Форма 503 (итог). РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер Проекта
14-07-00697

3.2. Название Проекта
Модели и методы разграничения доступа к ресурсам единого информационно-коммуникационного пространства разнородных автоматизированных систем, основанные на технологии искусственного интеллекта

3.3. Коды классификатора, соответствующие содержанию фактически проделанной работы
07-241, 07-235, 07-956, 01-224

3.4. Объявленные ранее цели Проекта

Основные цели проекта на 2014-2016 годы определялись как разработка, совершенствование, реализация и экспериментальная оценка элементов научно-методологического обеспечения (моделей, методов и методик построения и функционирования) систем разграничения доступа к ресурсам единого информационно-коммуникационного пространства (ЕИКП), объединяющего разнородные автоматизированные системы, на основе применения методов искусственного интеллекта. При этом были выделены следующие научные направления: 1) оценка защищенности информационных и телекоммуникационных ресурсов ЕИКП разнородных автоматизированных систем от несанкционированного доступа и эффективности построения систем контроля и разграничения доступа к ЕИКП; 2) ориентированное на знания представление, верификация и оптимизация политик и схем разграничения доступа к информационным и телекоммуникационным ресурсам ЕИКП разнородных автоматизированных систем; 3) интеллектуальная поддержка принятия решений по разграничению доступа к ресурсам ЕИКП на основе логического вывода на знаниях и визуализации данных о политиках, схемах и событиях доступа; 4) управление уровнем защищенности информационных и телекоммуникационных ресурсов ЕИКП от несанкционированных воздействий на основе применения методов адаптации политик и схем разграничения доступа к изменениям условий и режимов функционирования ЕИКП.

Для достижения этих целей планировалось решение следующих задач: 1) анализ состояния исследований в области построения систем контроля и разграничения доступа к информационным и телекоммуникационным ресурсам ЕИКП разнородных автоматизированных систем, включая анализ угроз информационной безопасности ЕИКП; 2) общая формальная постановка задачи исследования; 3) разработка моделей, методов и алгоритмов, включая эволюционные алгоритмы, основанного на знаниях представления, верификации и оптимизации политик и схем разграничения доступа к информационным и телекоммуникационным ресурсам ЕИКП; 4) разработка методики поддержки принятия решений по разграничению доступа к ресурсам ЕИКП на основе логического вывода на знаниях и визуализации данных о политиках, схемах и событиях доступа, включая обоснование общей архитектуры и архитектуры отдельных компонентов единой системы разграничения доступа и формирование методики интеграции локальных схем разграничения доступа ЕИКП; 5) разработка моделей и методов адаптации политик и схем разграничения доступа к изменениям условий и режимов функционирования ЕИКП, в том числе с использованием онтологий и на основе эволюционных алгоритмов; 6) выработка научно-технических предложений по применению разработанных моделей, методов, методик и алгоритмов для обеспечения требований по разграничению доступа к ресурсам ЕИКП; 7) разработка программных прототипов и экспериментальная оценка полученных моделей, методов, методик и алгоритмов разграничения доступа к ресурсам ЕИКП.

3.5. Полученные в ходе выполнения Проекта важнейшие результаты

1. Модели и методы оценки эффективности функционирования единой системы разграничения доступа к разнородным информационным и телекоммуникационным ресурсам в ЕИКП.

Обоснована специфика моделей и методов оценки эффективности функционирования единой системы разграничения доступа (ЕСРД), обусловленная тем, что ЕСРД, с одной стороны, должна обеспечивать сохранение значений функциональных показателей разграничения доступа, имеющихся у отдельных субъектов доступа (пользователей либо автоматизированных систем) до их вхождения в ЕИКП, а с другой – обеспечивать поддержание значений новых функциональных показателей, характеризующих эффективность доступа одних субъектов доступа к ресурсам других субъектов доступа. При этом ЕСРД должна обеспечивать комплексирование различных моделей разграничения доступа (дискреционной, мандатной, ролевой и т.д.), присущих отдельным субъектам доступа, и возможность сохранения исходной модели разграничения доступа при выполнении операции проекции ЕСРД на отдельный субъект доступа.

Разработанные модели и методы оценки эффективности функционирования ЕСРД основаны на принципах имитационного моделирования попыток несанкционированного доступа, а также

автоматической генерации объектов и полномочий доступа. В качестве показателей эффективности функционирования ЕСРД учитывается количество ошибок первого и второго рода, совершаемых за заданный период модельного времени, а также рассчитываемая на их основе вероятность реализации несанкционированного доступа. В ходе автоматической генерации объектов и полномочий доступа учитываются заданные плотности распределения значений последних, а также общие количественные ограничения. Кроме того, используются различные алгоритмы поиска рациональных вариантов построения системы разграничения доступа. В частности, одним из разновидностей реализованных алгоритмов являются генетические алгоритмы оптимизации схем разграничения доступа к информационным и коммуникационным ресурсам, которые позволяют решать NP-полные задачи оптимизации, встречающиеся при формировании схем RBAC, VLAN и VPN. Разработан подход к использованию предложенных моделей и методов оценки эффективности функционирования ЕСРД, позволяющий не только проводить оценку ЕСРД по предложенным показателям, но и обнаруживать «узкие места» формируемой системы разграничения доступа в интересах повышения обоснованности принимаемых решений по обеспечению защищенности ЕИКП от несанкционированного доступа.

2. Модели и методики оценки и обеспечения оперативной доступности к информационным и телекоммуникационным ресурсам в ЕИКП.

Разработаны аналитические модели оценки и обеспечения оперативной доступности к ресурсам ЕИКП. При этом вид критериев оптимальности зависит от режимов функционирования ЕИКП, которыми являются on-line и off-line режимы. Сформирована постановка задача оптимизации размещения ресурсов по узлам ЕИКП с учетом имеющихся ограничений и коммуникационных возможностей. В состав исходных данных задачи входят: множество узлов ЕИКП; допустимый объем памяти для каждого узла; множество ресурсов, распределяемых по узлам; объемы ресурсов; матрица частот обращений к ресурсам с запросами; матрица пропускных способностей сети ЕИКП. Требуется распределить множество ресурсов по узлам таким образом, чтобы максимизировать показатели оперативной доступности с соблюдением ограничений по допустимым объемам памяти. Переменными являются элементы булевой матрицы, определяющие принадлежность ресурса к конкретному узлу. Целевые функции задачи зависят от режимов. Задача в режиме on-line рассматривается как задача обеспечения, а в режиме off-line – как задача оценки оперативной доступности к ресурсам ЕИКП. В on-line режиме дополнительно в состав исходных данных включаются требования по своевременности получения ресурсов по запросам.

Задача оценки оперативной доступности относится к классу линейного, а задача обеспечения – к классу нелинейного булевого программирования. Для решения задачи оценки предложены традиционные методы (алгоритм Гомори, метод ветвей и границ). Для решения задачи обеспечения оперативной доступности разработана методику, основанная на применении генетического алгоритм. Для его реализации предложены структура хромосом и вид соответствующей им функции пригодности (fitness function).

3. Модели, методы и алгоритмы основанного на знаниях представления, верификации и оптимизации политик и схем разграничения доступа к информационным и телекоммуникационным ресурсам ЕИКП.

Были предложены два подхода к построению данного класса моделей, методов и алгоритмов. Первый подход основан на использовании онтологий. Второй подход заключается в формировании оптимизационной постановки задачи и применении для ее решения методов биоинспирированной оптимизации (в частности, усовершенствованных генетических алгоритмов). Первый подход рассматривается как обладающий большей степенью универсальности. Однако он предполагает, что изначально в каждой из интегрируемых автоматизированных систем разграничение доступа осуществляется с использованием частных онтологий. Такое предположением не всегда справедливо на практике. Второй подход является менее универсальным и требует для каждого конкретного случая интеграции автоматизированных систем в ЕИКП формировать целевые функции и критерии оптимизации. Однако при втором подходе в проекте разработан ряд усовершенствований, позволяющих успешно применять для решения данных задач метод генетической оптимизации. К числу таких усовершенствований, разработанных и предложенных в ходе текущих исследований, относятся: (1) применение мульти-хромосомного кодирования возможных решений; (2) использование сложных объектов (в частности, столбцов искомых булевых матриц) в качестве генов хромосом; (3) введение в рассмотрение дополнительных хромосом (управляющих), предотвращающих появление недействительных решений и ускоряющих, тем самым, работу алгоритма; (4) двумерное скрещивание родительских хромосом, кодирующих переменные, выраженные в матричной форме; (5) генерация специального вида особей для начальной популяции (например, особей, соответствующих тривиальным решениям задачи).

4. Эволюционные алгоритмы, модели и методы разграничения доступа к информационным и телекоммуникационным ресурсам в ЕИКП.

Выполнены разработка и тестирование эволюционных алгоритмов, моделей и методов для предметных областей разграничения доступа к информационным и телекоммуникационным ресурсам в ЕИКП. При этом рассматривались следующие сценарии: (1) виртуальные локальные

вычислительные сети (VLAN, virtual local area networks); (2) виртуальные частные сети (VPN, virtual private networks) в защищенном информационном пространстве; (3) ролевые схемы доступа (RBAC, Role-based access control) к базам данных критических инфраструктур.
Для предметных областей VLAN и RBAC были разработаны унифицированные эвристические алгоритмы на основе метода генетической оптимизации. По сути, эти алгоритмы отличались друг от друга видом функции пригодности, зависящий от вида целевой функции в постановке задачи, а также структурой хромосом, которыми обладали особи в популяции алгоритма. Так, для VLAN особи имели одну хромосому, генами которой являлись столбцы матрицы требуемой логической связности компьютеров в сети. Для RBAC особи имели по три хромосомы, из которых две отражали связи между пользователями, ролями и ресурсами, а третья являлась служебной, предназначенной для обеспечения логической целостности хромосом. Кроме того, для скрещивания в случае RBAC применялся мульти-хромосомный подход, а в случае VLAN – двумерное скрещивание, повышающее результативность и оперативность работы алгоритма. В остальном работа алгоритмов была одинаковой.
Для предметной области VPN был разработан генетический алгоритм, в котором функция пригодности рассчитывалась как взвешенная сумма частных нормированных показателей эффективности, в роли которых выступали показатели пропускной способности, устойчивости и стоимости эксплуатации сети. Расчет частных показателей эффективности производился на аналитических моделях, основанных на теории массового обслуживания и теории графов. Теория массового обслуживания применялась для вывода выражений для оценки пропускной способности составного VPN-канала. Теория графов использовалась для разработки матричного метода расчета минимального числа транзитов в информационном направлении.
Тестирование разработанных алгоритмов проводилось на разработанном программно-инструментальном стенде, позволяющем автоматически генерировать требуемые схемы доступа для различных размерностей задач, управлять параметрами алгоритмов, а также проводить оценку и визуальный анализ хода решения задачи.

5. Модели, методы, методики и алгоритмы поддержки принятия решений по разграничению доступа к ресурсам ЕИКП на основе логического вывода на знаниях и визуализации данных о политиках, схемах и событиях доступа.

Предложена обобщенная методика поддержки принятия решений по разграничению доступа к ресурсам ЕИКП на основе логического вывода на знаниях и визуализации данных о политиках, схемах и событиях доступа. Методика содержит следующие этапы: (1) предварительный; (2) основной; (3) заключительный. На предварительном этапе формируется единая база знаний о разграничении доступа в онтологическом формате (формате RDF) путем интеграции частных онтологий разграничения доступа отдельных автоматизированных систем. На основном этапе для определения возможности доступа пользователя к конкретному ресурсу запускается механизм логического вывода, результат которого, с одной стороны, показывает, доступен ресурс пользователю или нет, а с другой – каковы полномочия пользователя в случае доступности ресурса. На заключительном этапе формируется визуальная модель представления данных, отражающая доступность ресурса и характер предоставленных пользователю полномочий по отношению как к заданному, так и к другим, соседним, ресурсам.
Для повышения эффективности визуального анализа данных о политиках, схемах и событиях доступа разработано семейство моделей, обладающих следующими возможностями: 1) кластеризация больших массивов данных; 2) автоматическая классификация массивов данных; 3) «ленивая» загрузка массивов данных при визуализации; 4) детализация кластеризованных данных (Drill-down). В качестве основного алгоритма кластеризации использовался алгоритм CLOPE (Clustering with sLOPE), обеспечивающий более высокую производительность и лучшее качество кластеризации в сравнении со многими иерархическими алгоритмами. Его достоинствами являются: а) высокая масштабируемость и скорость работы, а также качество кластеризации; б) автоматический подбор количества кластеров, регулируемый одним параметром - коэффициентом отталкивания. Для автоматической классификации применялись алгоритмы Naïve Bayes и Decision Tree, базовые предсказания которых объединялись с помощью алгоритма Stacking. Для обеспечения «ленивой» загрузки (lazy loading) реализован механизм загрузки данных, позволяющий отсрочить инициализацию объекта (объектов) до момента времени, в котором это необходимо. Для обеспечения детализации кластеризованных данных (Drill-down) разработаны подход и метод анализа информации в ЕСРД, предусматривающий пошаговый переход к более низким уровням иерархии элементов измерений для получения более детальных сведений об объектах и полномочиях доступа.
Разработанные модели и методы визуализации схем и политик разграничения доступа к ресурсам ЕИКП были реализованы табличными и иерархическими способами.

6. Общая архитектура и архитектура отдельных компонентов единой системы разграничения доступа к разнородным информационным и телекоммуникационным ресурсам в ЕИКП.

Произведена разработка общей архитектуры и архитектуры отдельных компонентов ЕСРД к разнородным информационным и телекоммуникационным ресурсам в ЕИКП. При этом учитывалось,

что ЕИКП является не только системой, обеспечивающая требуемую защищенность информационных и сетевых ресурсов, но и средством интеграции разнородных ресурсов. Разработанная общая архитектура ЕСРД включает три уровня своего построения: 1) локальный уровень; 2) уровень интеграции данных; 3) аналитический уровень.
Локальный уровень ЕСРД образуют локальные системы разграничения доступа (ЛСРД) отдельных автоматизированных систем, ресурсы которых интегрируются в ЕИКП. Формальное задание ЛСРД обеспечивается с помощью локальных схем и политик разграничения доступа отображением декартова произведения множества пользователей и множества ресурсов локальной автоматизированной системы на множество полномочий. Вид этого отображения зависит от используемых в ЛСРД моделей управления доступом.
На уровне интеграции данных ЕСРД осуществляется формирование единых схем и политик разграничения доступа. Формально задача их построения сводится к тому, чтобы сформировать отображение декартова произведения множества пользователей и множества ресурсов всего ЕИКП на множество полномочий. При этом должно выполняться условие, заключающееся в том, что проекция ЕСРД по локальным множествам пользователей, ресурсов и полномочий должна приводить к соответствующей ЛСРД.
Обосновано основное противоречие построения ЕСРД, которое обусловлено тремя факторами. Во-первых, один и тот же пользователь может являться пользователем различных локальных систем. С другой стороны, один и тот же контролируемый ресурс может являться общим для различных локальных систем. Наконец, полномочия доступа между этим пользователем и ресурсом в различных локальных системах могут быть также различными. В силу существования данного противоречия решение задачи построения ЕСРД не является тривиальным.
В результате основным компонентом ЕСРД на уровне интеграции данных является центральное хранилище схем разграничения и политик доступа, которое должно обеспечивать возможность хранения данных как в SQL-формате, так и в форматах, обеспечивающих применение методов искусственного интеллекта, а именно XML- и RDF-форматах. Обосновано, что в основу построения центрального хранилища ЕСРД целесообразно положить онтологический подход.
На аналитическом уровне основными компонентами ЕСРД являются компонент анализа и компонент принятия решений. Необходимость в данных компонентах обусловлена основным противоречием построения ЕСРД. Компонент анализа решает задачу обеспечения целостности и непротиворечивости ЕСРД. Компонент принятия решений решает задачу формирования адекватных изменений схем и политик ЕСРД при появлении изменений в ЛСРД, причем выполняемых с минимальными затратами. Последнее условие необходимо для обеспечения разрешимости основного противоречия построения ЕСРД.

7. Модели и методы адаптации политик и схем разграничения доступа к изменениям условий и режимов функционирования ЕИКП.

В ходе исследования вопросов реализации моделей и методов адаптации политик и схем разграничения доступа к изменениям условий и режимов функционирования ЕИКП были сформулированы постановки задачи адаптивного изменения политик и схем разграничения доступа к разнородным ресурсам. В качестве критерия задачи предложено условие минимизации трудозатрат администратора безопасности на выполнение работ по переходу к новой схеме разграничения доступа с сохранением уровней конфиденциальности и доступности информации, обеспечиваемых предыдущей схемой доступа. Показано, что в случае схем разграничения доступа к телекоммуникационным ресурсам (на примере виртуальных подсетей) постановка задачи сводится к поиску минимума для DX при заданной DA и матрице X, которые связаны друг с другом уравнением вида X*XT+DA=(X+DX)(X+DX)T. Постановка задачи для адаптивного изменения политик и схем разграничения доступа к информационным ресурсам заключается в поиске минимума для (DX+DY) при заданных DA, X и Y, связанных уравнением X*Y+DA= (X+DX)(Y+DY).
Показано, что сформулированные задачи являются задачами булевой матричной факторизации и являются NP-полными. Для их решения разработаны генетические алгоритмы в которых в качестве генов хромосом используются столбцы искомых булевых матриц, а скрещивание хромосом родительских особей выполняется в двумерном режиме. Для реализации предложенных алгоритмов разработаны программные прототипы.

8. Моделей и методов использования онтологий для управления разграничением доступа к разнородным ресурсам ЕИКП.

Произведены исследование и разработка моделей и методов использования онтологий для управления разграничением доступа к разнородным ресурсам ЕИКП. При этом выявлено, что онтология как средство поддержки логического вывода может быть использована для многих современных моделей доступа, таких как RBAC, ABAC (Attributes Based Access Control), OrBAC (Organization Based Access Control) и других.
Показано, что в качестве базисной онтологии ЕСРД может выступать онтология предметной области, политику доступа которой можно рассматривать как совокупность правил оперирования объектами, представленными в данной онтологии. При этом данные правила не составляют суть самих объектов

или процессов с их участием, а являются лишь отображением корректных действий субъектов доступа ЕИКП по отношению к объектам доступа.
Сущность модели использования онтологий заключается в создании универсальной, кросс-платформенной информационной структуры, использующей как собственные семантические метаописания данных, так и надстройки к уже существующим разнородным информационным массивам (базам данных). Предложенная формальная онтологическая модель управления доступом позволяет полностью описать семантику базовых понятий управления доступа к сервисам ЕИКП. Онтологическая модель инвариантна относительно форматов представления описаний прав доступа к сервисам, что позволяет ее использовать как конечными пользователями, так и автоматизированными анализаторами. Формальная модель онтологии для разграничения доступа определяется в виде тройки следующего вида: O = <C, R, F>, где C – конечное множество концептов; R – конечное множество отношений между концептами; F – конечное множество функций интерпретации, заданных на концептах и/или отношениях. В состав онтологической модели ЕСРД включена собственная подсистема доступа, содержащая формальные записи политик доступа к сервисам, семантика которых определена онтологической моделью. Подсистема доступа обеспечивает управление доступом к сервисам на основе RBAC и возможность делегирования полномочий управления доступа к объектам доступа.
Метод использования онтологии для управления разграничением доступа к ЕИП содержит два этапа. На первом этапе для каждой автоматизированной системы создается локальная онтология, содержащая концепты предметной области, задач, сведения о пользователей. На втором уровне создается онтология верхнего уровня, предназначение которой является установление соответствия терминов и семантических связей локальных онтологий.

9. Программные прототипы разработанных моделей, методов, методик и алгоритмов разграничения доступа к ресурсам ЕИКП.

Произведена экспериментальная оценка полученных моделей, методов, методик и алгоритмов с использованием разработанных программных прототипов, составляющих программно-инструментальный стенд для оценки и формирования ЕСРД к ресурсам ЕИКП. Стенд позволяет не только вычислять значения показателей эффективности проектируемых схем разграничения доступа для различных сценариев (VLAN, VPN, RBAC и т.д.), но и осуществлять визуальный анализ хода поиска оптимального решения. Проведенные на стенде эксперименты показали, что разработанные модели, методы и алгоритмы обладают высокими значениями частных показателей эффективности (точности, оперативности, достоверности). Найденные на стенде экспериментальные зависимости могут найти широкое применение на практике. Разработанные программные средства «Поддержка принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи», «Программно-инструментальный стенд визуализации и оценки качества проектирования виртуальных компьютерных сетей для поддержки принятия решений при мониторинге и управлении информационной безопасностью», «Программное средство оценки оперативности доступа к ресурсам единого информационно-коммуникационного пространства» и «Программное средство оценки защищенности информации от угроз несанкционированного доступа в автоматизированных системах на основе экспертных оценок» зарегистрированы в Реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности (свидетельства о государственной регистрации программы для ЭВМ №№ 2014660775, 2015615772, 2015662574 и 2016614484).

3.6. Сопоставление полученных результатов с мировым уровнем

Основные научные результаты являются новыми и оригинальными, они основываются на разработках исполнителей проекта, выполненных ранее и выполняемых в настоящее время, а также базируются на современных достижениях в области защиты информации от несанкционированного доступа, интеллектуального анализа данных, эволюционного моделирования, оптимизации сложных систем, онтологического моделирования, разработки и применения механизмов логического вывода и др.
Все результаты, полученные в ходе выполнения проекта в 2014-2016 гг., соответствуют мировому уровню. Авторы проекта изложили основные результаты в 11 статьях, опубликованных в изданиях, индексируемых в международных базах цитирования WoS и Scopus, в 27 статьях, опубликованных в журналах, входящих в список ВАК, а также в прочих журналах и трудах конференций.
Результаты были апробированы на множестве различных всероссийских и международных конференций, основными из которых являются следующие: 8-й международный симпозиум по интеллектуальным распределенным вычислениям (IDC-2014), Мадрид, Испания, 2014; 6-й международный симпозиум по безопасности и защите киберпространства (CSS 2014), Париж, Франция, 2014; 16-я и 17-я Международные конференции «РусКрипто», Московская обл., 2014 и 2015; IV Международная научно-практическая конференция «ИнтеллектТранс-2014», Санкт-Петербург, 2014; Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности», Минск, Республика Беларусь, 2014; 14-я и 15-я национальные конференции по искусственному интеллекту с международным участием (КИИ), Казань (2014), Смоленск (2015); Международный конгресс по интеллектуальным системам и

информационным технологиям «IS&IT’14», Дивноморское, Краснодарский край, 2014, 2015, 2016; 23-я, 24-я и 25-я научно-технические конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 2014, 2015, 2016; 8-я и 9-я Всероссийские конференции «Информационные технологии в управлении» (ИТУ), Санкт-Петербург, 2014, 2016; XIV и XV Санкт-Петербургские международные конференции «Региональная информатика (РИ), 2014, 2015; IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР), Санкт-Петербург, 2015; Международный конгресс по информатике: информационные системы и технологии (CSIST), Республика Беларусь, Минск, 2016; XIX Международная конференция по мягким вычислениям и измерениям (SCM), Санкт-Петербург, 2016; Международный симпозиум по безопасности мобильного Интернета (MobiSec’16), Тайвань, 2016; 29-я Международная научная конференция «Математические методы в технике и технологиях» (ММТТ), Санкт-Петербург, 2016.

3.7.1. Методы и подходы, использованные в ходе выполнения Проекта

В ходе выполнения проекта получили дальнейшее развитие следующие методы и подходы:
1) методы теории оптимизации в части формирования формализованных постановок задач синтеза схем разграничения доступа к разнородным информационным и телекоммуникационным ресурсам и применения генетических алгоритмов оптимизации для их решения;
2) методы эволюционного моделирования сложных систем в части разработки усовершенствованных генетических алгоритмов оптимизации, которые ориентированы на повышение своего быстродействия при больших размерностях задачи;
3) методы генетической оптимизации в применении к новым областям разграничения доступа, в частности, для задач адаптивного изменения схем разграничения доступа к ролевым схемам разграничения доступа и схем разграничения доступа к виртуальным локальным вычислительным сетям ЕИКП;
4) методы интеллектуального анализа данных в части разработки усовершенствованного алгоритма для решения проблемы нахождения минимального множества виртуальных подсетей;
5) метод интеллектуального иерархического управления разграничением доступа в защищенных мультисервисных сетях;
6) метод нечеткого логического вывода применительно к мультисервисным сетям ЕИКП;
7) онтологический подход к построению и управлению единой системы разграничения доступа к разнородным ресурсам ЕИКП;
8) методы системного анализа и теории систем в части их применения для разработки концепции интеллектуализации разграничения доступа в компьютерных системах и сетях.

3.7.2. Вклад каждого члена коллектива в выполнение Проекта в 2016 году

Десницкий Василий Алексеевич:
- разработка моделей и методов для новых предметных областей разграничения доступа к информационным и телекоммуникационным ресурсам в ЕИКП (Интернет вещей, системы контроля доступа периметра и др.)
- разработка моделей и методов выявления аномальных данных в схемах и политиках разграничения доступа информационно-телекоммуникационных систем на основе экспертных знаний;
- разработка модели и реализация методики верификации политиках разграничения доступа информационно-телекоммуникационных систем;
- разработка предложений по проектированию защищенного ЕИКП в кибер-физических системах;
- экспериментальная оценка полученных результатов.

Дойникова Елена Владимировна:
- разработка методики оценки защищенности ЕИКП от несанкционированного доступа к информационным и сетевым ресурсам, учитывающей иерархическую систему показателей;
- разработка методики и программного средства выбора контрмер для обеспечения защищенности ЕИКП от несанкционированного доступа к информационным и сетевым ресурсам, реализующих динамический перерасчет показателей;
- разработка методики и программного компонента оценки рисков безопасности ресурсов ЕИКП;
- экспериментальная оценка полученных результатов.

Комашинский Дмитрий Владимирович:
- разработка предложений по интеграции локальных схем разграничения доступа к разнородным ресурсам ЕИКП;
- разработка предложений по совершенствованию онтологического подхода к управлению доступов к ресурсам ЕИКП;
- экспериментальная оценка полученных результатов.

Новикова Евгения Сергеевна:
- разработка методов и методик выявление аномалий в схемах и политиках разграничения доступа ЕИКП на основе применения специализированных моделей визуализации данных;
- экспериментальная оценка полученных результатов.

Саенко Игорь Борисович:
- разработка моделей, методик и алгоритмов интеграции локальных схем разграничения доступа к разнородным информационным и телекоммуникационным ресурсам в ЕИКП;
- разработка моделей и методик оценки и обеспечения оперативной доступности к информационным и телекоммуникационным ресурсам в ЕИКП;
- совершенствование моделей и методов использования онтологий для управления разграничением доступа к разнородным ресурсам ЕИКП;
- совершенствование эволюционных алгоритмов, моделей и методов для новых предметных областей разграничения доступа к информационным и телекоммуникационным ресурсам в ЕИКП;
- разработка моделей и методов визуального анализа схем и политик разграничения доступа к ресурсам единого информационного пространства;
- разработка научно-технических предложений по применению разработанных моделей, методов, методик и алгоритмов для обеспечения требований по разграничению доступа к ресурсам ЕИКП;
- разработка программных прототипов для полученных моделей, методов, методик и алгоритмов разграничения доступа к ресурсам ЕИКП;
- экспериментальная оценка полученных результатов.

Чечулин Андрей Алексеевич:
- разработка моделей и комплексной методики формирования единого системы разграничения доступа к информационным и коммуникационным ресурсам;
- разработка моделей, методов и алгоритмов анализа угроз защищенности информационных и сетевых ресурсов от несанкционированного доступа;
- разработка моделей и методик визуализации данных о топологии компьютерной сети и их применения для управления разграничением доступа к информационным и сетевым ресурсам ЕИКП;
- классификация условий, влияющих на необходимость реконфигурации схем и политик разграничения доступа в ЕИКП;
- разработка предложений по использованию моделей корреляции событий и инцидентов безопасности в интересах управления схемами и политиками разграничения доступа к ресурсам ЕИКП;
- разработка программных прототипов для полученных моделей, методов, методик и алгоритмов разграничения доступа к ресурсам ЕИКП;
- экспериментальная оценка полученных результатов.

Браницкий Александр Александрович:
- разработка моделей и методов применения эволюционно-генетической иммунной системы и логического вывода на основе сигнатурного анализа и методов вычислительного интеллекта для выявления аномалий в системах разграничения доступа к информационным и сетевым ресурсам;
- экспериментальная оценка полученных результатов.

Федорченко Андрей Владимирович:
- разработка методики оценки эффективности системы разграничения доступа на основе анализа и моделирования комбинированного процесса корреляции событий безопасности.
- экспериментальная оценка полученных результатов.

3.8.1. Количество научных работ по Проекту, опубликованных в 2016 году

32

3.8.1.1. Из них в изданиях, включенных в перечень ВАК

11

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

23

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

2

3.8.2. Количество научных работ, подготовленных в ходе выполнения Проекта и принятых к печати в 2016 году

1

3.9. Участие в 2016 году в научных мероприятиях по тематике Проекта

1. Международный конгресс по информатике: информационные системы и технологии (CSIST-2016), 24–27 октября 2016 г., Республика Беларусь, Минск; пленарный доклад.
2. XIX International Conference on Soft Computing and Measurements (SCM'2016), St. Petersburg, May 25-27, 2016; секционные доклады.

3. International Symposium on Mobile Internet Security (MobiSec'16), Taichung, Taiwan, July 14-15, 2016; секционный доклад.
4. 9-я конференция "Информационные технологии в управлении" (ИТУ-2016), 4-6 октября 2016 г., Санкт-Петербург; секционные доклады.
5. Международная научная конференция «Математические методы в технике и технологиях» (ММТТ-29), 31 мая – 3 июня 2016 г., Санкт-Петербург; секционные доклады.
6. 25-я научно-техническая конференция «Методы и технические средства обеспечения безопасности информации». 4 июля - 7 июля 2016 г., Санкт-Петербург; секционные доклады.
7. Международный конгресс по интеллектуальным системам и информационным технологиям (IS-IT'16), 4-9 сентября 2016 г., Дивноморское; секционные доклады.
8. Пятнадцатая национальная конференция по искусственному интеллекту с международным участием (КИИ-2016), 3-7 октября 2016 года, Смоленск; секционные доклады.
9. XV Санкт-Петербургская международная конференция "Региональная информатика-2016" ("РИ-2016"), 25-27 октября 2016 г., Санкт-Петербург; секционные доклады.

3.10. Участие в 2016 году в экспедициях по тематике Проекта, которые проводились при финансовой поддержке Фонда

Не было

3.11.1. Финансовые средства, полученные в 2016 году от Фонда *(в руб.)*

525000

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

600000

3.11.3. Финансовые средства, полученные в 2014 году от Фонда *(в руб.)*

500000,00

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

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

3.13. Библиографический список всех публикаций по проекту за весь период выполнения проекта, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.

В изданиях, индексируемых в международных базах Scopus, WoS:

1. Igor Kotenko, Igor Saenko. A Genetic Approach for Virtual Computer Network Design // Intelligent Distributed Computing VIII. Studies in Computational Intelligence. Springer-Verlag, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain. Springer-Verlag. P.95-105.
2. I.V. Kotenko and I.B. Saenko. Creating New Generation Cybersecurity Monitoring and Management Systems // Herald of the Russian Academy of Sciences, 2014, Vol.84, No.6. P.993–1001.
3. Igor Kotenko, Elena Doynikova. Security Evaluation Models for Cyber Situational Awareness // The 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS 2014). August 20-22, 2014, Paris, France. 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.1229-1236.
4. Igor Kotenko, Olga Polubelova, Igor Saenko. Logical Inference Framework for Security Management in Geographical Information Systems // V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems, Lecture Notes in Geoinformation and Cartography, Springer-Verlag, Berlin, Heidelberg, 2014. P.203-218.
5. Igor Saenko, Igor Kotenko. Design of Virtual Local Area Network Scheme based on Genetic Optimization and Visual Analysis // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 2014, Vol.5, No.4. P.86-102.
6. Igor Kotenko, Igor Saenko. Improved genetic algorithms for solving the optimization tasks in access scheme design for computer networks // International Journal of Bio-Inspired Computation, Inderscience Enterprises Ltd., Vol. 7, No. 2, 2015, P.98-110.
7. Vasily Desnitsky, Igor Kotenko. Design and Verification of Protected Systems with Integrated Devices Based on Expert Knowledge // Automatic Control and Computer Sciences, Allerton Press, Inc., Vol. 49, No. 8, 2015. P.648-652.
8. Andrey Chechulin, Igor Kotenko. Attack Tree-based Approach for Real-Time Security Event Processing. Automatic Control and Computer Sciences, Allerton Press, Inc., 2015, Vol. 49, No. 8, P.701-704.
9. Maksim Kolomeec, Andrey Chechulin, Igor Kotenko. Methodological Primitives for Phased Construction of Data Visualization Models // Journal of Internet Services and Information Security (JISIS), 2015, Vol. 5, No. 4. P.60-84.

10. Vasily Desnitsky, Igor Kotenko. Event analysis for security incident management on a perimeter access control system // XIX International Conference on Soft Computing and Measurements (SCM'2016). IEEE Xplore, 2016. P.481-483.
11. Igor Kotenko, Dmitry Levshun, Andrey Chechulin. Event correlation in the integrated cyber-physical security system // XIX International Conference on Soft Computing and Measurements (SCM'2016). IEEE Xplore, 2016. P.484-486.

В изданиях по перечню ВАК и индексируемых в РИНЦ:
12. Котенко И.В., Саенко И.Б., Чечулин А.А. Проактивное управление информацией и событиями безопасности в информационно-телекоммуникационных системах // Вопросы радиоэлектроники. Сер. СОИУ. 2014. Вып. 1. С. 170–180.
13. Котенко И.В., Саенко И.Б., Юсупов Р.М. Новое поколение систем мониторинга и управления инцидентами безопасности // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. СПбГПУ, 2014, № 3 (198), С.7-18.
14. Котенко И.В., Саенко И.Б. К новому поколению систем мониторинга и управления безопасностью // Вестник Российской академии наук, Том 84, № 11, 2014, С.993–1001.
15. Дойникова Е.В., Котенко И.В. Отслеживание текущей ситуации и поддержка принятия решений по безопасности компьютерной сети на основе системы показателей защищенности // Изв. вузов. Приборостроение, Т.57, № 10, 2014, С.72-77. ISSN 0021-3454.
16. Носков А.Н., Чечулин А.А. Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных // Труды СПИИРАН. Вып.6 (37). СПб.: Наука, 2014.
17. Саенко И.Б., Котенко И.В. Применение средств генетической оптимизации и визуального анализа для формирования схем доступа в виртуальных локальных вычислительных сетях // Информационные технологии и вычислительные системы, № 1, 2015, С.33-46.
18. Куваев В.О., Чечулин А.А., Ефимов В.В., Лыжинкин К.В. Варианты построения единого информационного пространства для интеграции разнородных автоматизированных систем // Научно-технический журнал «Информация и космос», № 4, 2015. С.83-87.
19. 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.
20. М.В. Коломеец, А.А. Чечулин, И.В. Котенко. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Вып. 42. С. 232-257.
21. Браницкий А.А., Котенко И.В. Построение нейросетевой и иммуноклеточной системы обнаружения вторжений // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С. 23-27.
22. Котенко И.В., Чечулин А.А., Комашинский Д.В. Автоматизированное категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Проблемы информационной безопасности. Компьютерные системы, № 2, 2015. С.69-79.
23. Браницкий А.А., Котенко И.В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейро-нечетких классификаторов // Информационно-управляющие системы, 2015, № 4. С.69-77.
24. Десницкий В.А., Котенко И.В. Формирование экспертных знаний для разработки защищенных систем со встроенными устройствами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С. 35-41.
25. 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.
26. Дойникова Е.В., Котенко И.В., Чечулин А.А. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах // Безопасность информационных технологий, № 3, 2015. С. 33-42.
27. Саенко И.Б., Котенко И.В., Скорик Ф.А. Мониторинг и прогнозирование состояния компьютерных сетей на основе применения гибридных нейронных сетей // Изв. вузов. Приборостроение, Т.59, № 10, 2016, С.795-800.
28. Саенко И. Б., Лаута О. С., Котенко И. В. Применение метода преобразования стохастических сетей для моделирования мобильных банковских атак // Изв. вузов. Приборостроение, Т.59, № 11, 2016, С.928-933.
29. Коломеец М.В., Чечулин А.А., Котенко И.В. Методика визуализации топологии компьютерной сети для мониторинга безопасности // Изв. вузов. Приборостроение, Т.59, № 10, 2016, С.807-812.
30. Дойникова Е.В., Котенко И.В. Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности // Информационно-управляющие системы, 2016, № 5, С.54-65.

