НАЗВАНИЕ ПРОЕКТА Разработка математических моделей, методик и алгоритмов анализа защищенности, моделирования атак и выработки контрмер в режиме близком к реальному времени в системе защиты информационно-телекоммуникационной системы	НОМЕР ПРОЕКТА 15-07-07451
ОБЛАСТЬ ЗНАНИЯ (цифровой код) 07	КОД КЛАССИФИКАТОРА 07-298, 07-205, 08-608
КОД И НАЗВАНИЕ КОНКУРСА А- Конкурс инициативных научно-исследовательских проектов 2015 года	
ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА Чечулин Андрей Алексеевич	ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА +78123287181
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, предоставляющей условия для выполнения работ по Проекту физическим лицам: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук	

*Форма 503.***РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ**

3.1. Номер Проекта

15-07-07451

3.2. Название Проекта

Разработка математических моделей, методик и алгоритмов анализа защищенности, моделирования атак и выработки контрмер в режиме близком к реальному времени в системе защиты информационно-телекоммуникационной системы

3.3. Коды классификатора, соответствующие содержанию фактически проделанной работы

07-298, 07-205, 08-608

3.4. Объявленные ранее цели Проекта

Одной из фундаментальных научных проблем является разработка методологических основ обеспечения безопасности информации в информационно-телекоммуникационных системах. В настоящее время данные системы используются во всех областях от повседневной жизни, до управления критически важными инфраструктурами, и поэтому решение этой проблемы является одной из приоритетных задач, решаемых органами государственного, регионального и местного управления во всех развитых государствах мира. Целью данного фундаментального исследования является повышение уровня защищенности информационно-телекоммуникационных систем за счет разработки новых математических моделей, методик и алгоритмов анализа защищенности, моделирования атак и выработки контрмер в режиме близком к реальному времени. Предполагается, что данная цель будет достигнута путем достижения следующих задач: 1. Разработка математических моделей, методик и алгоритмов анализа защищенности, моделирования атак и выработки контрмер для защиты информации в информационно-телекоммуникационных системах на основе создания и применения средств аналитического моделирования и проактивного мониторинга. 2. Оптимизация процесса аналитического моделирования информационно-телекоммуникационной системы и ее системы защиты в условиях проведения атак в режиме близком к реальному времени. Таким образом, обобщенной задачей данного исследования является разработка новых математических моделей, методик и алгоритмов анализа защищенности, моделирования атак и выработки контрмер, которые могли бы использоваться в условиях больших объемов исходных данных и производить анализ системы защиты в условиях проводящихся атак в режиме близком к реальному времени, и, как следствие, рекомендовать оператору способы изменения политики безопасности системы защиты за ограниченное время. Таким образом, система, основанная на результатах данного исследования, должна учитывать события безопасности, происходящие в реальном времени и адаптировать политику безопасности информационно-телекоммуникационной системы таким образом, чтобы максимально снизить возможные последствия проводящейся атаки. С помощью реализации разрабатываемых моделей и методов, предполагается достичь значительного повышения уровня защищенности информационно-телекоммуникационных систем, обеспечить возможность манипулировать информацией о безопасности и осуществлять проактивное управление инцидентами и событиями безопасности. Система защиты информации, основанная на

предложенном подходе должна обладать способностью успешно решать следующие задачи: получение информации о текущем состоянии защищенности информационно-телекоммуникационной системы и ее компонентов; проведение обоснованного анализа и управление рисками безопасности защищаемой информационно-телекоммуникационной системы (в том числе своевременное устранение или снижение рисков безопасности); обнаружение несоответствия реального уровня защищенности важных ресурсов требуемому уровню, определяемому внутренними политиками безопасности, и приведение их в соответствие друг с другом; принятие эффективных решений по защите информации. Использование разрабатываемых математических моделей, методик и алгоритмов анализа защищенности, моделирования атак и выработки контрмер позволит повысить уровень информационной безопасности за счет постоянного отслеживания текущих показателей защищенности в режиме, близком к реальному времени. Кроме того, предлагаемый подход позволит производить предварительную оценку влияния предлагаемых оператором контрмер на защищенность информационно-телекоммуникационной системы что позволит повысить качество принимаемых решений.

3.5. Полученные в 2015 году важнейшие результаты

В ходе первого этапа проекта были выполнены все запланированные задачи, а именно:

1. Выполнен обзор и анализ существующих подходов к описанию информационно-телекоммуникационных систем и их элементов, существующие классификации нарушителей и угроз безопасности информационно-телекоммуникационных систем, а также анализ существующих моделей атак.

По результатам анализа существующих подходов к описанию информационно-телекоммуникационных систем и их элементов, были выбраны несколько стандартов корпорации MITRE, которые позволяют составить полную и непротиворечивую (хотя и не лишенную некоторых недостатков) модель защищаемой системы, уязвимостей и атак. Так, например, стандарт «Общее перечисление платформ» (Common Platform Enumeration, CPE) представляет собой унифицированный язык описания программно-аппаратного обеспечения. Данный стандарт содержит формализованное представление имени и мета-язык для описания комбинаций уязвимого программно-аппаратного обеспечения (например, для ситуации, когда уязвимое приложение может быть атаковано только в случае его запуска в определенной версии операционной системы). Также использование данного стандарта позволяет связать установленное программно-аппаратне обеспечение с уязвимостями и шаблонами атак.

Для представления отдельных уязвимостей и возможных подходов и методик, которые могут быть использованы нарушителями корпорацией MITRE были созданы стандарты «Общее перечисление уязвимостей» (Common Vulnerability Enumeration, CVE) и «Общее перечисление и классификация шаблонов атак» (Common Attack Pattern Enumeration and Classification, CAPEC). Данные стандарты содержат как общую таксономию, так и шаблоны отдельных компьютерных атак и уязвимостей. Данные базы постоянно обновляются. Однако, как показали проведенные исследования, использование других открытых баз данных

атак и уязвимостей позволяет повысить качество моделирования.
В современной литературе существует множество различных классификаций нарушителей. Так, некоторые выделяют следующие параметры: (1) физический тип доступа к объектам анализируемой компьютерной сети; (2) возможности нарушителя; (3) цели нарушителя.
С точки зрения возможностей физического доступа к объектам анализируемой компьютерной сети нарушители подразделяются на два типа: (1) нарушители, не имеющие возможностей доступа к объектам защищаемой сети – внешние нарушители; (2) нарушители, имеющие доступ к объектам защищаемой сети – внутренние нарушители. Цель нарушителя зависит от многих параметров и определяется индивидуально для каждого нарушителя. В зависимости от типа доступа, возможностей и целей нарушителя могут изменяться и наиболее эффективные средства противодействия.

2. Проведено исследование основных типов информационных систем и их особенностей с точки зрения защиты от атак.

В результате проведенного исследования были выделены следующие основные типы информационно-телекоммуникационных систем:
По назначению данные системы могут быть сгруппированы следующим образом: (1) системы телерадиовещания; (2) системы голосовой связи; (3) компьютерные сети. По типу среды передачи информации: (1) проводные; (2) беспроводные. По типу маршрутизации: (1) статическая; (2) динамическая (здесь иногда выделяют ячеистые сети, также называемые multi-hop сетями).
С точки зрения защиты, информационно-телекоммуникационных систем можно разделить по типу доступа: (1) доступные из сети Интернет; (2) доступные из локальной сети предприятия; (3) полностью независимые сети. По типу используемого программно-аппаратного обеспечения: (1) стандартное; (2) специализированное. По типу защитных средств: (1) встроенные в систему; (2) дополняющие систему; (3) отсутствующие.
Все вышеперечисленные типы определяют возможности нарушителей и необходимые средства защиты.

3. Разработана обобщенная модель информационно-телекоммуникационной системы, включающей в себя описания хостов и связей между ними.

Для представления элементов информационно-телекоммуникационной системы разработана обобщенная модель, включающей в себя описания хостов, связей между ними и параметров безопасности. Модель хоста определяет: (1) установленное программно-аппаратное обеспечение (позволяет определить возможности нарушителя выполнять атаки на этот хост); (2) ценность информации, хранящейся на данном хосте (позволяет определить возможный ущерб от успешной атаки на этот хост). В данном исследовании программно-аппаратное обеспечение задается с помощью стандарта Common Platform Enumeration (CPE), что позволяет использовать информацию от существующих средств анализа компьютерных сетей, а также определить присущие этому хосту уязвимости.
Модель связей информационно-телекоммуникационной системы задают

типы отношения между её элементами. Так, например, сетевой доступ позволяет выполнять атаки на связанный хост, а отношения функциональной зависимости позволяют нанести информационно-телекоммуникационной системе дополнительный ущерб (например, вывод из строя сервера домена нарушает работу всей информационно-телекоммуникационной системе, а не только одному, хотя и значимому хосту). Данные определяемые моделью связей представляют собой описание возможных путей, по которым нарушитель сможет выполнять атакующие действия или распространять ущерб от атак.
Модели параметров безопасности связей и хостов представляют собой множество правил политики безопасности, каждый из которых задает ограничение на уязвимость или на метод сбора информации. Моделирование параметров безопасности позволяет имитировать работу таких систем безопасности как межсетевые экраны (которые могут заблокировать определенные виды сетевого сканирования или пакеты, характерные для некоторых видов атак) и антивирусы (которые могут заблокировать эксплуатацию ряда уязвимостей).

4. Разработана модель нарушителя безопасности информационно-телекоммуникационных систем, учитывающей знания нарушителя, права доступа к защищаемой информационно-телекоммуникационной системе (для учета возможности того, что нарушитель является внутренним пользователем) и цели, по которым можно определить наиболее вероятные пути развития атак.

Модель нарушителя, предложенная в настоящем исследовании, содержит: (1) информацию о начальных условиях; (2) сведения о квалификации и (3) целях нарушителя. Начальные условия задаются как список элементов информационно-телекоммуникационной системы, с которых нарушитель может начать выполнение атакующих действий (в случае, когда нарушитель начинает свои действия не с хоста, которым он владеет, первые атаки направлены на этот же хост) и как список прав нарушителя в сети (для моделирования возможности того, что нарушитель является внутренним пользователем). Квалификация нарушителя определяется: (1) уровенем знаний нарушителя; (2) списком известных уязвимостей, которые нарушитель может эксплуатировать (для моделирования, например, автоматических средств взлома); (3) списком известных нарушителю уязвимостей нулевого дня.
Для определения целей нарушителя в предлагаемую модель вводится список действий, к выполнению которых будет стремиться нарушитель (например, это может быть компрометация определенного хоста, кража конфиденциальной информации из базы данных и т.д). Цель (цели) определяют, в какой момент нарушитель завершит свои атакующие действия. Также, данный параметр позволит в дальнейшем определять вероятностные характеристики при выборе потенциальных путей развития дерева атак для конкретного нарушителя.

5. Разработана модель атак, позволяющая описать эксплуатацию как известных, так и неизвестных уязвимостей, а так же сценарии атак, состоящие из последовательного выполнения разнородных атакующих действий.

В качестве модели атак в настоящем исследовании было предложено использовать представление, основанное на графах атак. Подобные графы, являющиеся результатом моделирования атак, позволяют описать пути проникновения в систему, в виде набора различных атак. Для конкретного нарушителя граф атак состоит из корня, являющегося атакующими действиями, которые нарушитель может выполнить на своей начальной позиции , и листьев, представляющих собой атакующие действия, приводящие достижению целей нарушителя. Последовательность узлов графа представляет возмодные последовательности атакующих действий, ведущие нарушителя к его цели. Все пути от корня до листьев являются маршрутами атак приводящими к реализации одной из целей нарушителя. Для формирования графа атак необходимы следующие исходные данные: (1) заполненная модель защищаемой информационно-телекоммуникационной системы; (2) данные о существующих узявимостях; (3) модель нарушителя.

Для формирования исходных данных для моделирования атак, эксплуатирующих известные уязвимости, в настоящем исследовании предлагается использовать открытые базы данных уязвимостей (например, Common Vulnerabilities and Exposures (CVE)) и атак (например, Common Attack Pattern Enumeration and Classification (CAPEC)). Данные базы содержат списки уязвимостей, которые могут быть использованы при моделировании, так как их описания в этих базах содержит как предусловия, так и оценки, характеризующие результат реализации атак, эксплуатирующих эти уязвимости. Кроме того, описания уязвимостей содержат списки конкретных программно-аппаратных продуктов, содержащих данные уязвимости. Для проведения экспериментов было принято решение сформировать обобщенную модель уязвимости для объединения уязвимостей из разных источников. Предполагается, что объединение открытых баз данных уязвимостей приведёт к: (1) интеграции самих записей уязвимостей, что обеспечит более систематизированный доступ к информации об уязвимостях; (2) расширению списка продуктов, в которых уязвимости могут иметь успешную реализацию, что позволит повысить вероятность обнаружения уязвимых программно-аппаратных средств, используемых в анализируемых системах, и, как следствие, улучшит точность оценки защищенности этих систем. Кроме того, использование структуры базы данных, адаптированной для поиска записей уязвимостей посредством удаленного сервиса, позволит применять эту базу в системах оценки защищённости, проводящих анализ безопасности в режиме, близком к реальному времени.

6. Выполнен обзор и анализ существующих методик визуализации данных, касающихся защищенности информационно-телекоммуникационных систем.

В условиях постоянного увеличения объёма и размерности визуализируемых данных, весьма актуальна проблема формирования концептуально новых моделей визуализации. Для разработки новых методик визуализации, необходимо знать общие особенности процесса их построения, а также уметь ориентироваться в уже существующих методиках, в том числе тех, которые используются вне сферы

информационной безопасности, в которой авторы проводят интенсивные исследования и разрабатывают подсистему визуализации. Работы, рассматривающие методики визуализации данных, как правило, уделяют недостаточно внимания целостности данного процесса, а именно, не рассматривают требуемые для визуализации аспекты, не упоминают при помощи каких инструментов и библиотек реализуется графическая модель или какие концептуальные инструменты могут расширить возможности той или иной графической модели, а также не рассматривают новые и уникальные графические модели.
При построении или выборе модели отображения данных важно понимать, как различные этапы и элементы процесса визуализации влияют на модель. В процессе анализа существующих методик визуализации данных, касающихся защищенности информационно-телекоммуникационных систем, были рассмотрены основные методологические примитивы на примере поэтапного построения модели визуализации с уже подготовленными данными, с целью сформировать комплексное видение процесса создания модели и влияющих на неё аспектов. Была сформирована классификация визуализационных примитивов:
- примитивы процесса визуализации аспекты, которые влияют на процесс построения модели визуализации и с использованием которых разрабатывается начальная метамодель;
- примитивы графических моделей основные принципы построения модели визуализации; часто, именно выбор графической концепции определяет формат взаимодействия данных с пользователем, а также определяет ограничения и возможности расширения этого взаимодействия;
- дополнительные инструменты компоненты инструментов, расширяющие возможности графических моделей.
Также были рассмотрены библиотеки визуализации на популярных языках программирования, реализующие разные модели визуализации.

7. Реализована программная библиотека, реализующая отдельные модели и алгоритмы автоматизированного заполнения разработанных моделей на основе экспертных знаний и результатов анализа защищаемых информационных систем.

В качестве практической реализации была разработана программная библиотека, который обеспечивает, в том числе формирование исходных данных для моделирования. Одним из результатов работы этой библиотеки является интегрированная база данных уязвимостей, которая содержит данные из следующих источников описания уязвимостей и продуктов: (1) база CVE; (2) база NVD; (3) база OSVDB; (4) база X-Force; (5) словарь CPE. В результате формирования интегрированной базы общее число уникальных записей уязвимостей составило примерно 90 тысяч (для сравнения, число загруженных записей уязвимостей из базы CVE составило ~67 тыс., из базы OSVDB ~100 тыс., а из базы X-Force ~65,5 тыс.). В свою очередь, общей размер интегрированного словаря продуктов составил 192 тыс. оригинальных записей (из них 99,5 тыс. из словаря CPE). Данные показатели обосновывают преимущество данной базы перед используемыми источниками описания уязвимостей и продуктов, а также теоретическое повышение точности при

использовании разработанной программной библиотеки в средствах оценки защищенности информационно-телекоммуникаций систем.

При сравнении сформированной базы уязвимостей с аналогами, а именно, с online-сервисом "CVE Details", были выявлены следующие преимущества разработанной базы: (1) превосходство по количеству обрабатываемых производителей, продуктов и их версий; (2) наличие соответствия записей уязвимостей базы CVE с базами OSVDB и X-Force, а также между собой; (3) предоставление возможности как автоматизированного, так и ручного (для администраторов безопасности посредством web-интерфейса) доступа к возможностям поиска уязвимостей в интегрированной базе.

Дополнительным качеством разработанной библиотеки является наличие возможности автоматизированного обновления, как из сети Интернет, так и с локальных ресурсов (жесткий диск, FTP ресурсы), что позволяет поддерживать актуальность информации об уязвимостях на должном уровне для обеспечения высокой точности оценки защищенности исследуемых инфраструктур.

3.6. Сопоставление полученных результатов с мировым уровнем

Научные и практически результаты, полученные в рамках проведенного в 2015 году исследования, соответствуют мировому уровню. Это подтверждается успешной апробацией на ряде российских и иностранных конференциях и публикациями в российских и иностранных рецензируемых журналах. Авторы проекта изложили основные результаты в 3 статьях, опубликованных в изданиях, индексируемых в международных базах цитирования (журналы «Automatic Control and Computer Sciences» и «Journal of Internet Services and Information Security» и «Lecture Notes in Computer Science (LNCS), Vol.9357») и в 5 статьях, опубликованных в журналах, входящих в список ВАК Минобрнауки России (журналы «Информационно-управляющие системы», «Проблемы информационной безопасности. Компьютерные системы», «Безопасность информационных технологий», «Труды СПИИРАН»), а также в прочих журналах и трудах конференций.

Кроме публикаций в журналах, результаты также были апробированы на множестве различных российских и международных конференций, в частности, на Семнадцатой Международной конференции “РусКрипто’2015”, Московская область, г. Солнечногорск, март 2015 года; 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, июнь-июль 2015 года;

Международном конгрессе по интеллектуальным системам и информационным технологиям (IS-IT'15), Дивноморское, Россия, сентябрь 2015 года; LI Международной научно-практической конференции "Технические науки - от теории к практике", Новосибирск, октябрь 2015 года; IX Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России" (ИБРР-2015), Санкт-Петербург, октябрь 2015 года; LII Международной научно-практической конференции "Технические науки - от теории к практике", Новосибирск, ноябрь 2015 года.

3.7.1. Методы и подходы, использованные в ходе выполнения Проекта

Для достижения поставленных в 2015 году целей использовались следующие методы и подходы:

(1) методы интеллектуального анализа данных для подготовки исходных данных для моделирования защищаемой информационно-телекоммуникационной системы и атак на нее;

(2) методы визуального анализа информации, позволяющие повысить скорость выбора контрмер за счет учета когнитивных особенностей оператора системы защиты;

(3) методы аналитического моделирования для прогнозирования атак и подготовки исходных данных для оценки защищенности и анализа рисков;

(4) методы оценки защищенности и анализа рисков;

(5) методы объединения аналитических моделей, описывающих различных аспекты информационно-телекоммуникационных систем;

(6) онтологический подход к моделированию предметной области в части создания и применения онтологии, охватывающей метрики защищенности, структурные элементы информационно-телекоммуникационных систем и контрмеры по обеспечению требуемого уровня защищенности;

(7) методы системного анализа и теории систем, в части их применения для разработки обобщенной модели защищаемой информационно-телекоммуникационной системы и атак на нее.

3.7.2. Вклад каждого члена коллектива в выполнение Проекта в 2015 году

Десницкий Василий Алексеевич:

- разработка моделей встроенных устройств
- разработка моделей нарушителей для систем, содержащих встроенные устройства
- выявление факторов, определяющих специфику моделирования в информационно-телекоммуникационных сетях, содержащих встроенные устройства;
- анализ существующих классификаций нарушителей и угроз безопасности в информационно-телекоммуникационных сетях, содержащих встроенные устройства;

Дойникова Елена Владимировна:

- исследование основных типов информационных систем;
- исследование систем защиты, применяемых в информационно-телекоммуникационных сетях.
- реализация программной библиотеки, реализующей отдельные модели и алгоритмы автоматизированного заполнения разработанных моделей на основе экспертных знаний и результатов анализа защищаемых информационных систем.

Полубелова Ольга Витальевна:

- анализ существующих подходов к моделированию информационно-телекоммуникационных системы, включающих в себя описания хостов и связей между ними;
- реализация программной библиотеки, реализующей отдельные модели и алгоритмы автоматизированного заполнения разработанных моделей на основе экспертных знаний и результатов анализа защищаемых информационных систем.

Саенко Игорь Борисович:
- обзор и анализ существующих подходов к описанию информационно-телекоммуникационных систем и их элементов, существующие классификации нарушителей и угроз безопасности информационно-телекоммуникационных систем, а также анализ существующих моделей атак
- разработка общей структуры моделей элементов информационно-телекоммуникационых систем;
- разработка общей структуры моделей атак на информационно-телекоммуникационые системы;

Федорченко Андрей Владимирович:
- анализ возможных источников данных для заполнения моделей атак, использующих как известные, так и неизвестные уязвимости;
- анализ возможных источников данных для построения сценариев атак, состоящих из последовательного выполнения разнородных атакующих действий;
- разработка моделей распределенных атак отказа в обслуживании (DDoS);
- реализация программной библиотеки, реализующей отдельные модели и алгоритмы автоматизированного заполнения разработанных моделей на основе экспертных знаний и результатов анализа защищаемых информационных систем.

Чечулин Андрей Алексеевич:
- обзор и анализ существующих подходов к описанию информационно-телекоммуникационных систем и их элементов, существующие классификации нарушителей и угроз безопасности информационно-телекоммуникационных систем, а также анализ существующих моделей атак
- анализ существующих методов визуализации данных, касающихся защищенности информационно-телекоммуникационных систем;
- разработка методов динамического моделирования информационно-телекоммуникационых систем;
- разработка общей модели нарушителя безопасности информационно-телекоммуникационных систем, учитывающей знания и цели нарушителя, а также права доступа к защищаемой информационно-телекоммуникационной системе;
- реализация программной библиотеки, реализующей отдельные модели и алгоритмы автоматизированного заполнения разработанных моделей на основе экспертных знаний и результатов анализа защищаемых информационных систем.

Шоров Андрей Владимирович:
- разработка методов динамического моделирования информационно-телекоммуникационых систем;
- разработка моделей распределенных атак отказа в обслуживании (DDoS).

3.8.1. Количество научных работ по Проекту, опубликованных в 2015 году

32

3.8.1.1. Из них в изданиях, включенных в перечень ВАК

5

3.8.1.2. Из них в изданиях, включенных в библиографическую базу данных РИНЦ

6

3.8.1.3. Из них в изданиях, включенных в международные системы цитирования (библиографические и реферативные базы научных публикаций)

3

3.8.2. Количество научных работ, подготовленных в ходе выполнения Проекта и принятых к печати в 2015 году

3

3.9. Участие в 2015 году в научных мероприятиях по тематике Проекта

1. Семнадцатая Международная конференция “РусКрипто’2015”, Московская область, г. Солнечногорск, март 2015 года (секционные доклады).
2. 24-й научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, июнь-июль 2015 года (секционные доклады).
3. Международный конгресс по интеллектуальным системам и информационным технологиям (IS-IT'15), Дивноморское, Россия, сентябрь 2015 года (1 пленарный, 2 секционных доклада).
4. LI Международная научно-практическая конференция "Технические науки - от теории к практике", Новосибирск, октябрь 2015 года;
5. IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015), октябрь 2015 года (секционные доклады).
6. LII Международная научно-практическая конференция "Технические науки - от теории к практике", Новосибирск, ноябрь 2015 года.

3.10. Участие в 2015 году в экспедициях по тематике Проекта, которые проводились при финансовой поддержке Фонда

не было

3.11. Финансовые средства, полученные в 2015 году от Фонда *(в руб.)*

700000,00

3.12. Адреса *(полностью)* ресурсов в Интернете, подготовленных авторами по данному проекту

http://www.comsec.spb.ru/chechulin/ ,
http://www.comsec.spb.ru/ru/staff/chechulin,
http://www.comsec.spb.ru/en/papers,
http://www.comsec.spb.ru/ru/papers/

3.13. Библиографический список всех публикаций по Проекту, опубликованных в 2015 году, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.

1. Chechulin A.A., Kotenko I.V. Real-Time Security Events Processing using an Approach based on the Attack Trees Analysis // Automatic Control and Computer Sciences, № 8, 2015, Springer, 2015. Принято к публикации.
2. Maxim Kolomeec, Andrey Chechulin and Igor Kotenko. Methodological Primitives for Phased Construction of Data Visualization Models. Journal of Internet Services and Information Security (JISIS), Vol.5, No.4, November,

2015. P.60-84. http://www.jisis.org/vol5no4.php
3. Yana Bekeneva, Konstantin Borisenko, Andrey Shorov, Igor Kotenko. Investigation of DDoS Attacks by Hybrid Simulation // The 2015 Asian Conference on Availability, Reliability and Security (AsiaARES 2015). In conjunction with ICT-EurAsia 2015. October 4th – 7th, 2015, Daejeon, Korea / ICT-EurAsia 2015, Lecture Notes in Computer Science (LNCS), Vol.9357. IFIP International Federation for Information Processing (2015). Springer. 2015, P.179-189.
4. Дойникова Е.В., Котенко И.В., Чечулин А.А. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах // Безопасность информационных технологий, № 3, 2015. Принято к публикации.
5. Котенко И.В., Дойникова Е.В. Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности // Информационно-управляющие системы, 2015, № 3, С.60-69. doi:10.15217/issn1684-8853.2015.3.60.
6. Коломеец М.В., Чечулин А.А., Котенко И.В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Вып. 42. С. 232-257.
7. Котенко И.В., Новикова Е.С., Чечулин А.А. Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С.42-47.
8. Котенко И.В., Шоров А.В. Исследование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети» // Проблемы информационной безопасности. Компьютерные системы, № 3, 2015. С.45-55.
9. Десницкий В.А. Конфигурирование компонентов защиты встроенных устройств на основе эвристического подхода // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №46, 2015, С.16-20.
10. Проноза А.А., Чечулин А.А. Модель извлечения данных разнородной структуры об информационных объектах компьютерной сети для подсистемы визуализации систем управления событиями и информацией безопасности // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.125-127.
11. Дойникова Е.В. Генератор сценариев атак на основе классификации шаблонов атак CAPEC // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.71-72.
12. Дойникова Е.В., Котенко И.В. Выбор защитных мер для управления защищенностью компьютерных сетей на основе комплексной системы показателей // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.114-115.
13. Котенко И.В., Саенко И.Б., Чечулин А.А. Разработка систем управления информацией и событиями безопасности нового поколения // Материалы 24-й научно-технической конференции «Методы и

технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.123-124.
14. Федорченко А.В Комбинированный процесс корреляции событий безопасности в SIEM-системах // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.102-103.
15. Дойникова Е.В. Применение графов зависимостей сервисов в рамках задачи анализа защищенности компьютерных сетей для оценивания критичности ресурсов системы и обоснованного выбора защитных мер // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 68-69.
16. Коломеец М.В., Чечулин А.А., Котенко И.В. Визуализация параметров безопасности компьютерных сетей с помощью диаграммы Вороного // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 73-74.
17. Федорченко А.В. Правило-ориентированный метод корреляции событий безопасности в SIEM-системах // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 86-87.
18. Чечулин А.А. Математические модели и алгоритмы моделирования атак и выработки контрмер в режиме, близком к реальному времени // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 90.
19. Саенко И.Б., Котенко И.В. Модели и методы оценки эффективности функционирования системы разграничения доступа к ресурсам информационного пространства // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 85-86.
20. Чечулин А.А. Классификация и модели представления связей между объектами в компьютерных сетях // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С. 165-170.
21. Смирнов Д.Б., Чечулин А.А. Корреляция данных безопасности в сетях «Интернет вещей» // Семнадцатая Международная конференция “РусКрипто’2015”. Московская область, г.Солнечногорск, 17-20 марта 2015 г. http://www.ruscrypto.ru/
22. Дойникова Е.В., Чечулин А.А. Генератор случайных последовательностей атакующих действий для тестирования сетей Интернета вещей. Свидетельство № 2015615368. Зарегистрировано в Реестре программ для ЭВМ 15.05.2015.
23. Котенко И.В., Чечулин А.А. Компонент визуализации графов атак системы оценки защищенности компьютерных сетей. Свидетельство № 2015615640. Зарегистрировано в Реестре программ для ЭВМ 22.05.2015.
24. Котенко И.В., Чечулин А.А. Компонент визуализации топологии компьютерной сети для мониторинга и управления безопасностью

информационно-телекоммуникационных систем. Свидетельство № 2015615773. Зарегистрировано в Реестре программ для ЭВМ 22.05.2015.
25. Федорченко А.В., Чечулин А.А., Котенко И.В. Компонент анализа статистики и оценки качественных параметров интегрированной базы уязвимостей. Свидетельство № 2015662208. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
26. Федорченко А.В., Чечулин А.А. Интегрированная база уязвимостей для систем мониторинга и управления безопасностью информационно-телекоммуникационных систем. Свидетельство № 2015621655. Зарегистрировано в Реестре баз данных 17.11.2015.
27. Саенко И.Б., Чечулин А.А., Агеев С.А., Котенко И.В. Классификатор состояния элементов компьютерной сети при оценке рисков угроз информационной безопасности. Свидетельство № 2015662186. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
28. Чечулин А.А., Котенко И.В. Компонент моделирования атак для защиты информационно-телекоммуникационных систем. Свидетельство № 2015619128. Зарегистрировано в Реестре программ для ЭВМ 25.11.2015.
29. Дойникова Е.В., Котенко И.В. Компонент оценивания критичности ресурсов на основе построения модели зависимостей сервисов при тестировании компонентов защиты в сетях Интернета вещей. Свидетельство № 2015615374. Зарегистрировано в Реестре программ для ЭВМ 24.03.2015.
30. Саенко И.Б., Браницкий А.А. Программно-инструментальный стенд визуализации и оценки качества проектирования виртуальных компьютерных сетей для поддержки принятия решений при мониторинге и управлении информационной безопасностью. Свидетельство № 2015615772. Зарегистрировано в Реестре программ для ЭВМ 22.05.2015.
31. Федорченко А.В., Котенко И.В. Сервисы доступа и управления интегрированной базой уязвимостей для систем мониторинга и управления безопасностью информационно-телекоммуникационных систем. Свидетельство № 2015615366. Зарегистрировано в Реестре программ для ЭВМ 15.05.2015.
32. Чечулин А.А., Дойникова Е.В. Компонент анализа моделей атак для защиты информационно-телекоммуникационных систем. Свидетельство № 2015619151. Зарегистрировано в Реестре программ для ЭВМ 16.11.2015.

3.14. Приоритетное направление развития науки, технологий и техники РФ, которому, по мнению исполнителей, соответствуют результаты данного проекта

Информационно-телекоммуникационные системы

3.15. Критическая технология РФ, которой, по мнению исполнителей, соответствуют результаты данного проекта Технологии информационных, управляющих, нвигационных систем

3.16. Основное направление технологической модернизации экономики России, которому, по мнению исполнителей, соответствуют результаты данного проекта

Стратегические информационные технологии, включая вопросы создания суперкомпьютеров и разработки программного обеспечения.

Основные результаты проекта

В ходе первого этапа проекта были выполнены все запланированные задачи, а именно:

1. Выполнен обзор и анализ существующих подходов к описанию информационно-телекоммуникационных систем и их элементов, существующие классификации нарушителей и угроз безопасности информационно-телекоммуникационных систем, а также анализ существующих моделей атак.

По результатам анализа существующих подходов к описанию информационно-телекоммуникационных систем и их элементов, были выбраны несколько стандартов корпорации MITRE, которые позволяют составить полную и непротиворечивую (хотя и не лишенную некоторых недостатков) модель защищаемой системы, уязвимостей и атак. Так, например, стандарт «Общее перечисление платформ» (Common Platform Enumeration, CPE) представляет собой унифицированный язык описания программно-аппаратного обеспечения. Данный стандарт содержит формализованное представление имени и мета-язык для описания комбинаций уязвимого программно-аппаратного обеспечения (например, для ситуации, когда уязвимое приложение может быть атаковано только в случае его запуска в определенной версии операционной системы). Также использование данного стандарта позволяет связать установленное программно-аппаратне обеспечение с уязвимостями и шаблонами атак.

Для представления отдельных уязвимостей и возможных подходов и методик, которые могут быть использованы нарушителями корпорацией MITRE были созданы стандарты «Общее перечисление уязвимостей» (Common Vulnerability Enumeration, CVE) и «Общее перечисление и классификация шаблонов атак» (Common Attack Pattern Enumeration and Classification, CAPEC). Данные стандарты содержат как общую таксономию, так и шаблоны отдельных компьютерных атак и уязвимостей. Данные базы постоянно обновляются. Однако, как показали проведенные исследования, использование других открытых баз данных атак и уязвимостей позволяет повысить качество моделирования.

В современной литературе существует множество различных классификаций нарушителей. Так, некоторые выделяют следующие параметры: (1) физический тип доступа к объектам анализируемой компьютерной сети; (2) возможности нарушителя; (3) цели нарушителя.

С точки зрения возможностей физического доступа к объектам анализируемой компьютерной сети нарушители подразделяются на два типа: (1) нарушители, не имеющие возможностей доступа к объектам защищаемой сети – внешние нарушители; (2) нарушители, имеющие доступ к объектам защищаемой сети – внутренние нарушители. Цель нарушителя зависит от многих параметров и определяется индивидуально для каждого нарушителя. В зависимости от типа доступа, возможностей и целей нарушителя могут изменяться и наиболее эффективные средства противодействия.

2. Проведено исследование основных типов информационных систем и их особенностей с точки зрения защиты от атак.

В результате проведенного исследования были выделены следующие основные типы информационно-телекоммуникационных систем:

По назначению данные системы могут быть сгруппированы следующим образом: (1) системы телерадиовещания; (2) системы голосовой связи; (3) компьютерные сети. По типу среды передачи информации: (1) проводные; (2) беспроводные. По типу маршрутизации: (1) статическая; (2) динамическая (здесь иногда выделяют ячеистые сети, также называемые multi-hop сетями).

С точки зрения защиты, информационно-телекоммуникационных систем можно разделить по типу доступа: (1) доступные из сети Интернет; (2) доступные из локальной сети предприятия; (3) полностью независимые сети. По типу используемого программно-аппаратного обеспечения: (1) стандартное; (2) специализированное. По типу защитных средств: (1) встроенные в систему; (2) дополняющие систему; (3) отсутствующие.
Все вышеперечисленные типы определяют возможности нарушителей и необходимые средства защиты.

3. Разработана обобщенная модель информационно-телекоммуникационной системы, включающей в себя описания хостов и связей между ними.

Для представления элементов информационно-телекоммуникационной системы разработана обобщенная модель, включающей в себя описания хостов, связей между ними и параметров безопасности. Модель хоста определяет: (1) установленное программно-аппаратное обеспечение (позволяет определить возможности нарушителя выполнять атаки на этот хост); (2) ценность информации, хранящейся на данном хосте (позволяет определить возможный ущерб от успешной атаки на этот хост). В данном исследовании программно-аппаратное обеспечение задается с помощью стандарта Common Platform Enumeration (CPE), что позволяет использовать информацию от существующих средств анализа компьютерных сетей, а также определить присущие этому хосту уязвимости.
Модель связей информационно-телекоммуникационной системы задают типы отношения между её элементами. Так, например, сетевой доступ позволяет выполнять атаки на связанный хост, а отношения функциональной зависимости позволяют нанести информационно-телекоммуникационной системе дополнительный ущерб (например, вывод из строя сервера домена нарушает работу всей информационно-телекоммуникационной системе, а не только одному, хотя и значимому хосту). Данные определяемые моделью связей представляют собой описание возможных путей, по которым нарушитель сможет выполнять атакующие действия или распространять ущерб от атак.
Модели параметров безопасности связей и хостов представляют собой множество правил политики безопасности, каждый из которых задает ограничение на уязвимость или на метод сбора информации. Моделирование параметров безопасности позволяет имитировать работу таких систем безопасности как межсетевые экраны (которые могут заблокировать определенные виды сетевого сканирования или пакеты, характерные для некоторых видов атак) и антивирусы (которые могут заблокировать эксплуатацию ряда уязвимостей).

4. Разработана модель нарушителя безопасности информационно-телекоммуникационных систем, учитывающей знания нарушителя, права доступа к защищаемой информационно-телекоммуникационной системе (для учета возможности того, что нарушитель является внутренним пользователем) и цели, по которым можно определить наиболее вероятные пути развития атак.

Модель нарушителя, предложенная в настоящем исследовании, содержит: (1) информацию о начальных условиях; (2) сведения о квалификации и (3) целях нарушителя. Начальные условия задаются как список элементов информационно-телекоммуникационной системы, с которых нарушитель может начать выполнение атакующих действий (в случае, когда нарушитель начинает свои действия не с хоста, которым он владеет, первые атаки направлены на этот же хост) и как список прав нарушителя в сети (для моделирования возможности того, что нарушитель является внутренним пользователем). Квалификация нарушителя определяется: (1) уровенем знаний нарушителя; (2) списком известных уязвимостей, которые нарушитель может

эксплуатировать (для моделирования, например, автоматических средств взлома); (3) списком известных нарушителю уязвимостей нулевого дня.
Для определения целей нарушителя в предлагаемую модель вводится список действий, к выполнению которых будет стремиться нарушитель (например, это может быть компрометация определенного хоста, кража конфиденциальной информации из базы данных и т.д). Цель (цели) определяют, в какой момент нарушитель завершит свои атакующие действия. Также, данный параметр позволит в дальнейшем определять вероятностные характеристики при выборе потенциальных путей развития дерева атак для конкретного нарушителя.

5. Разработана модель атак, позволяющая описать эксплуатацию как известных, так и неизвестных уязвимостей, а так же сценарии атак, состоящие из последовательного выполнения разнородных атакующих действий.

В качестве модели атак в настоящем исследовании было предложено использовать представление, основанное на графах атак. Подобные графы, являющиеся результатом моделирования атак, позволяют описать пути проникновения в систему, в виде набора различных атак. Для конкретного нарушителя граф атак состоит из корня, являющегося атакующими действиями, которые нарушитель может выполнить на своей начальной позиции , и листьев, представляющих собой атакующие действия, приводящие достижению целей нарушителя. Последовательность узлов графа представляет возмодные последовательности атакующих действий, ведущие нарушителя к его цели. Все пути от корня до листьев являются маршрутами атак приводящими к реализации одной из целей нарушителя. Для формирования графа атак необходимы следующие исходные данные: (1) заполненная модель защищаемой информационно-телекоммуникационной системы; (2) данные о существующих узявимостях; (3) модель нарушителя.
Для формирования исходных данных для моделирования атак, эксплуатирующих известные уязвимости, в настоящем исследовании предлагается использовать открытые базы данных уязвимостей (например, Common Vulnerabilities and Exposures (CVE)) и атак (например, Common Attack Pattern Enumeration and Classification (CAPEC)). Данные базы содержат списки уязвимостей, которые могут быть использованы при моделировании, так как их описания в этих базах содержит как предусловия, так и оценки, характеризующие результат реализации атак, эксплуатирующих эти уязвимости. Кроме того, описания уязвимостей содержат списки конкретных программно-аппаратных продуктов, содержащих данные уязвимости. Для проведения экспериментов было принято решение сформировать обобщенную модель уязвимости для объединения уязвимостей из разных источников. Предполагается, что объединение открытых баз данных уязвимостей приведёт к: (1) интеграции самих записей уязвимостей, что обеспечит более систематизированный доступ к информации об уязвимостях; (2) расширению списка продуктов, в которых уязвимости могут иметь успешную реализацию, что позволит повысить вероятность обнаружения уязвимых программно-аппаратных средств, используемых в анализируемых системах, и, как следствие, улучшит точность оценки защищенности этих систем. Кроме того, использование структуры базы данных, адаптированной для поиска записей уязвимостей посредством удаленного сервиса, позволит применять эту базу в системах оценки защищённости, проводящих анализ безопасности в режиме, близком к реальному времени.

6. Выполнен обзор и анализ существующих методик визуализации данных, касающихся защищенности информационно-телекоммуникационных систем.

В условиях постоянного увеличения объёма и размерности визуализируемых данных, весьма актуальна проблема формирования концептуально новых моделей визуализации.

Для разработки новых методик визуализации, необходимо знать общие особенности процесса их построения, а также уметь ориентироваться в уже существующих методиках, в том числе тех, которые используются вне сферы информационной безопасности, в которой авторы проводят интенсивные исследования и разрабатывают подсистему визуализации. Работы, рассматривающие методики визуализации данных, как правило, уделяют недостаточно внимания целостности данного процесса, а именно, не рассматривают требуемые для визуализации аспекты, не упоминают при помощи каких инструментов и библиотек реализуется графическая модель или какие концептуальные инструменты могут расширить возможности той или иной графической модели, а также не рассматривают новые и уникальные графические модели.
При построении или выборе модели отображения данных важно понимать, как различные этапы и элементы процесса визуализации влияют на модель. В процессе анализа существующих методик визуализации данных, касающихся защищенности информационно-телекоммуникационных систем, были рассмотрены основные методологические примитивы на примере поэтапного построения модели визуализации с уже подготовленными данными, с целью сформировать комплексное видение процесса создания модели и влияющих на неё аспектов. Была сформирована классификация визуализационных примитивов:
- примитивы процесса визуализации аспекты, которые влияют на процесс построения модели визуализации и с использованием которых разрабатывается начальная метамодель;
- примитивы графических моделей основные принципы построения модели визуализации; часто, именно выбор графической концепции определяет формат взаимодействия данных с пользователем, а также определяет ограничения и возможности расширения этого взаимодействия;
- дополнительные инструменты компоненты инструментов, расширяющие возможности графических моделей.
Также были рассмотрены библиотеки визуализации на популярных языках программирования, реализующие разные модели визуализации.

7. Реализована программная библиотека, реализующая отдельные модели и алгоритмы автоматизированного заполнения разработанных моделей на основе экспертных знаний и результатов анализа защищаемых информационных систем.

В качестве практической реализации была разработана программная библиотека, который обеспечивает, в том числе формирование исходных данных для моделирования. Одним из результатов работы этой библиотеки является интегрированная база данных уязвимостей, которая содержит данные из следующих источников описания уязвимостей и продуктов: (1) база CVE; (2) база NVD; (3) база OSVDB; (4) база X-Force; (5) словарь CPE. В результате формирования интегрированной базы общее число уникальных записей уязвимостей составило примерно 90 тысяч (для сравнения, число загруженных записей уязвимостей из базы CVE составило ~67 тыс., из базы OSVDB ~100 тыс., а из базы X-Force ~65,5 тыс.). В свою очередь, общей размер интегрированного словаря продуктов составил 192 тыс. оригинальных записей (из них 99,5 тыс. из словаря CPE). Данные показатели обосновывают преимущество данной базы перед используемыми источниками описания уязвимостей и продуктов, а также теоретическое повышение точности при использовании разработанной программной библиотеки в средствах оценки защищенности информационно-телекоммуникаций систем.
При сравнении сформированной базы уязвимостей с аналогами, а именно, с online-сервисом "CVE Details", были выявлены следующие преимущества разработанной базы: (1) превосходство по количеству обрабатываемых производителей, продуктов и их версий; (2) наличие соответствия записей уязвимостей базы CVE с базами OSVDB и X-

Force, а также между собой; (3) предоставление возможности как автоматизированного, так и ручного (для администраторов безопасности посредством web-интерфейса) доступа к возможностям поиска уязвимостей в интегрированной базе.

Дополнительным качеством разработанной библиотеки является наличие возможности автоматизированного обновления, как из сети Интернет, так и с локальных ресурсов (жесткий диск, FTP ресурсы), что позволяет поддерживать актуальность информации об уязвимостях на должном уровне для обеспечения высокой точности оценки защищенности исследуемых инфраструктур.

Аннотации публикаций

1. Chechulin A.A., Kotenko I.V. Real-Time Security Events Processing using an Approach based on the Attack Trees Analysis // Automatic Control and Computer Sciences, № 8, 2015, Springer, 2015. Принято к публикации.

В настоящей работе рассмотрен подход, позволяющий повысить скорость обработки событий безопасности с помощью деревьев атак. Особенностью предложенной методики является возможность получения за ограниченное время необходимых решений, причем обоснованность этих решений повышается с увеличением предоставляемого времени. Использование программных средств, основанных на применении данной методики, приведет к возможности выполнять аналитическое моделирование в современных средствах защиты, работающих в режиме, близком к реальному времени.

2. Maxim Kolomeec, Andrey Chechulin and Igor Kotenko. Methodological Primitives for Phased Construction of Data Visualization Models. Journal of Internet Services and Information Security (JISIS), Vol.5, No.4, November, 2015. P.60-84. http://www.jisis.org/vol5no4.php

В статье рассматриваются основные методологические примитивы для поэтапного построения модели визуализации с заранее подготовленными данными. Приводится методика поэтапного построения модели визуализации и пример построения модели визуализации на основе диаграммы Вороного.

3. Yana Bekeneva, Konstantin Borisenko, Andrey Shorov, Igor Kotenko. Investigation of DDoS Attacks by Hybrid Simulation // The 2015 Asian Conference on Availability, Reliability and Security (AsiaARES 2015). In conjunction with ICT-EurAsia 2015. October 4th – 7th, 2015, Daejeon, Korea / ICT-EurAsia 2015, Lecture Notes in Computer Science (LNCS), Vol.9357. IFIP International Federation for Information Processing (2015). Springer. 2015, P.179-189.

В настоящее время защита от распределенных атак типа "отказ в обслуживании" (DDoS) является одной из важнейших задач в области компьютерной безопасности. В статье рассматривается среда моделирования DDoS-атак различных типов, основанная на использовании комбинации имитационного подхода и реальных программно-аппаратных стендов. В работе описаны архитектура системы и серия экспериментов для моделирования DDoS-атак на транспортном уровне и уровне приложений. Представлены экспериментальные результаты и проведен их анализ.

4. Дойникова Е.В., Котенко И.В., Чечулин А.А. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах // Безопасность информационных технологий, № 3, 2015. Принято к публикации.

В статье предлагается подход к оцениванию защищенности компьютерных сетей, основанный на графах атак, и предназначенный для систем управления информацией и событиями безопасности. Основной особенностью подхода является применение разноуровневой системы показателей защищенности, определяющей профиль защищаемой системы в зависимости от характера применяемых для расчета показателей данных и методик вычисления показателей. Это позволяет корректировать оценку защищенности в режиме, близком к реальному времени, распознавать предыдущие и прогнозировать последующие шаги атак, определять цели и характеристики атакующих. На основе предлагаемого подхода реализован прототип системы оценивания защищенности и проведен анализ его функционирования на нескольких сценариях атак.

5. Котенко И.В., Дойникова Е.В. Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления

информацией и событиями безопасности // Информационно-управляющие системы, 2015, № 3, С.60-69. doi:10.15217/issn1684-8853.2015.3.60.
В статье предлагается методика выбора контрмер в процессе управления информацией и событиями безопасности. Разработанная методика основана на предложенной авторами комплексной системе показателей защищенности, отражающих ситуацию по безопасности в системе. Для выбора контрмер в систему показателей вводится дополнительный уровень поддержки принятия решений, базирующийся на показателях оценки эффективности применения контрмер. Основными особенностями предлагаемого подхода является использование графов атак и зависимостей сервисов, применение введенной в статье модели контрмер и предложенных показателей защищенности, а также возможность предоставления решения по выбору контрмер в любой момент времени в зависимости от текущей информации о состоянии защищенности и событиях безопасности.

6. Коломеец М.В., Чечулин А.А., Котенко И.В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Вып. 42. С. 232-257.
В статье рассматриваются основные методологические примитивы на примере поэтапного построения модели визуализации с заранее подготовленными данными, с целью сформировать комплексное видение процесса создания модели и влияющих на неё аспектов. Приводится классификация примитивов и их связи между собой в соответствии с этапами построения модели. Рассматриваются библиотеки визуализации на популярных языках программирования.

7. Котенко И.В., Новикова Е.С., Чечулин А.А. Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С.42-47.
В статье представлен анализ существующих методов визуализации информации, относящейся к безопасности. Приведена архитектура визуальной модели для отображения набора метрик, которая позволяет проводить их сравнительный анализ. Разработанная визуальная модель может быть использована для представления разных типов метрик, в том числе и для традиционных параметров безопасности, таких как, например, сетевые потоки.

8. Котенко И.В., Шоров А.В. Исследование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети» // Проблемы информационной безопасности. Компьютерные системы, № 3, 2015. С.45-55.
Развивается подход к имитационному моделированию механизмов защиты от инфраструктурных атак на основе биологической метафоры. Дана спецификация моделей инфраструктурных атак и механизмов защиты от них с помощью теоретико-множественного подхода. Представлены алгоритмы реализации атак и механизмов защиты. Детально рассмотрена среда моделирования механизмов защиты на основе биологической метафоры «нервная система сети». Произведена оценка основных показателей эффективности реализованной среды моделирования.

9. Десницкий В.А. Конфигурирование компонентов защиты встроенных устройств на основе эвристического подхода // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №46, 2015, С.16-20.
Цель работы – разработка процесса конфигурирования компонентов защиты встроенных устройств в части комбинирования компонентов защиты. с использованием экспертных

знаний в предметной области. В работе предложена эвристика для определения порядка учета нефункциональных характеристик в процессе комбинирования, а также используются правила для осуществления многокритериального выбора компонентов защиты.

10. Проноза А.А., Чечулин А.А. Модель извлечения данных разнородной структуры об информационных объектах компьютерной сети для подсистемы визуализации систем управления событиями и информацией безопасности // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.125-127.

Модель извлечения данных разнородной структуры об информационных объектах для подсистемы визуализации, описанная в данном тезисе, состоит из процедуры извлечения всех формализованных сообщений безопасности из всех имеющихся физических источников, а также процедуры вычисления количественных показателей безопасности по всем имеющимся логическим источникам. Полученная таким образом информация должна быть передана подсистеме визуализации для последующей обработки и анализа.

11. Дойникова Е.В. Генератор сценариев атак на основе классификации шаблонов атак CAPEC // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.71-72.

В публикации предлагается методика генерации сценариев атак на основе шаблонов атак открытой базы CAPEC. Рассматриваются основные входные данные методики и алгоритм генерации сценариев, а также область применения генератора.

12. Дойникова Е.В., Котенко И.В. Выбор защитных мер для управления защищенностью компьютерных сетей на основе комплексной системы показателей // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.114-115.

В публикации предлагается методика выбора защитных мер на основе показателей защищенности, вычисляемых с применением графов атак и графов зависимостей сервисов. Определяется модель контрмеры на основе открытых стандартов. Рассматриваются основные входные данные методики и основные этапы выбора контрмер в статическом и динамическом режимах работы системы.

13. Котенко И.В., Саенко И.Б., Чечулин А.А. Разработка систем управления информацией и событиями безопасности нового поколения // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.123-124.

Работа посвящена методам управления безопансостью мультисервисных сетей, составляющих телекоммуникационную основу единого информационного пространства. Рассматриваются постановки задач управления рисками безопасности сетей и методы их решения, основанные на использовании нечеткого логического вывода.

14. Федорченко А.В Комбинированный процесс корреляции событий безопасности в SIEM-системах // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-

02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.102-103.
В работе описываются методы корреляции событий безопасности и способ их комбинирования. Оценивается использование методов на разных стадиях процесса корреляции

15. Дойникова Е.В. Применение графов зависимостей сервисов в рамках задачи анализа защищенности компьютерных сетей для оценивания критичности ресурсов системы и обоснованного выбора защитных мер // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 68-69.
В публикации рассматривается методика оценивания критичности ресурсов системы на основе графов зависимостей сервисов. Определяются основные модели, применяемые для оценивания, в том числе модель сервиса и модель графа зависимостей сервисов. Описываются основные этапы оценивания.

16. Коломеец М.В., Чечулин А.А., Котенко И.В. Визуализация параметров безопасности компьютерных сетей с помощью диаграммы Вороного // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 73-74.
В публикации рассматривается разрабатываемая модель визуализации на основе Диаграммы Вороного, которая повысит эффективность отображения информации касающейся безопасности компьютерных сетей как со стороны визуализируемых данных, так и со стороны когнитивных особенностей человеческого восприятия.

17. Федорченко А.В. Правило-ориентированный метод корреляции событий безопасности в SIEM-системах // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 86-87.
Рассматриваются основы правило-ориентированного метода корреляции событий безопасности. Указаны особенности использования данного метода в SIEM-системах, а также описана возможные варианты применения на разных стадиях процесса корреляции

18. Чечулин А.А. Математические модели и алгоритмы моделирования атак и выработки контрмер в режиме, близком к реальному времени // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 90.
Основной темой данной публикации является разработка новых математических моделей и алгоритмов моделирования атак и выработки контрмер, которые могли бы использоваться в условиях больших объемов исходных данных и производить анализ системы защиты в условиях проводящихся атак в режиме близком к реальному времени, и, как следствие, рекомендовать оператору способы изменения политики безопасности системы защиты за ограниченное время.

19. Саенко И.Б., Котенко И.В. Модели и методы оценки эффективности функционирования системы разграничения доступа к ресурсам информационного пространства // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 85-86.

Рассматриваются модели и методы оценки эффективности функционирования системы разграничения доступа к ресурсам информационного пространства, основанные на имитационном моделировании попыток несанкционированного доступа, а также автоматической генерации объектов и полномочий доступа. Предложено в качестве показателей эффективности функционирования системы разграничения доступа использовать величину ошибок первого и второго рода за период модельного времени и рассчитываемую на их основе вероятность несанкционированного доступа.

20. Чечулин А.А. Классификация и модели представления связей между объектами в компьютерных сетях // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С. 165-170.
Современные информационные системы характеризуются большим объемом обрабатываемых данных, поэтому средства визуализации стали важным средством для решения задач анализа данных. Визуальный анализ данных позволяет значительно повысить эффективность работы аналитика благодаря использованию особенностей обработки зрительной информации человеком и возможностей вычислительных средств, предоставляя удобный инструмент по извлечению новых знаний из зашумленных данных большого объема. Одним из направлений в визуализации является визуализация компьютерных сетей. В данной работе предложена классификация и математические модели для представления связей между сетевыми объектами. Разработанные модели позволят повысить эффективность процессов мониторинга и управления информационной безопасностью в информационно-телекоммуникационных системах.

21. Смирнов Д.Б., Чечулин А.А. Корреляция данных безопасности в сетях «Интернет вещей» // Семнадцатая Международная конференция “РусКрипто’2015”. Московская область, г.Солнечногорск, 17-20 марта 2015 г. http://www.ruscrypto.ru/
В тезисе описана архитектура распределенной системы предназначенной для корреляции событий безопасности от встроенных устройств, представляющих собой элементы сети «Интернет вещей».