

Изобретение относится к вычислительной технике. Технический результат заключается в обнаружении компьютерных атак разных видов, комбинированных одновременных атак разных видов и определении видов атак. Способ обнаружения компьютерных атак на сетевую компьютерную систему, включающую, по крайней мере, один компьютер, подключенный к сети и имеющий установленную операционную систему и установленное прикладное программное обеспечение, включающее систему анализа трафика, в котором для анализа получаемых из сети пакетов выбираются определенные параметры и вычисляются их значения, которые затем сравниваются с эталонными значениями, а факт наличия одиночной или комбинированной одновременной атаки и определение видов атак определяется по сочетанию установленных условий для параметров. Для обработки получаемых из сети пакетов данных используется система анализа трафика, позволяющая вычислять параметры трафика в реальном масштабе времени. 13 ил., 3 табл.



Фиг. 2

RU 2538292 C1

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2014614440

Программа обнаружения вредоносного трафика сетевых атак типа отказ в обслуживании

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (RU)***

Авторы: ***Левоневский Дмитрий Константинович (RU), Фаткиева Роза Равильевна (RU)***

Заявка № **2014612134**

Дата поступления **14 марта 2014 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***24 апреля 2014 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Б.П. Симонов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2016612251

Программа агрегации событий систем обнаружения вторжений

Правообладатель: *Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (RU)*

Авторы: *Левоневский Дмитрий Константинович (RU), Фаткиева Роза Равильевна (RU)*

Заявка № 2015663200
Дата поступления 31 декабря 2015 г.
Дата государственной регистрации
в Реестре программ для ЭВМ *20 февраля 2016 г.*

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019660739

Программный комплекс решения задач мониторинга событий для прогнозирования террористических угроз

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (RU)***

Авторы: ***Левоневский Дмитрий Константинович (RU), Осипов Василий Юрьевич (RU), Фаткиева Роза Равильевна (RU)***

Заявка № **2019617104**

Дата поступления **14 июня 2019 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***13 августа 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев