На правах рукописи

Коломойцев Владимир Сергеевич

МОДЕЛИ И МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ И ОБОСНОВАНИЕ ВЫБОРА ИХ КОМПЛЕКТАЦИИ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2018

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

Научный руководитель: доктор технических наук, профессор
Богатырев Владимир Анатольевич

Официальные оппоненты: **Молдовян Николай Андреевич**
доктор технических наук, профессор
Санкт-Петербургский институт информатики и автоматизации Российской академии наук, научно-исследовательская лаборатория безопасности информационных систем,
главный научный сотрудник

Овчинников Андрей Анатольевич
кандидат технических наук, доцент
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
кафедра безопасности информационных систем,
заведующий кафедрой

Ведущая организация: Закрытое акционерное общество «Эврика»,
Санкт-Петербург

Защита состоится 26 декабря 2018 года в 14.00 на заседании объединенного диссертационного совета Д 999.121.03 при федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», федеральном государственном бюджетном образовательном учреждении высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 23 ноября 2018 года.

Ученый секретарь
диссертационного совета Д 999.121.03,
канд. техн. наук  А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В процессе обеспечения защиты трафика и узлов, входящих в состав вычислительной системы (далее – ВС), требуется учитывать специфику деятельности организаций, которые используются ВС, а также решать смежные с процессом организации безопасности сетей задачи, такие как контроль за вносимыми задержками обслуживания и надежностью, стоимостью создания и обслуживания системы и сложностью архитектурной реализации ВС. При этом, наличие в современных ВС множества как внутренних, так и внешних связей, создает дополнительные сложности в процессе создания согласованной и правильно работающей защищенной ВС.

При организации сетевой безопасности в каждой конкретной организации необходимо учитывать, какие из параметров работы ВС являются для нее наиболее важными, а какими имеется возможность пренебречь. По этой причине внедрение большого количества разнообразных средств защиты не всегда является лучшим решением, когда, например, необходимо, чтобы система защиты информации (далее, СЗИ) не вносила больших задержек обслуживания. Тем самым, требуется использовать именно то специальное решение, которое позволит оптимальным образом решить задачи проектирования, в области информационной безопасности (далее – ИБ).

Обеспечение указанных требований к высокоэффективным защищенным ВС затрудняется тем, насколько в большей или меньшей степени подвержена система различным видам угроз, какие архитектурные решения были использованы при её проектировании, а также области работы самой организации, напрямую влияющей на глубину внедрения в нее различных информационных технологий. Все это обусловливает актуальность разработки моделей и методов оценки эффективности СЗИ для качественного обоснования выбора их комплектации средствами защиты.

Степень разработанности темы. При проектировании высокоэффективных СЗИ, способных качественно выполнять свои функции при различных предъявляемым к ним требованиям, необходим комплекс моделей анализа и методов проектирования, позволяющий путем целенаправленного формирования возможных проектных решений и выработки системы частных и комплексных критериев показателей эффективности, синтезировать оптимальное проектное решение.

Под эффективным проектным решением будем понимать решение, соответствующее предъявляемым к нему требованиям по обеспечиваемому им уровню информационной защищенности, задержек обслуживания, вероятности безотказной работы и оперативной готовности при ограничениях на стоимость реализации системы.

Вопросам проектирования и анализа эффективности СЗИ посвящено большое количество работ. Существенный вклад в развитие теоретической и методологической базы был сделан многими отечественными и зарубежными учеными: Скотт Бармен, Зегжда Д. П., Толстой А.И., Молдовян Н.А., Домарев В.В., Кэрриэ Брайан, Шаньгин В.Ф., Нестерук Г. Ф., Герасименко В.А., Грушо А.А.

Результаты научной работы данных ученых в значительной мере повлияли на создание и совершенствование научных основ и методологии проектирования эффективных защищенных ВС и анализу средств и мер ЗИ.

Цель и задачи работы. Целью работы является повышение эффективности построения СЗИ, с учетом влияния комплектации и размещения средств ЗИ, последовательности их применения в схемах безопасного доступа и пересечения множеств угроз ИБ, обнаруживаемых и устраняемых используемыми средствами.

В рамках диссертационной работы должны быть решены следующие задачи:

1. Анализ существующих угроз ИБ и мест их возникновения в корпоративной сети.
2. Анализ существующих методов и средств ЗИ.

3. Анализ взаимного влияния используемых в ВС средств и мер по обеспечению ИБ.

4. Исследование методов проектирования и анализ возможных вариантов проектных решений организации процесса безопасного доступа узлов сети во внешнюю сеть.

5. Разработка математических моделей оценки эффективности схем безопасного доступа в составе СЗИ.

6. Формирование критериев оценки эффективности решений обеспечения ИБ ВС.

7. Анализ эффективности и обоснование выбора проектных решений построения СЗИ, с использованием рассматриваемых схем доступа.

Объект исследования – схема безопасного доступа, в составе СЗИ ВС.

Предмет исследования – модели, методы и способы повышения эффективности СЗИ, структуры организации СЗИ.

Научная задача, решаемая в диссертации, направлена на повышение эффективности проектирования защищенных ВС на основе моделей и методов анализа и синтеза проектных решений, обеспечивающих высокую информационную защищенность, вероятность безотказной работы и готовность системы и низкие задержки обслуживания, вносимые СЗИ.

Решение данной задачи имеет большое значение для развития методологии проектирования, модификации и повышения эффективности работы защищенных ВС, разработки новых методов оценки защищенности СЗИ.

Научная новизна. В результате проведенных исследований получены следующие новые научные результаты:

1. Построена математическая модель оценки достигаемого СЗИ уровня информационной защищенности, основывающаяся на вероятности обнаружения угроз ИБ средствами ЗИ, учитывающая пересекаемость множеств угроз, обнаруживаемых и устраняемых средствами ЗИ, которыми укомплектована СЗИ и вариантности её комплектации средствами защиты.

2. Построены математические модели оценки задержек обслуживания вносимых СЗИ, учитывающие снижение интенсивности входного потока в результате его фильтрации при прохождении через последовательно применяемые средства ЗИ и вид распределения среднего времени этапов обслуживания.

3. Построены математические модели надежности СЗИ, позволяющие оценить вероятность безотказной работы СЗИ и её оперативную готовность при условии налагаемых ограничений на нагрузку в промежуточных узлах СЗИ, основываясь на построенных математических моделях оценки задержек обслуживания, и финансовых ограничений на проектирование СЗИ.

4. Предложены комплексные критерии эффективности, включающие показатели информационной защищенности, обеспечиваемой СЗИ от различных угроз, задержек, вносимых СЗИ, оперативной готовности и безотказной работы СЗИ.

5. Предложен метод построения СЗИ, основывающийся на применении предложенных критериев эффективности СЗИ и позволяющий повысить качество проектирования и модификации СЗИ, ориентированных на выбор оптимальных решений построения системы защиты при условии ограничений материальных затрат на её реализацию при выборе состава, количества и места размещения применяемых средств защиты.

Теоретическая и практическая значимость результатов исследования заключается в том, что предложены модели и методы оценки эффективности и обоснования выбора проектных решений по обеспечению информационной защищенности СЗИ, с учетом:

1. влияния на достигаемый СЗИ уровень информационной защищенности при пересекаемости множеств угроз ИБ, обнаруживаемых и устраняемых средствами ЗИ, и вариантности её комплектации средствами ЗИ;

2. задержек обслуживания, вносимых СЗИ, отражающие снижение интенсивности входного потока в результате его фильтрации при прохождении через последовательно применяемые средства ЗИ;

3. надежной и безотказной работы СЗИ при снижении нагрузки в промежуточных узлах;

4. комплексных критериев эффективности СЗИ, включающих показатели информационной защищенности, обеспечиваемой СЗИ от различных угроз, задержек, вносимых СЗИ, оперативной готовности и безотказной работы СЗИ.

Результаты исследования позволяют:

1. повысить качество оценки эффективности применения той или иной СЗИ в составе ВС;

2. проектировать СЗИ, способные выдерживать большее число отказов при обеспечении требования стационарности режима обслуживания;

3. повысить качество проектирования СЗИ, ориентированных на выбор оптимальных решений построения системы защиты при условии ограничений материальных затрат на её реализацию при выборе состава, количества и места размещения применяемых средств защиты.

Реализация и внедрение результатов работы. Предложенные методы построения СЗИ и результаты работы использованы в исследованиях кафедры вычислительной техники Университета ИТМО, в том числе НИР № 414650 «Методы и модели обеспечения интегрированной безопасности и устойчивости функционирования», № 615869 «Методы проектирования ключевых систем информационной инфраструктуры», № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность» кафедры вычислительной техники Университета ИТМО, а также в НИОКР № 416031 «Интерактивный оптический лабиринт», Университета ИТМО. Результаты, полученные в диссертации использованы при выполнении ОКР «Проектирование и сопровождение высоконадежной и защищенной системы обработки информации» (договор АкТд-Р№15 от 01 марта 2018г) в ООО «Академия тепла» и ОКР «Проектирование и организация работы защищенной компьютерной системы межструктурного взаимодействия» (договор №37 от 28 апреля 2018г) в International Police Association – Международная неправительственная организация с консультативным статусом «SPECIAL» при Экономическом и Социальном Совете ООН.

Методология и методы исследования основаны на теории рисков, теории вероятностей, теории массового обслуживания, теории надежности, методах системного анализа.

Положения, выносимые на защиту.

1. Метод и аналитическая модель оценки защищенности ВС, при различных вариантах комплектации СЗИ, учитывающий взаимное пересечение множеств обнаруживаемых и устраняемых угроз ИБ, применяемыми средствами ЗИ.

2. Математические модели оценки надежности и задержек, вносимых СЗИ, учитывающие пересекаемость множеств угроз ИБ, обнаруживаемых и устраняемых средствами ЗИ, снижение нагрузки на промежуточных узлах системы и различные варианты комплектации СЗИ.

3. Система частных и комплексных показателей эффективности: информационной защищенности и надежности ВС, задержки, оперативной готовности и вероятности безотказной работы СЗИ.

4. Метод проектирования и обоснования выбора проектных решений построения схем безопасного доступа узлов корпоративной сети к ресурсам внешней сети, на основе моделей оценки задержек обслуживания, вносимых СЗИ, уровня информационной защищенности ВС и надежности работы СЗИ.

Достоверность результатов подтверждается применением корректных исходных данных и используемых методов исследования, математического аппарата и теоретической базы в области ИБ и защищенных компьютерных систем, апробацией результатов исследования в докладах на российских и зарубежных научных конференциях, публикациях в журналах, рекомендованных ВАК и входящих в реферативные базы данных SCOPUS и WoS, а также результатами внедрения.

Апробация результатов. Результаты и основные положения диссертационного исследования докладывались на 32 зарубежных и отечественных научных конференциях, форумах и конгрессах: XLIV-XLVII научных конференциях Университета ИТМО (Россия, СПб., 2015-2018); IV Всероссийский конгресс молодых ученых (Россия, СПб., 2015); V-VII Конгрессах молодых ученых (Россия, СПб., 2016-2018); DCCN-2015 – DCCN-2017 (Distributed Computer and Communication Networks: control, computation, communications) (Россия, г. Москва, 2015-2017); XIV-XV Санкт-Петербургских международных конференциях «Региональная информатика» (Россия, СПб., 2014, 2016); XIX Международная конференция по мягким вычислениям и измерениям (SCM'2016) (Россия, СПб., 2016); Международная научно-практическая конференция «Теоретические и практические аспекты технических наук» (Россия, г. Уфа, 2014); Международная научно-практическая конференция «Наука и образование в жизни современного общества» (Россия, г. Тамбов, 2014); Международная научно-практическая конференция «Наука: прошлое, настоящее, будущее» (Россия, г. Уфа, 2015); Международный научный форум молодых ученых «Наука будущего – наука молодых» (Россия, г. Севастополь, 2015); Информационная безопасность регионов России (Россия, СПб., 2015); Международная научно-практическая конференция «Инновационное развитие: ключевые проблемы и решения» (Россия, г. Казань, 2015); Новая наука: современное состояние и пути развития (Россия, г. Стерлитамак, 2015); Информационные системы и технологии в моделировании и управлении (Россия, г. Ялта, 2016); Международная научно-практическая конференция «Новая наука: от идеи к результату (Россия, г. Сургут, 2016); Вторая Международная Научная Конференция «Технологические перспективы в рамках евразийского пространства: новые рынки и точки экономического роста (Россия, СПб., 2016); Международная научно-практическая конференция «Новая наука: от идеи к результату» (Россия, г. Стерлитамак, 2016); Международная научно-практическая конференция «Новые информационные технологии в науке» (Россия, г. Уфа, 2016); Международная научно-практическая конференция «Единство и идентичность науки: проблемы и пути решения» (Россия, г. Казань, 2017); Международная научно-практическая конференция «Интеграционные процессы в науке в современных условиях» (Россия, г. Волгоград, 2017); ETOP-2017 The 14th International Conference on Education and Training in Optics and Photonics (Hangzhou, China, 2017); Information technologies in Science, Management, Social sphere and Medicine (ITSMSSM 2017) (Россия, г. Томск, 2017).

Исследования, в рамках диссертационной работы, были отмечены следующими наградами – «Диплом финалиста международного научного форума молодых ученых «Наука будущего – Наука молодых», «Диплом за лучший доклад на IV Всероссийском конгрессе молодых ученых», «Победитель конкурса на право получения стипендии Президента РФ по специальностям или направлениям, соответствующим приоритетным направлениям модернизации и технологического развития российской экономики –

2016» и «Победитель конкурса грантов Санкт-Петербурга для студентов, аспирантов, молодых ученых, молодых кандидатов наук 2015 г.».

Публикации. По теме диссертационной работы опубликовано 35 печатных работ, включая 4 статьи в изданиях из перечня ВАК и 4 статьи в изданиях из перечня SCOPUS/WoS.

Работа соответствует следующим пунктам **паспорта специальности 05.13.01:** п. 6 – «Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования» и п. 10 – «Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты»

Личный вклад. Все теоретические и практические выводы, разработка методов проектирования и построение аналитических моделей оценки эффективности систем защиты информации, анализ результатов измерений, содержащиеся в данной диссертационной работе, выполнены автором самостоятельно.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка литературы и приложения. Общий объем диссертации: 175 страницы. Работа содержит 34 рисунка, 1 таблицу и 122 наименования библиографических источников.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Во **введении** обоснована актуальность диссертационного исследования, сформулированы цель и задачи работы, перечислены используемые в работе методы исследования, показана научная новизна и практическая значимость результатов работы.

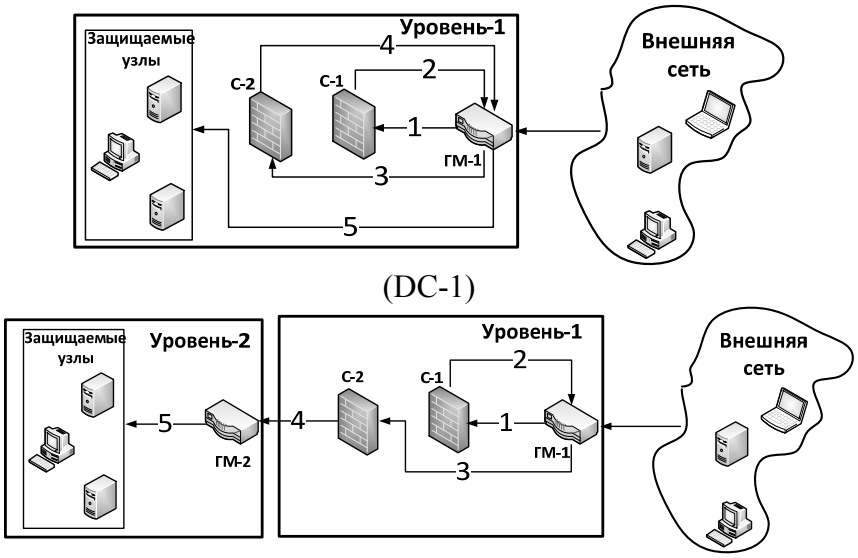
В **первой главе** рассмотрены структура соединения ВС с ресурсами внешней сети, основные подходы и методы обеспечения информационной защищенности ВС, типовые решения, позволяющие создать защищенную ВС. Сформулированы проблемы проектирования высокоэффективных защищенных ВС, дана постановка задач диссертационной работы.

На основе анализа методов обеспечения информационной защищенности ВС – применение различного вида средств межсетевого экранирования; средств защиты от несанкционированного доступа; антивирусных средств и рассмотрение типовых решений по обеспечению ЗИ в корпоративной сети сформулированы задачи диссертационного исследования.

Во **второй главе** продемонстрированы типовые решения по обеспечению ИБ на разных этапах работы ВС и выявлены проблемы при использовании «Типовой» схемы доступа. Предложены две модификации существующей «Типовой» схемы доступа – схема доступа "Прямое соединение" и схема доступа «Связующий узел». Показаны варианты построения схем доступа, а также предложена дальнейшая модификация схемы доступа «Связующий узел» – гибридный вариант схемы доступа «Связующий узел». Проведен сравнительный анализ предлагаемых схем доступа. Сформулирована задача выработки критериев моделирования и оптимизации.

Схема доступа «Прямое соединение» представляет собой набор последовательно подключенных между собой элементов ЗИ, обеспечивающих безопасное соединение оконечных узлов системы с внешней сетью. У схемы доступа «Прямое соединение» существует несколько вариантов построения при создании нескольких уровней информационной защищенности с помощью групп маршрутизаторов (далее, ГМ), соединяющих средства ЗИ между собой и оконечными узлами ВС и/или путем прямого подключения всех используемых в СЗИ средств ЗИ друг к другу. Для варианта схемы доступа, использующей два средства ЗИ, можно получить одноуровневую систему

защиты (используя одну ГМ на всю СЗИ) и многоуровневую систему защиты (например, используя две ГМ). На рис. 1, показан процесс прохождения данных из внешней сети на оконечные узлы ВС для одноуровневого варианта схемы доступа, использующей два средства ЗИ (DC-1), и для одного из двухуровневых вариантов схемы доступа (DC-2).



(DC-1)

(DC-2)

Рисунок 1 – Варианты сетевой архитектуры схемы «Прямое подключение», с одной ГМ (DC-1) и с двумя ГМ (DC-2)

Ключевым для схемы доступа «Связующий узел» является использование набора средств ЗИ, располагающихся на «вычислительном узле» («связующем узле») в качестве основного элемента ЗИ СЗИ. Это дает схеме доступа возможность быстрой реконфигурации и настройки строго под те задачи, которые актуальны на текущий момент. Данная схема доступа может быть также модифицирована путем подключения к «вычислительному узлу» аппаратного или аппаратно-программного средства ЗИ (например, межсетевого экрана) с целью повышения обеспечиваемого уровня информационной защищенности и расширения возможностей СЗИ теми функциями, которые не могут обеспечить средства ЗИ, имеющиеся на «вычислительном узле» – гибридный вариант схемы доступа «Связующий узел». Варианты схемы доступа «Связующий узел», показаны на рис. 2.

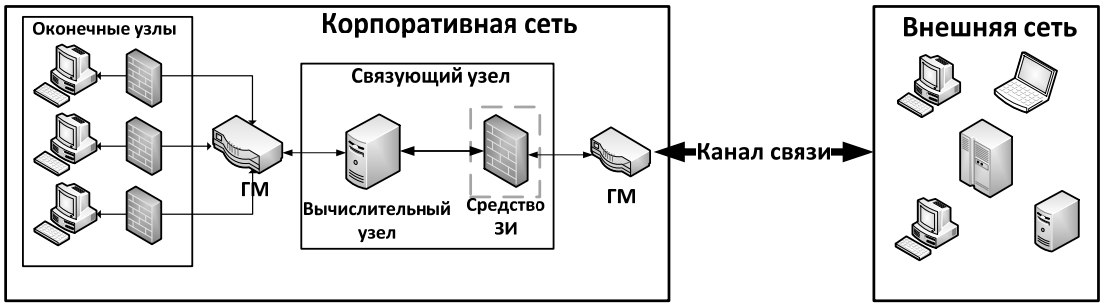


Рисунок 2 – Схема доступа «Связующий узел»

Анализ рассматриваемых схем безопасного доступа показал необходимость в решении задач:

– разработки и оценки вариантов распределения нагрузки между элементами схем доступа и внутри «вычислительного узла»;

– оценки информационной защищенности, надежности и задержек ВС, с учетом согласованной работы совокупности средств ЗИ, использующихся в СЗИ.

В **третьей главе** разработана система показателей эффективности СЗИ, предложены модели оценки вероятности обнаружения и устранения угроз и задержек их поиска в зависимости от числа применяемых средств ЗИ, последовательности применения средств ЗИ в СЗИ и вычислительных узлах, укомплектованных ими, и ограниченности вычислительных ресурсов вычислительного узла, с учетом пересекаемости множеств угроз, обнаруживаемых различными средствами ЗИ. Построены модели оценки надежности СЗИ, основывающиеся на вероятности безотказной работы системы и коэффициента оперативной готовности системы для разных вариантов построения схем доступа, используемых в СЗИ.

Проектирование СЗИ для сложных инфокоммуникационных систем требует модельно-ориентированного подхода, при котором предполагается оценку эффективности проектных решений по построению СЗИ с дальнейшим обоснованием выбора проектных решений и их оптимизацию, формирование системы критериев эффективности СЗИ, включающей совокупность частных и комплексных критериев, позволяющих провести разработку моделей оценки эффективности построения системы.

Исследуемые в рамках работы схемы доступа («Прямое соединение» и «Связующий узел») используют последовательный алгоритм активизации работы применяемых средств ЗИ (поэтапно), с возможностью их запуска в любом порядке, в случае использования схемы доступа «Связующий узел» и одноуровневого варианта исполнения схемы доступа «Прямое соединение».

Эффективность системы охарактеризуем некоторым набором частных и комплексных критериев (показателей). Набор критериев, характеризующие задержки поиска угроз, вероятность их обнаружения и надежность системы по выполнению требуемых функций, включает: среднее время обнаружения угрозы (x); второй начальный момент ($x^{(2)}$) распределения времени обнаружения угрозы; среднее время пребывания (ожидания) запросов (T_S) в СЗИ, во время поиска угроз; вероятность обнаружения и устранения угроз i-м элементом СЗИ (p_i); вероятность обнаружения и устранения угроз СЗИ (E_{S_R}); коэффициент готовности ($k_г$); вероятность безотказной работы системы за время пребывания в ней запроса на обнаружение и устранение угрозы ($P(T_S)$).

Задержку, вероятность обнаружения и устранения угроз СЗИ и надежность системы, охарактеризуем по комплексному критерию показатель эффективности СЗИ. При условии, что каждый из используемых частных критериев эффективности – равноценны между собой:

$$Q_s = k_{\text{ог}} \cdot E_{S_R} \cdot (T_0 - T_S) / T_0 = k_{\text{г}} \cdot P(T_S) \cdot E_{S_R} \cdot (T_0 - T_S) / T_0,$$

где $k_{\text{ог}}$ – коэффициент оперативной готовности, T_0 – предельно допустимые задержки обслуживания, T_S – вносимые задержки обслуживания, E_{S_R} – вероятность обнаружения и устранения угроз СЗИ (показывает степень защищенности ВС), состоящей из R-элементов.

Предложенный критерий выражает нормированную среднюю экономию времени до обнаружения и устранения угрозы относительно предельно допустимого времени задержки, вносимой СЗИ, учитывая готовность СЗИ в некоторый момент времени, и вероятность безотказной работы системы в течение реализации процедуры обнаружения и устранения угроз.

Могут быть использованы части данного комплексного критерия, например, для оценки нормированной средней экономии времени до обнаружения и устранения угрозы относительно предельно допустимого времени задержки, вносимой СЗИ, учитывая вероятность безотказной работы СЗИ $P(T_{Sys})$, в течение требуемого промежутка времени без возможности её восстановления:

$$Q_s = E_{S_R} \cdot P(T_{Sys}) \cdot (T_0 - T_S) / T_0 .$$

Аналитическая модель оценки защищенности вычислительной системы. В общем виде, пересечения множеств угроз ИБ для СЗИ, включающей, например, три элемента, с указанием доли угроз ИБ, устраняемых каждым из элементов или группой элементов, показаны диаграммой Венна на рис. 3.

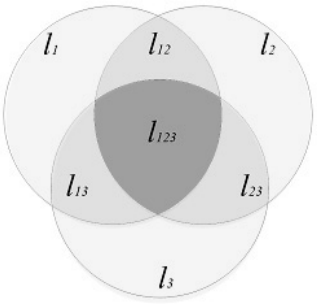


Рисунок 3 – Пересечения множеств угроз, устраняемых тремя средствами защиты

Для характеристики зависимости обнаружения угроз используемыми средствами ЗИ, определим:

– долю угроз от общего множества угроз ИБ, которые обнаруживаются и устраняются *i*-м элементом – L_i;

– долю угроз от общего множества угроз ИБ, обнаруживаемых и устраняемых *i*-м элементом, применяемым в составе СЗИ, состоящей из *r*-элементов – l_i;

– долю угроз от общего множества угроз ИБ, обнаруживаемых и устраняемых элементами *i*, *j* (используя для этого отличные друг от друга методы и/или алгоритмы), применяемыми в составе СЗИ, состоящей из *r*-элементов – l_{ij};

– долю угроз от общего множества угроз ИБ, обнаруживаемых (и устраняемых) элементами *i*, *j,…m* (используя для этого отличные друг от друга методы и/или алгоритмы), применяемыми в составе СЗИ, состоящей из *r*-элементов – $l_{ij..m}$;

– вероятность обнаружения СЗИ угроз ИБ, которым может быть подвержена ВС – I_S.

$$I_S = F(E)/F(H);\ L_i = F(A_i)/F(E);\ l_i = F\left(A_i \setminus \bigcup_{\substack{j=1 \\ j\neq i}}^{r} A_j\right)/F(E);$$

$$l_{ij} = F\left(A_i \cap A_j \setminus \bigcup_{\substack{a=1 \\ a\neq i\neq j}}^{r} A_a\right)/F(E);\ l_{ij\ldots m} = F\left(A_i \cap A_j \cap \ldots \cap A_m \setminus \bigcup_{\substack{w=1 \\ w\neq i\neq j\neq \ldots \neq m}}^{r} A_w\right)/F(E).$$

где $F(x)$ – функция, описывающая потери (условный вес) угроз в множестве. Потери угроз, которые могут быть выражены в виде: материальных, вычислительных, временных и иных потерь организации, которые она может понести в результате реализации угрозы и/или её поиска и устранения. Метод и критерий оценки потерь угроз может зависеть от требований, предъявляемых к той или иной ВС и СЗИ, в частности.

При этом множество угроз:

– H – с которыми необходимо бороться в рамках конкретной ВС;

– E – которые способен обнаружить (и с некоторой вероятностью устранить) набор из R средств (мер), использующихся в составе СЗИ;

– A_i – которые способен обнаружить и устранить *i*-й элемент СЗИ.

– Вероятность обнаружения и устранения угрозы E_{S_R} при применении R средств защиты, с учетом пересечения множеств угроз ИБ, вычислим как:

$$E_{S_R} = I_S \cdot W \cdot \sum_{i=1}^{R} \left(\begin{array}{l} l_i \cdot p_i + \sum\limits_{j=1}^{j<i} (l_{ji} \cdot (1 - \overline{p_i} \cdot \overline{p_j}) + \sum\limits_{q=1}^{q<j} (l_{qji} \cdot (1 - \overline{p_i} \cdot \overline{p_j} \cdot \overline{p_q}) + \\ + ... + \sum\limits_{m=1}^{m<t} (l_{mt...i} \cdot (1 - \overline{p_i} \cdot \overline{p_j} \cdot .... \cdot \overline{p_m})) ...) \end{array} \right),$$

где $W = \lambda_T / \lambda$ – доля угроз ИБ в поступающем потоке запросов, здесь λ_T и λ – соответственно интенсивности входного потока угроз ИБ и общего потока запросов (в том числе с угрозами ИБ); $\overline{p_j}$ – вероятность, определяемая как $\overline{p_j} = 1 - p_j$; $i, j, ..., t$ – порядковые номера элементов СЗИ.

Вероятность устранения угрозы E_i на i-м шаге (этапе) обслуживания:

$$E_i = I_S \cdot W \cdot \left(l_i p_i + \sum_{j=1}^{j<i} \left(l_{ji} \cdot (p_i \cdot \overline{p_j}) + \sum_{q=1}^{q<j} \left(\begin{array}{l} l_{qji} \cdot (p_i \cdot \overline{p_j} \cdot \overline{p_q}) + \\ + ... + \sum\limits_{m=1}^{m<t} (l_{mt...i} \cdot (p_i \cdot \overline{p_j} \cdot ... \cdot \overline{p_m}) \end{array} \right) \right) ... \right).$$

Аналитическая модель оценки надежности схемы безопасного доступа во внешнюю сеть. При оценке надежности считаем, что отказы различных узлов независимы, а поток отказов распределен по экспоненциальному закону. Надежность СЗИ при условии, что маршрутизаторы в каждой из групп одинаковы, определим для не восстанавливаемых (P_{S1}) и восстанавливаемых (P_{S2}) систем соответственно, как:

$$P_{S1} = \prod_i \sum_{a=1}^{n_{C_i}} \delta_{C_i} C_{n_{C_i}}^a r_{C_i}{}^a (1 - r_{C_i})^{n_{01} - a} \cdot \prod_j \sum_{b=1}^{n_{M_j}} \delta_{M_j} C_{n_{M_j}}^b r_0{}^b (1 - r_0)^{n_{M_j} - b},$$

$$P_{S2} = \prod_i \left(\begin{array}{l} (\sum\limits_{a=1}^{n_{C_i}} \delta_{C_i} C_{n_{C_i}}^a k_{C_i}{}^a (1 - r_{C_i})^{n_{01} - a}) \cdot \\ \cdot (\sum\limits_{a=1}^{n_{C_i}} \delta_{C_i} C_{n_{C_i}}^a r_{C_i}{}^a (1 - r_{C_i})^{n_{01} - a}) \end{array} \right) \cdot \prod_j \left(\begin{array}{l} (\sum\limits_{b=1}^{n_{M_j}} \delta_{C_i} C_{n_{C_i}}^a k_0{}^b (1 - r_{C_i})^{n_{M_j} - b}) \cdot \\ \cdot (\sum\limits_{b=1}^{n_{M_j}} \delta_{C_i} C_{n_{C_i}}^a r_0{}^b (1 - r_{C_i})^{n_{M_j} - b}) \end{array} \right).$$

Здесь для невосстанавливаемой системы $r_j = e^{-\lambda_j T_{Sys}}$, а для восстанавливаемой системы $r_j = e^{-\lambda_j T_{S_j}}$ и при неограниченном восстановлении $k_j = \mu_j / (\mu_j + \lambda_j)$, где λ_0 – интенсивность отказов маршрутизаторов; λ_i – средств ЗИ, $i = 1 \ldots n$, где n – число элементов ЗИ в составе СЗИ; T_{Sys} – время с момента запуска СЗИ; T_{Sj} – среднее требуемое время безотказной работы j-го узла СЗИ; C_i – порядковый номер аппаратно-программного элемента ЗИ, использующегося в схеме СЗИ; M_i – порядковый номер группы маршрутизаторов, использующейся в схеме СЗИ; μ_0 – интенсивность восстановления маршрутизаторов; μ_i – средств ЗИ; $\delta_{i1}, \delta_{i2}, \delta_{i01}, \delta_{i02}$ условия обеспечения стационарности режима работы узлов, принимающих значение «1», если условия стационарности выполняются и «0» – в противном случае.

Аналитические модели оценки задержек обслуживания в схемах безопасного доступа во внешнюю сеть. При рассмотрении схем доступа каждый узел корпоративной сети представим системой массового обслуживания (далее, СМО) типа M/M/1 с бесконечной очередью, для которой задержки обслуживания определим через среднее время пребывания запросов в системе. При прохождении запросов через несколько узлов среднее время пребывания в системе определяется как сумма времен пребывания в узлах, которые последовательно задействованы в его обслуживании. Таким образом, с учетом снижения интенсивности входного потока при прохождении через

каждое из использованных в схеме средств ЗИ и распределении потока запросов на обслуживание в *n*-узлов (в результате их резервирования), получим: $T_{\text{общ}} = \sum_i \nu_i / (1 - \lambda_i \cdot \nu_i / n_i)$, где $\nu_i = 1/\mu_i$ – среднее время обслуживания запроса в *i*-м узле, $\lambda_i = d_{i-1} \cdot \lambda$ – интенсивность потока запросов на *i*-м узле, $d_i = P_{S_i}$ – доля входного потока, оставшаяся после прохождения через *i*-задействованных в работе элементов ЗИ, в составе СЗИ, определяемая по вероятности обнаружения и устранения угроз СЗИ.

В дополнении к показанной аналитической модели, в схеме доступа «Связующий узел» каждый вычислительный узел («связующий узел») можно представить в виде одноканальной СМО с общей бесконечной очередью и поэтапным выполнением запросов. Процесс обслуживания запроса системой защиты, включающей *R*-этапов, в таком случае будет иметь вид:

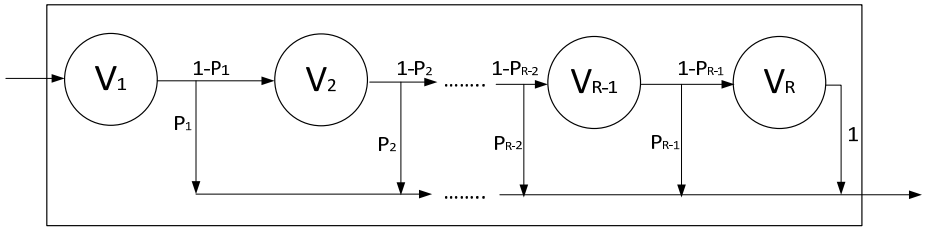


Рисунок 4 – Процесс обслуживания запроса системой защиты, включающей *R*-этапов: $V_1, \ldots, V_R$ – время обработки на этапах системы защиты; $P_1, \ldots, P_{R-1}$ – вероятность прохождения запросом *i*-го этапа системы защиты, $i = 1, \ldots, R$

Рассматриваемая модель поэтапного обслуживания – частный случай СМО типа M/G/1, поэтому для нахождения среднего времени пребывания запроса в системе *T* можно воспользоваться формулой Полячика–Хинчина. Таким образом, с учетом резервирования вычислительных узлов, получим, что: $T = \bar{x} + \lambda \cdot (\bar{x})^2 \cdot (1 + \sigma_b^2 / (\bar{x})^2) / 2 \cdot (M - \lambda \cdot \bar{x})$, где $\bar{x}$ – среднее время обслуживания; $\rho = \lambda \cdot \bar{x}$ – коэффициент использования $(\rho < 1)$, здесь λ – интенсивность входного потока; σ_b^2 – дисперсия времени обслуживания.

Предположим, что время обслуживания каждого этапа – детерминированная величина $V_i = \text{const}$. Тогда среднее время и дисперсию *R*-этапного обслуживания определим как:

$$\bar{x} = V_1 \cdot E_1 + \left(\sum_{i=2}^{R-1} E_i \left(\prod_{j=1}^{i=1} (1 - E_j) \right) \sum_{q=1}^{i} V_q \right) + \sum_{i=1}^{R} V_i \left(\prod_{j=1}^{R-1} (1 - E_j) \right),$$

$$\sigma_b^2 = (V_1 - \bar{x})^2 \cdot E_1 + \sum_{i=2}^{R-1} E_i \left(\prod_{j=1}^{i-1} (1 - E_j) \right) \cdot \left(\sum_{q=1}^{i} V_q - \bar{x} \right)^2 + \left(\sum_{i=1}^{R} V_i - \bar{x} \right)^2 \cdot \prod_{i=1}^{R-1} (1 - E_j).$$

Здесь E_i – вероятность устранения угрозы на *i*-м этапе обслуживания.

Предположим, что среднее время выполнения этапов распределено по показательному закону. Тогда, с учетом резервирования вычислительных узлов, среднее время пребывания запроса в системе будет равно:

$T_S = \bar{x} + \lambda \cdot x^{(2)} / 2 \cdot (M - \lambda \cdot \bar{x})$, где $x^{(2)}$ – второй начальный момент.

Используя распределение Кокса, получаем преобразование Лапласа для плотности распределения вероятностей времени обслуживания в виде:

$$B(s) = \left(\frac{\mu_1}{s + \mu_1}\right) E_1 + \left(\sum_{i=2}^{R-1} E_i \left(\prod_{j=1}^{i=1} (1 - E_j) \right) \prod_{j=1}^{i-1} \left(\frac{\mu_j}{s + \mu_j}\right) \right) + \prod_{i=1}^{R} \left(\frac{\mu_i}{s + \mu_i}\right) \left(\prod_{j=1}^{R-1} (1 - E_j) \right).$$

Для вычисления *n*-го начального момента случайной величины, воспользуемся следующей формулой: $\overline{X^n} = (-1)^n A^{*(n)}(0)$.

Первая производная преобразования Лапласа для плотности распределения вероятностей времени обслуживания соответствует первому начальному моменту, а также математическому ожиданию, а вторая производная – второму начальному моменту.

Распределение вычислительной нагрузки на вычислительном узле. В случае единовременного использования на «связующем узле» нескольких средств ЗИ (например, предполагается их конвейерное/параллельное использование и/или каждое из средств ЗИ располагается на отдельной виртуальной машине, запущенной на вычислительном узле), возникает задача распределения вычислительных ресурсов «связующего узла» между средствами ЗИ, которыми он укомплектован.

Пусть общее количество ресурсов, выделяемых на сервере («связующем узле») на реализацию функций информационной защиты, имеет ограничение *Q*, а для поддержания нормального уровня функциональности (работоспособности) средств ЗИ требуется: $\sum_i n_i \cdot q_i \le Q$, где q_i – затраты ресурсов сервера на поддержание нормальной работоспособности *i*-го программного обеспечения (далее, ПО), n_i – число копий (в случае резервирования) *i*-го ПО; $q_i \ge r_i$, где r_i – минимальное количество ресурсов сервера, необходимых для работы *i*-го ПО.

Тогда в условиях ограниченности ресурсов общее снижение потенциально возможной производительности для всей совокупности ПО защиты будет: $k_i = k = Q / \sum_i q_i \cdot n_i$. При разграничении ресурсов на различное ПО защиты, снижение потенциального уровня возможной производительности *i*-го ПО определим как: $k_i = u_i / q_i \cdot n_i$, где $k_i \le 1$; $u_i \ge r_i \cdot n_i$ – количество выделяемых ресурсов для работы *i*-го ПО.

В **четвертой главе** рассмотрены методы выбора и оптимизации вариантов построения схем доступа, основывающиеся на частных и комплексных критериях эффективности, показана эффективность применения тех или иных из рассматриваемых вариантов схем доступа в ВС.

Метод выбора вариантов построения схем доступа по показателям информационной безопасности. Разработанная математическая модель для оценки уровня информационной защищенности зависит от количества элементов ЗИ, использующихся в СЗИ. Оценим, например, СЗИ, использующую схему доступа «Связующий узел», укомплектованную двумя видами ПО, установленных на «связующем узле» и двумя ГМ. В таком случае получим:

$$E_{S_3} = I_S \cdot W \cdot (p_2 \cdot (L_2 - l_{23} - l_{12} + l_{123}) + (1 - p_1) \cdot (L_1 - l_{12} - l_{13} + l_{123}) + p_3 \cdot (L_3 - l_{23} - l_{13} + l_{123}) + (l_{12} - l_{123}) \cdot (1 - \overline{p}_1 \cdot \overline{p}_2) + (l_{13} - l_{123}) \cdot (1 - \overline{p}_1 \cdot \overline{p}_3) + (l_{23} - l_{123}) \cdot (1 - \overline{p}_2 \cdot \overline{p}_3) + l_{123} \cdot (1 - \overline{p}_1 \cdot \overline{p}_2 \cdot \overline{p}_3))$$

При множестве угроз, которые способно обнаружить и устранить средство – $A_1 = 25\%$; $A_2 = 50\%$; $A_3 = 80\%$; вероятности обнаружения угроз средством ЗИ – $p_1 = 0.9$; $p_2 = 0.925$; $p_3 = 0.925$; доли угроз от общего множества угроз ИБ, которые обнаруживаются и устраняются несколькими средствами, в составе СЗИ – $l_{123} = 22.5\%$; $l_{12} = 22.5\%$; $l_{13} = 25\%$; $l_{23} = 30\%$; вероятности обнаружения СЗИ угроз ИБ, которым может быть подвержена ВС – $I_S = 100\%$; доле угроз ИБ в поступающем потоке запросов – $W = 100\%$; $\overline{p}_i = (1 - p_i)$, получим, что уровень информационной защищенности при одновременном использовании ПО-1 и ПО-2, в составе системы защиты, равен: $Es_2 = 0.9486$, при использовании на вычислительном узле только ПО-1: $Es_1 = 0.5004$, при использовании только ПО-2: $Es_1 = 0.7569$.

Метод выбора и оптимизации вариантов построения схем доступа по показателю временных задержек в системе. Расчет вносимых задержек схемой доступа «Прямое соединение» и «Типовой» схемой доступа, требует оптимизации. Оптимизация системы защиты включает поиск распределения числа узлов каждого типа, обеспечивающего минимум среднего времени пребывания запросов в системе (T_S) при условии ограничений на нагрузку на каждый элемент системы и стоимость реализации системы $C_i \le C$ и соблюдения условий стационарности режима обслуживания: $Minimize: T(n_1, n_2, ..., n_S)$ при условии, что $C_i \le C$ и $\lambda_i \cdot \nu_i / n_i \le 1$, где λ_i – интенсивность входного потока на *i*-м элементе СЗИ.

В таком случае, для «Типовой» схемы и, например, для вариантов схемы доступа «Прямое соединение», включающих одну, две группы маршрутизаторов и два средства ЗИ (DC-2), с учетом фильтрации входного потока на этапах последовательного прохождения через средства СЗИ, когда после первого средства поток уменьшается в d_1, после второго – в d_2 и так далее, средние задержки обслуживания вычислим как:

$$T_{STD} = \frac{\nu_1}{1-\lambda\cdot\nu_1/n_{11}} + \frac{\nu_3}{1-d_1\cdot F_2} + \frac{\nu_1}{1-d_2\cdot\lambda\cdot\nu_1/n_{11}},$$

$$T_{DC-1} = \frac{\nu_1}{1-\lambda\cdot\nu_1/n_{11}} + \frac{\nu_2}{1-d_1\cdot F_1} + \frac{\nu_1}{1-d_2\cdot\lambda\cdot\nu_1/n_{11}} + \frac{\nu_3}{1-d_3\cdot F_2} + \frac{\nu_1}{1-d_4\cdot\lambda\cdot\nu_1/n_{11}},$$

$$T_{DC-2} = \frac{\nu_1}{1-\lambda\cdot\nu_1/n_{11}} + \frac{\nu_2}{1-d_1\cdot F_1} + \frac{\nu_1}{1-d_2\cdot\lambda\cdot\nu_1/n_{11}} + \frac{\nu_3}{1-d_3\cdot F_2} + \frac{\nu_1}{1-d_4\cdot\lambda\cdot\nu_1/n_{12}},$$

где $F_1 = \nu_2 / n_2$; $F_2 = \nu_3 / n_3$, n_{1i}, n_2, n_3 – число маршрутизаторов в каждой из *i*-ой групп, С-1, С-2; $d_i = P_{S_i}$ – доля входного потока, оставшаяся после прохождения через *i*-задействованных в работе элементов ЗИ, в составе СЗИ.

Таким образом, уменьшение входного потока при прохождении средств СЗИ для данной системы, определим как:

$$\begin{aligned}
d_1 &= 1 - I_S \cdot W \cdot L_1 \cdot p_1;\\
d_2 &= 1 - I_S \cdot W \cdot (p_2 \cdot (L_2 - l_{12}) + p_1 \cdot (L_1 - l_{12}) + l_{12} \cdot (1 - \overline{p}_1 \cdot \overline{p}_2));\\
d_3 &= 1 - I_S \cdot W \cdot (p_2 \cdot (L_2 - l_{12}) + p_1 \cdot (L_1 - l_{12}) + l_{12} \cdot (1 - \overline{p}_1 \cdot \overline{p}_2));\\
d_4 &= 1 - I_S \cdot W \cdot (p_2 \cdot M_{e1} + p_1 \cdot R_e + p_3 \cdot M_{e2} + (l_{12} - l_{123}) \cdot (1 - \overline{p}_1 \cdot \overline{p}_2) +\\
&\quad + (l_{13} - l_{123}) \cdot (1 - \overline{p}_1 \cdot \overline{p}_3) + (l_{23} - l_{123}) \cdot (1 - \overline{p}_2 \cdot \overline{p}_3) + l_{123} \cdot (1 - \overline{p}_1 \cdot \overline{p}_2 \cdot \overline{p}_3)),
\end{aligned}$$

где $R_e = (L_1 - l_{12} - l_{13} + l_{123})$, $M_{e1} = (L_2 - l_{23} - l_{12} + l_{123})$, $M_{e2} = L_3 - l_{23} - l_{13} + l_{123}$ (см. диаграмму Венна – Рисунок 3); $\overline{p}_i = (1 - p_i)$.

Учтем условия стационарности обслуживания для каждого из вариантов построения схемы доступа «Прямое соединение» (DC-1 и DC-2) и «Типовой» схемы доступа (STD):

$$\begin{aligned}
&\text{DC-1)}\ \lambda\cdot\nu_1/n_{11} < 1,\ d_1\cdot\lambda\cdot\nu_2/n_2 < 1,\ \lambda\cdot\nu_1\cdot(1+d_2)/n_{11} < 1,\ d_3\cdot\lambda\cdot\nu_3/n_3 < 1,\\
&\lambda\cdot\nu_1\cdot(1+d_2+d_4)/n_{11} < 1,\ C_{1D} = c_1\cdot n_{11} + c_2\cdot n_2 + c_3\cdot n_3;\\
&\text{DC-2)}\ \lambda\cdot\nu_1/n_{11} < 1,\ d_1\cdot\lambda\cdot\nu_2/n_2 < 1,\ \lambda\cdot\nu_1\cdot(1+d_2)/n_{11} < 1,\ \lambda\cdot\nu_1\cdot(1+d_2+d_4)/n_{12} < 1,\\
&C_{2D} = c_1\cdot(n_{11}+n_{12}) + c_2\cdot n_2 + c_3\cdot n_3,\ d_3\cdot\lambda\cdot\nu_3/n_3 < 1;\\
&\text{STD)}\ \lambda\cdot\nu_1/n_{11} < 1,\ d_1\cdot\lambda\cdot\nu_3/n_3 < 1,\ C_{STD} = c_1\cdot n_{11} + c_3\cdot n_3.
\end{aligned}$$

где стоимости маршрутизаторов – c_1, средств ЗИ первого типа – c_2, средств ЗИ второго типа – c_3.

Зависимость задержек обслуживания от интенсивности входного потока при аналогичных параметрах СЗИ и среднем времени обслуживания маршрутизатора – $\nu_1 = 0{,}025$ с., средства ЗИ первого типа – $\nu_2 = 0{,}04$ с., средства ЗИ второго типа –

$\nu_3 = 0{,}075$ с.; стоимости маршрутизатора – $c_1 = 10$ у.е., средства ЗИ первого типа – $c_2 = 20$ у.е., средство ЗИ второго типа – $c_3 = 35$ у.е.; ограничении средств на построение системы $C = 500$ у.е.; доле угроз ИБ в поступающем потоке запросов – $W = 20\%$, представлена на рис. 5.

Оценим временные задержки обслуживания нескольких вариантов комплектации и последовательной активации ПО «связующего узла», укомплектованного тремя видами ПО при различных распределениях среднего времени задержки обслуживания (является детерминированной величиной или имеет показательное распределение) каждым из ПО «связующего узла». Для примера расчета предположим, что СЗИ ВС включает три элемента ЗИ ($R = 3$).

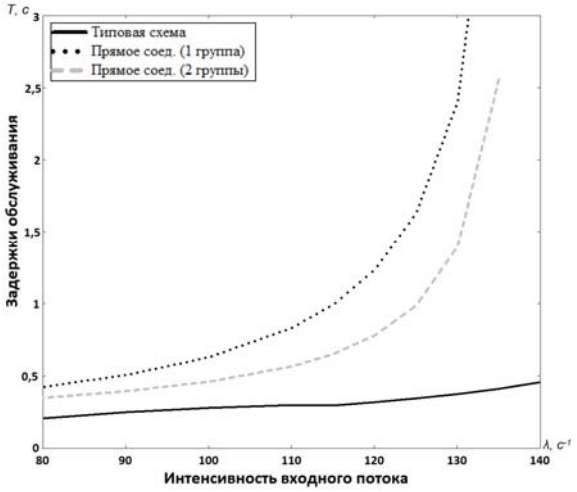


Рисунок 5 – Зависимость задержек обслуживания от интенсивности входного потока для схемы доступа «Прямое соединение»

Предположим, что среднее время задержки обслуживания каждого из ПО «связующего узла» – детерминированная величина. Тогда среднее время и дисперсия могут быть найдены, как:

$$\bar{x} = V_1 \cdot E_1 + (V_1 + V_2) \cdot (1 - E_1) \cdot E_2 + (V_1 + V_2 + V_3) \cdot (1 - E_1) \cdot (1 - E_2);$$

$$\sigma_b^2 = (V_1 - \bar{x})^2 \cdot E_1 + (V_1 + V_2 - \bar{x})^2 \cdot (1 - E_1) \cdot E_2 + (V_1 + V_2 + V_3 - \bar{x})^2 \cdot (1 - E_1) \cdot (1 - E_2),$$

где $E_1 = I_S \cdot W \cdot p_1 \cdot L_1$; $E_2 = I_S \cdot W \cdot \left(p_2 \cdot (L_2 - l_{12}) + l_{12} \cdot \left(1 - (1 - p_1)(1 - p_2)\right)\right)$.

В результате при: доле угроз ИБ в поступающем потоке запросов – $W = 10\%$; вероятности обнаружения СЗИ угроз ИБ, которым может быть подвержена ВС – $I_S = 90\%$, среднем времени обслуживания средством ЗИ – $V_1 = 0{,}0075$ с., $V_2 = 0{,}012$ с., $V_3 = 0{,}0225$ с.; вероятности обнаружения угроз средством ЗИ – $p_1 = 90\%$, $p_2 = 95\%$, $p_3 = 92{,}5\%$; множестве угроз, которые способно обнаружить и устранить средство – $A_1 = 35\%$, $A_2 = 50\%$; доля угроз от общего множества угроз ИБ, которые обнаруживается и устраняется первым и вторым средством ЗИ – $l_{12} = 15\ \%$, получим, что: $\bar{x} = 0{,}0399$ с., а $\sigma_b^2 = 5{,}6548 \cdot 10^{-5}$ с^2.

Если среднее время задержки обслуживания каждого из ПО «связующего узла» имеет показательное распределение, то получим, что первая производная преобразования Лапласа для плотности распределения вероятностей времени обслуживания (которая при подстановке $s = 0$ соответствует первому начальному моменту) для системы, включающей три этапа обслуживания, будет равна:

$$B'(s)=\frac{E_1\cdot\mu_1}{(\mu_1+s)^2}+\frac{\mu_1\cdot\mu_2\cdot E_2\cdot(1-E_1)}{(\mu_1+s)\cdot(\mu_2+s)^2}+\frac{\mu_1\cdot\mu_2\cdot E_2\cdot(1-E_1)}{(\mu_1+s)^2\cdot(\mu_2+s)}+\frac{(1-E_2)\cdot(1-E_1)\cdot\mu_1\cdot\mu_2\cdot\mu_3}{(\mu_1+s)\cdot(\mu_2+s)\cdot(\mu_3+s)^2}-$$
$$-\frac{\mu_3}{\mu_3+s}\cdot(-\frac{(1-E_2)\cdot(1-E_1)\cdot\mu_1\cdot\mu_2}{(\mu_1+s)\cdot(\mu_2+s)^2}-\frac{(1-E_2)\cdot(1-E_1)\cdot\mu_1\cdot\mu_2}{(\mu_1+s)^2\cdot(\mu_2+s)})$$

Таким образом, среднее время обслуживания:

$$\bar{x}=V_1\cdot E_1+(V_1+V_2)\cdot(1-E_1)\cdot E_2+(V_1+V_2+V_3)\cdot(1-E_1)\cdot(1-E_2).$$

Вторая производная преобразования Лапласа для плотности распределения вероятностей времени обслуживания (которая при подстановке $s=0$ соответствует второму начальному моменту) для системы, включающей три этапа обслуживания, будет равна:

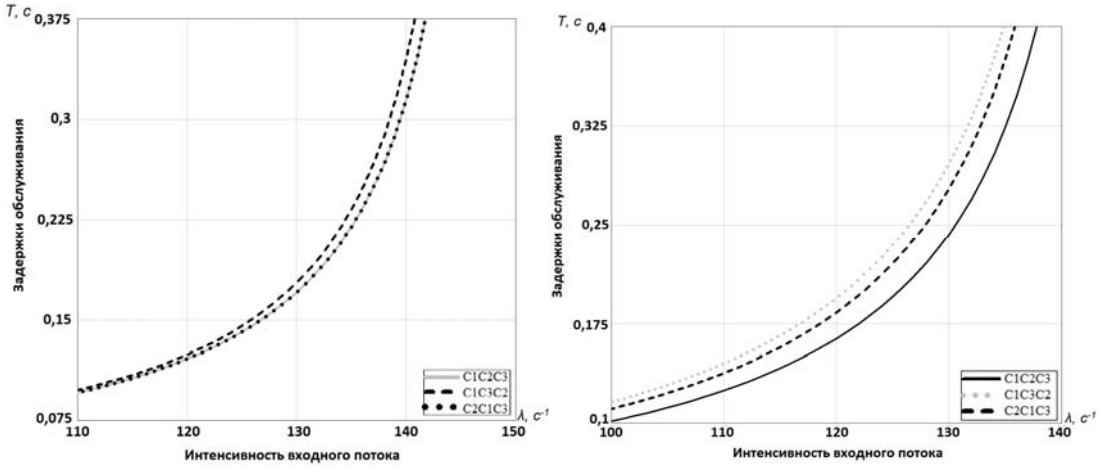
$$B''(s)=\frac{\mu_1}{\mu_1+s}\cdot(\frac{2\cdot E_1}{(\mu_1+s)^2}+\frac{2\cdot\mu_2\cdot E_2\cdot(1-E_1)}{(\mu_2+s)^3}+\frac{2\cdot\mu_2\cdot E_2\cdot(1-E_1)}{(\mu_1+s)\cdot(\mu_2+s)^2}+\frac{2\cdot\mu_2\cdot E_2\cdot(1-E_1)}{(\mu_1+s)^2\cdot(\mu_2+s)}+$$
$$+\frac{\mu_2\cdot\mu_3\cdot(1/(\mu_2+s)+1/(\mu_1+s))\cdot(1-E_1)\cdot(1-E_2)}{(\mu_3+s)^2\cdot(\mu_2+s)}+\frac{\mu_2\cdot\mu_3\cdot(1-E_1)\cdot(1-E_2)}{(\mu_2+s)^2\cdot(\mu_3+s)^2}+$$
$$\frac{2\cdot\mu_2\cdot\mu_3\cdot(1-E_1)\cdot(1-E_2)}{(\mu_2+s)\cdot(\mu_3+s)}\cdot(\frac{1}{(\mu_2+s)^2}+\frac{1}{(\mu_1+s)\cdot(\mu_2+s)}+\frac{1}{(\mu_1+s)^2})+$$
$$+\frac{2\cdot\mu_2\cdot\mu_3\cdot(1-E_1)\cdot(1-E_2)}{(\mu_2+s)\cdot(\mu_3+s)^3}+\frac{\mu_2\cdot\mu_3\cdot(1-E_1)\cdot(1-E_2)}{(\mu_1+s)\cdot(\mu_2+s)\cdot(\mu_3+s)^2})$$

Таким образом, второй начальный момент:

$$x^{(2)}=2\cdot(V_1^2\cdot(E_1+E_2\cdot(1-E_1))+V_2^2\cdot E_2\cdot(1-E_1)+V_1\cdot V_2\cdot E_2\cdot(1-E_1)+V_3^2\cdot(1-E_1)\cdot(1-E_2))+$$
$$+(V_1^2+V_1\cdot V_2+V_2^2)\cdot(1-E_1)\cdot(1-E_2)+2\cdot V_3\cdot(V_1+V_2)\cdot(1-E_1)\cdot(1-E_2)$$

При аналогичных параметрах “связующего узла”, получим, что: $\bar{x}=0,0402$ с., а $\sigma_b^2=8,2109\cdot10^{-4}$ с^2.

Зависимость задержек вносимых «связующим узлом» от интенсивности входного потока при различных последовательностях поэтапного применения трех средств защиты (С-1:С-2:С-3; С-1:С-3:С-2; С-2;С-1;С-3), использующихся на «связующем узле» при условии, что среднее время задержки обслуживания каждого из ПО «связующего узла» – детерминированная величина (а) и, если среднее время задержки обслуживания каждого из ПО «связующего узла» имеет показательное распределение (б), показана на рис. 6:



(а) (б)

Рисунок 6 – Зависимость интенсивности входного потока и задержек, вносимых «связующим узлом»

Оценим эффективность вычислительного узла с точки зрения распределения вычислительных ресурсов. Пусть на «вычислительном узле», используются два средства ЗИ. Результаты расчета при аналогичных параметрах СЗИ и интенсивности входного потока – $\lambda = 50\ c^{-1}$.; доле угроз ИБ в поступающем потоке запросов – $W = 40\%$; среднем времени обслуживания: маршрутизатором – $V_M = 0{,}015\ c.$, первым средством ЗИ – $\nu_1 = 0{,}025\ c.$, вторым средством ЗИ – $\nu_2 = 0{,}05\ c.$; стоимости маршрутизатора – $c_1 = 15$ у.е. и стоимости "вычислительного узла" – $c_2 = 90$ у.е.; и ограничении средств на построение системы $C = 400$ у.е.

Если ресурсов вычислительного узла хватает для полноценной работы ПО-1 и ПО-2: $q_1 = 35$, $r_1 = 20$ и $q_2 = 65$, $r_2 = 30$, а $Q = 100$, то задержки обслуживания будут равны $T_s = 0{,}185\ c$. Если ресурсов вычислительного узла недостаточно для полноценной работы двух ПО: $q_1 = 40$, $r_1 = 20$ и $q_2 = 70$, $r_2 = 35$, а $Q = 100$, то задержки обслуживания равны: $T_{s1.1} = 0{,}204\ c$, когда допускаем снижение производительности ПО-1 и $T_{s1.2} = 0{,}224\ c$, когда снижаем производительность ПО-2. Во втором случае, когда оба ПО используются на одинаковом уровне производительности $T_{s2} = 0{,}214\ c$.

Метод выбора и оптимизации варианта построения схем доступа по показателю надежности. Оценим надежность «Типовой» схемы доступа и различных вариантов схемы доступа «Связующий узел», рассчитав вероятность их безотказной работы.

Для вариантов построения схемы доступа «Связующий узел» надежность системы будет равна:

$P_{1C_{nr}} = P_{01}(T_{Sys}) \cdot P_{m1}(T_{Sys})$; $P_{2C_{nr}} = P_{01}(T_{Sys}) \cdot P_{m1}(T_{Sys}) \cdot P_{02}(T_{Sys})$ – для типового варианта «Связующего узла», а случае использования дополнительного МЭ (гибридный вариант «Связующего узла»), установленного перед «связующим узлом», надежность получим как:

$$P_{3C_{nr}} = P_{01}(T_{Sys}) \cdot P_{m1}(T_{Sys}) \cdot P_{m2}(T_{Sys});\ P_{4C_{nr}} = P_{01}(T_{Sys}) \cdot P_{m1}(T_{Sys}) \cdot P_{m2}(T_{Sys}) \cdot P_{02}(T_{Sys}).$$

Для «Типовой» схемы доступа надежность может быть найдена как: $P_{STD_{nr}} = P_{01}(T_{Sys}) \cdot P_{m1}(T_{Sys})$.

Оптимизация системы защиты включает поиск распределения числа узлов каждого типа, обеспечивающего максимум надежности всей системы (P_S) при условии ограничения стоимости реализации системы $C_i \le C$ и соблюдения условий стационарности режима обслуживания, с учетом предельно возможной нагрузки на каждый элемент системы: $Maximize: P(n_1, n_2, ..., n_S)$ при условии, что $C_i \le C$ и $\lambda_i \cdot \nu_i / n_i \le 1$. Накладываемые ограничения на обеспечения стационарности режима работы узлов, условия $\delta_{i1}, \delta_{i2}, \delta_{i01}, \delta_{i02}$, определяются исходя из требований для схем доступа.

Для СЗИ, использующей различные варианты построения схемы доступа «Связующий узел» (гибридный вариант и типовой вариант схемы доступа) и «Типовой» схемы доступа, результаты расчетов надежности при интенсивности отказов маршрутизаторов, «вычислительного узла» и межсетевого экрана: $\lambda_0 = 10^{-4}$, $\lambda_1 = 1{,}25 \cdot 10^{-4}$; $\lambda_2 = 8 \cdot 10^{-5}$; и времени работы системы $t = 1000$ часов, а также представленных ранее ограничений на пропускную способность узлов СЗИ и финансовые ограничения на проектирование СЗИ, будут иметь вид:

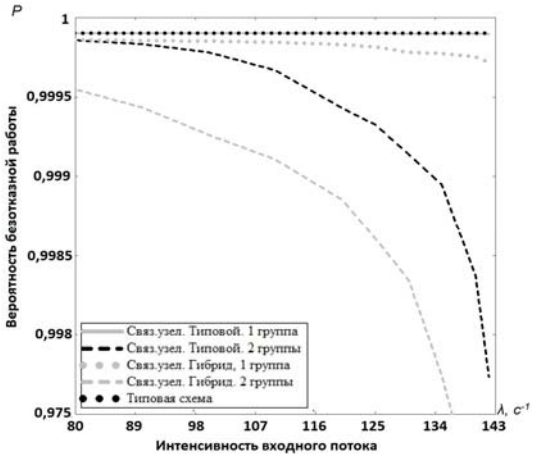


Рисунок 7 – Зависимость вероятности безотказной работы СЗИ от интенсивности входного потока при проектировании различных вариантов схемы доступа «Связующий узел».

Метод выбора и оптимизации вариантов построения схем доступа по показателям временных задержек в системе, безопасности и надежности. Сравнение эффективности различных схем доступа – «Типовой», «Прямое соединение» (использующую, одну ГМ и два средства ЗИ) и «Связующий узел» (в типовом и гибридном исполнении, использующие одну ГМ и три средства ЗИ, размещенных на «вычислительном узле»), используя комплексный критерий эффективности учитывающий уровень защищенности ВС, вносимые схемой доступа задержки обслуживания и оперативную готовность СЗИ ($Q_s = k_г \cdot P(T_S) \cdot E_{S_R} \cdot (T_0 - T_S)/T_0$), используя те же параметры СЗИ для каждой из рассмотренных схем доступа и предполагая, что: между маршрутизаторами и «связующим узлом» нет общих множеств угроз ИБ и $A_0 = 5\%$, в то время как между межсетевым экраном и маршрутизатором она есть – $l_{04} = 5\%$, а $A_4 = 10\%$; между межсетевым экраном и «связующим узлом» – общих множеств угроз также нет; стоимость каждого элемента ЗИ и ограничение на общую стоимость СЗИ равно: $C = 500$ у.е., для схемы доступа «Прямое соединение»: $c_1 = 10$ у.е., $c_2 = 20$ у.е., $c_3 = 35$ у.е.; для схемы доступа «Связующий узел»: $c_1 = 10$ у.е., $c_2 = 50$ у.е., $c_3 = 35$ у.е., где c_1, c_2, c_3 – стоимость маршрутизатора, «связующего узла» (или средства ЗИ первого типа), межсетевого экрана (или средства ЗИ второго типа), соответственно; доля угроз ИБ в поступающем потоке запросов – $W = 0.1$, а вероятность обнаружения СЗИ угроз ИБ, которым может быть подвержена ВС: $I_S = 1$ (для схем доступа «Прямое соединение» и «Связующий узел») и $I_S = 0{,}85$ (для «Типовой» схемы доступа), для «связующего узла» – $I_S = 0.95$ интенсивность восстановления элементов системы: $\mu = 1$ час, показано на рис. 8.

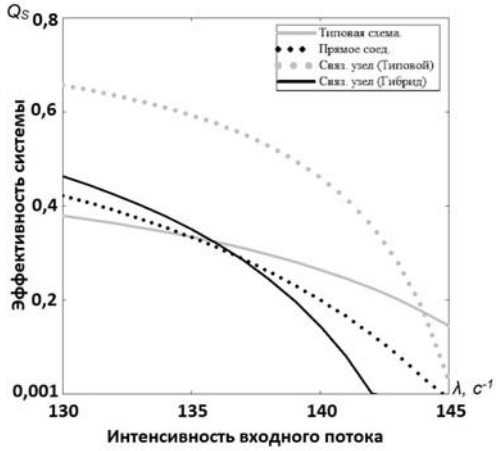


Рисунок 8 – Зависимость эффективности СЗИ от интенсивности входного потока для различных схем доступа

ЗАКЛЮЧЕНИЕ

В диссертационном исследовании предложены модели и методы оценки эффективности СЗИ и обоснования их комплектации, результаты которого позволят повысить качество проектирования и модернизации СЗИ при налагаемых ограничениях на задержки обслуживания, вносимые СЗИ и обеспечение требуемого уровня информационной защищенности, безопасности и надежности ВС.

Сформированы частные и комплексные критерии оценки эффективности СЗИ, учитывающие: информационную защищенность ВС, вносимые задержки обслуживания и оперативную готовность, и вероятность безотказной работы СЗИ.

Построены математические модели:

– Задержек обслуживания СЗИ, учитывающие: пересекаемость множеств угроз ИБ, обнаруживаемых и устраняемых средствами ЗИ и различные варианты комплектации СЗИ средствами ЗИ;

– Защищенности ВС, основывающаяся на вероятности обнаружения угроз ИБ средствами ЗИ СЗИ и учитывающая пересекаемость множеств угроз, обнаруживаемых и устраняемых средствами ЗИ, которыми укомплектована СЗИ.

– Надежности СЗИ, позволяющие оценить вероятность безотказной работы СЗИ и оперативную готовность СЗИ при условии налагаемых ограничений на нагрузку в промежуточных узлах СЗИ, основываясь на построенных математических моделях оценки задержек обслуживания, и финансовых ограничений на проектирование СЗИ.

Предложен метод построения СЗИ, заключающийся в применении комплексных и частных критериев оценки эффективности СЗИ, использующих разработанные методы и аналитические модели, с целью получения оценок эффективности работы СЗИ и, в результате, снижения экономических затрат на их проектирование и модификацию.

Проведен сравнительный анализ возможностей и эффективности нескольких схем безопасного доступа – «Прямое соединение», «Связующий узел» и «Типовая» – в результате которого было выявлено, что:

– Схему доступа «Прямое соединение» целесообразно применять в случае невозможности внесения кардинальных изменений в сетевую структуру корпоративной сети и необходимости создания высоко масштабируемой СЗИ, с возможностью создания целевых решений для различных частей ВС.

– Схему доступа «Связующий узел» целесообразно применять в случае необходимости создания высокоэффективной, гибкой и быстро реконфигурируемой СЗИ, способной обеспечить требуемый уровень защищенности и надежности ВС, с достижением приемлемого уровня вносимых задержек обслуживания.

– Схему доступа «Типовая» целесообразно применять в случае невозможности усложнения архитектуры ВС и жестких материальных ограничений на проектирование СЗИ при смещении практически всех функций по обеспечению защиты ВС на оконечные узлы системы.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в изданиях, рекомендованных ВАК

1. Коломойцев В.С., Богатырев В.А. Оценка эффективности и обоснование выбора структурной организации системы многоуровневого защищенного доступа к ресурсам внешней сети // Информация и космос. – 2015. – № 3. – С. 71-79.

2. Коломойцев В.С., Богатырев В.А. Вероятностно-временные показатели при поэтапном применении средств защиты информации // Вестник компьютерных и информационных технологий. – 2017. – № 11(161). – С. 37-43.

3. Коломойцев В.С. Выбор варианта построения многоуровневого защищенного доступа к внешней сети // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16. – № 1(101). – С. 115-121.

4. Коломойцев В. С., Богатырев В. А. Эффективность поэтапного применения средств защиты с пересечением областей обнаружения угроз // Программные продукты и системы. – 2018. – Т. 32. – № 3. – С. 557-564.

Статьи в изданиях, рекомендованных Scopus/WoS

5. Kolomoitcev V.S., Bogatyrev V.A. The fault-tolerant structure of multilevel secure access to the resources of the public network // Communications in Computer and Information Science. – 2016, Vol. 678, pp. 302-313.

6. Kolomoitcev V.S., Bogatyrev V.A. A Fault-tolerant Two-tier Pattern Of Secure Access 'Connecting Node' // ACSR-Advances in Computer Science Research. – 2017, Vol. 72, pp. 271-274.

7. Kolomoitcev V.S., Bodrov K.U., Krasilnikov A.V. Calculating the probability of detection and removal of threats to information security in data channels // Proceedings of the 19th International Conference on Soft Computing and Measurements, SCM 2016. – 2016, pp. 25-27.

8. Saitgalina A.K., Tolstoba N.D., Butova D.V., Orekhova M.K., Lyamets D.A., Kozhina A.D., Kolomoitcev V.S., Shevchenko D.N., Krivtcova R.S., Stepanenko M.A., Kochnev K.A., Beliaeva A.S. Design and implementation of a modular interactive labyrinth targeted for use in optical education // Proceedings of SPIE. – 2017, Vol. 10452, pp. 104524D.

Публикации в других издания

9. Коломойцев В.С. Сравнительный анализ подходов к организации безопасного подключения узлов корпоративной сети к сети общего доступа // Кибернетика и программирование. – 2015. – № 2. – С. 46-58.

10. Kolomoitcev V.S., Bogatyrev V.A. The Fault-tolerant Structure of Multilevel Secure Access to the Resources of the Public Network // Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2016) = Distributed computer and communication networks: control, computation, communications (DCCN-2016): материалы Девятнадцатой междударной научной конференции, г. Москва, 21–25ноября 2016 г. – 2016, Vol. 3, pp. 264-271.

11. Коломойцев В.С. Задачи и средства обеспечения безопасности информационных систем в условиях цифровой экономики // Технико-технологические проблемы сервиса. – 2017. – № 4(42). – С. 50-55.

12. Kolomoitcev V.S., Bogatyrev V.A. Selecting multilevel structure secure access to resources external network // Распределенные компьютерные и телекоммуникационные сети: управление, вычисление (DCCN-2015) = Distributed computer and communication network: control, computation, communications (DCCN-2015): Материалы восемнадцатой международной научной конференции, г. Москва, 19-22 октября 2015 г. – 2015, pp. 525-532.

13. Kolomoitcev V.S., Parshutina S.A., Bogatyrev V.A. A Fault-Tolerant Two-Tier System of Secure Access to Areas Beyond the Control of the Computing Network // Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2017) = Distributed computer and communication networks: control, computation, communications

(DCCN-2017): материалы Двадцатой междударной научной конференции, г. Москва, 25–29сентября 2017 г. – 2017, pp. 189-196.

14. Коломойцев В.С. Схема безопасного доступа во внешнюю сеть // Наука и образование в жизни современного общества: сборник научных трудов по материалам Международной научно-практической конференции (30декабря 2014г.) – 2015. – Т. 9. – С. 81-82.

15. Коломойцев В.С. Безопасность подключения к общедоступной сети // Теоретические и практические аспекты технических наук: сборник статей Международной научно-практической конференции, г. Уфа, 29 декабря 2014 г. – 2014. – С. 40-41.

16. Коломойцев В.С. Варианты конфигураций схемы доступа «Прямое соединение» // Наука: прошлое, настоящее, будущее: сборник статей Международной научно-практической конференции, г. Уфа, 15 августа 2015 г., в 2 частях. – 2015. – Т. 1. – С. 44-46.

17. Коломойцев В.С. Интеграция организационных и аппаратно-программных мер по защите информации // Инновационное развитие: ключевые проблемы и решения: сборник статей Международной научно-практической конференции, г. Казань, 8 декабря 2015 г. – 2015. – Т. 2. – С. 32-34.

18. Коломойцев В.С. О необходимости комплексного подхода к обеспечению информационной защищенности вычислительных систем // Новая наука: Современное состояние и пути развития [заочная конференция]. – 2015. – № 6-2. – С. 162-164.

19. Коломойцев В.С. Структура контура защиты автоматизированных систем // Альманах научных работ молодых ученых Университета ИТМО. – 2015. – Т. 2. – С. 44-46.

20. Коломойцев В.С. Применение аппаратных межсетевых экранов для обеспечения информационной безопасности вычислительных систем // Информационные системы и технологии в моделировании и управлении: I Всероссийская научно-практическая конференция, г. Ялта, 23-24 мая 2016 г. – 2016. – С. 40.

21. Коломойцев В.С. Межсетевые экраны с фильтрацией и с адаптивной проверкой пакетов // Новая наука: Опыт, традиции, инновации [заочная конференции]. – 2016. – № 5-2(84). – С. 171-173.

22. Коломойцев В.С., Красильников А.В., Бодров К.Ю. Расчет вероятности обнаружения и устранения угроз безопасности информации в канале передачи данных // Международная конференция по мягким вычислениям и измерениям. – 2016. – Т. 1. – № Секции 1-3. – С. 86-88.

23. Коломойцев В.С. К вопросу оценки защищенности вычислительных систем // Новая наука: От идеи к результату [заочная конференция]. – 2016. – № 11-2. – С. 105-107.

24. Коломойцев В.С. Проектирование защищенных вычислительных систем в условиях ограничений на их конечную стоимость // Новые информационные технологии в науке: сборник статей международной научно-практической конференции, г. Уфа, 28 ноября 2016 г.). – 2016. – Т. Ч. 2. – С. 88-90.

25. Богатырев В.А., Коломойцев В.С. Выбор межсетевых экранов в распределенных системах информационного сервиса // Технологическая перспектива в рамках Евразийского пространства: новые рынки и точки экономического роста: 2-я Международная научная конференция, Санкт-Петербург, 20-22 октября 2016 г.: сборник трудов конференции. – 2016. – С. 318-321.

26. Коломойцев В.С. Применение межсетевого экрана для обеспечения информационной защищенности вычислительных систем // Единство и идентичность науки: проблемы и пути решения: сборник статей Международной научно-практической конференции, г. Казань, 3 июня 2017 г. – 2017. – Т. 3. – С. 86-88.

27. Коломойцев В.С. Необходимость проведения аудита и стресс-тестов систем обеспечения защиты информации вычислительных систем // Интеграционные процессы в науке в современных условиях: сборник статей Международной научно-практической конференции, г. Волгоград, 5 июня 2017 г. – 2017. – Т. 3. –С. 70-72.

28. Коломойцев В.С. Обоснование выбора кластерной системы защищенного доступа // Альманах научных работ молодых ученых Университета ИТМО. – 2016. – Т. 2. – С. 340-342.

29. Коломойцев В.С. Организация безопасного доступа во внешнюю сеть // Сборник тезисов участников форума «Наука будущего – наука молодых». – Севастополь, 2015. – Т. 1. – С. 277-278.

30. Коломойцев В.С. Эффективность систем защищенного доступа с разным числом средств защиты информации // Информационно-технологическое обеспечение цифровой экономики: сборник статей. – 2018. – С. 61-67.

31. Коломойцев В.С. Анализ возможностей типов межсетевых экранов // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: материалы конференции, СПОИСУ. – СПб., 2015. – С. 218-219.

32. Бутова Д.В., Толстоба Н.Д., Кожина А.Д., Коломойцев В.С., Кочнев К.А., Кривцова Р.С., Саитгалина А.К., Степаненко М.А., Торопова А.П., Шевченко Д.Н., Орехова М.К. Интерактивный оптический лабиринт. Разработка эскизного проекта // XIV Межвузовской конференции молодых ученых: сборник тезисов. – 2017. – С. 1.

33. Коломойцев В.С. О проблеме проектирования безопасных вычислительных систем // Региональная информатика (РИ-2016): материалы конференции, Санкт-Петербург, 26-28 октября 2016 г. – 2016.

34. Богатырев В.А., Коломойцев В.С. Безопасность объединенных автоматизированных систем // Региональная информатика (РИ-2014). XIV Санкт-Петербургская Р32 международная конференция. Санкт-Петербург, 29-31 октября 2014 г.: материалы конференции, СПОИСУ. – СПб., 2014. – С. 402-403.

35. Saitgalina A.K., Tolstoba N.D., Butova D.V., Orekhova M.K., Lyamets D.A., Kozhina A.D., Kolomoitcev V.S., Shevchenko D.N., Krivtcova R.S., Stepanenko M.A., Kochnev K.A.Design and implementation of a modular interactive labyrinth targeted for use in optical education Maksim A. Stepanenko, Kirill A. Kochnev, Alina S. Beliaeva, IET - 2016. ISSUE ETP17-ETP100-76, No. ETP100-76.

Подписано в печать 24.10.2018. Формат 60×84 1/16.
Печ. л. 1,0. Тираж 70 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1