31. Новожилов Д.А., Чечулин А.А., Котенко И.В. Улучшение категорирования веб-сайтов для блокировки неприемлемого содержимого на основе анализа статистики html-тэгов // Информационно-управляющие системы, 2016 (в печати)
32. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных кибер-физических устройств // Труды СПИИРАН. 2016. Вып. 5(48). С.5-31.
33. Новикова Е.С., Котенко И.В. Выявление аномальной активности в сервисах мобильных денежных переводов с помощью RADViz-визуализации // Труды СПИИРАН. 2016. Вып. 5(48). С.32-51.
34. Проноза А.А., Чечулин А.А., Котенко И.В. Математические модели визуализации в SIEM-системах // Труды СПИИРАН. 2016. Вып. 3(46). С.90-107.
35. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2(45). С.207-244.
36. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В., Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. 2016. Вып. 4 (47). С. 5-27.
37. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В., Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 // Труды СПИИРАН. 2016. Вып. 6(49). С.208-225.
38. Новикова Е.С., Котенко И.В., Федотов Е.С. Визуальный анализ данных для обнаружения аномалий в сервисах мобильных денежных переводов // Защита информации. Инсайд, № 4, 2016. С.40-47; № 5, 2016. С.72-82.

Зарубежные международные конференции:
39. Саенко И.Б., Котенко И.В. Основы построения перспективных систем мониторинга и управления безопасностью для защиты критически важных объектов информатизации // Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности». 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
40. Нестерук Ф.Г. Специфика двухуровневой организации адаптивных систем защиты информации // Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности». 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.С. 227-231.
41. Саенко И.Б., Кушнеревич А.Г., Котенко И.В. Реализация платформы распределенных параллельных вычислений для сбора и предварительной обработки больших данных мониторинга в кибер-физических системах // Международный конгресс по информатике: информационные системы и технологии (CSIST-2016). Материалы международного научного конгресса. Республика Беларусь, Минск, 24–27 октября 2016 г., 641-645.
42. Igor Saenko, Oleg Lauta, Igor Kotenko. Analytical modeling of mobile banking attacks based on a stochastic network conversion technique // The 2016 International Symposium on Mobile Internet Security (MobiSec'16). Taichung, Taiwan. July 14-15, 2016. 10 p.

В изданиях, индексируемых в базе РИНЦ:
43. Куваев В.О., Саенко И.Б. Концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве // Проблемы экономики и управления в торговле и промышленности, № 7 (007), 2014. – С. 101-104. ISSN 2309-3064.
44. Саенко И.Б., Куваев В.О., Алышев С.В. Подход к построению системы показателей качества единого информационного пространства // Естественные и математические науки в современном мире, 2014. № 14. С. 51-56.
45. Котенко И.В., Саенко И.Б. Предложения по реализации логического вывода для управления кибербезопасностью в АСУ железнодорожного транспорта // Естественные и математические науки в современном мире. 2014. № 14. Новосибирск: Изд. «СибАК», С. 46-50.
46. Котенко И.В., Саенко И.Б. Методика верификации политик безопасности в многоуровневой интеллектуальной системе обеспечения комплексной безопасности железнодорожного транспорта // Технические науки - от теории к практике. Новосибирск: Изд. «СибАК», 2014. № 30. С. 18-22.
47. Десницкий В.А., Чечулин А.А. Обобщенная модель нарушителя и верификации информационно-телекоммуникационных систем со встроенными устройствами // Технические науки - от теории к практике. Новосибирск: Изд. «СибАК», 2014. №38, С.7-21.
48. Саенко И.Б., Куваев В.О. О применении методов искусственного интеллекта для разграничения доступа к ресурсам единого информационного пространства разнородных автоматизированных систем // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.631-637.
49. Котенко И.В., Саенко И.Б. О задачах обеспечения кибербезопасности в инфраструктурах «электронного города» на основе методов искусственного интеллекта // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.618-622.

50. Десницкий В.А. Верификация сетевых информационных потоков систем со встроенными устройствами на основе экспертных знаний // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.596-600.
51. Агеев С.А., Саенко И.Б. Управление рисками информационной безопасности защищенной мультисервисной сети специального назначения на основе интеллектуальных мультиагентов // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.556-562.
52. Саенко И.Б., Куваев В.О., Бирюков М.А. Использование онтологий для управления разграничением доступа к разнородным ресурсам единого информационно-коммуникационного пространства // Технические науки – от теории к практике, 2015, № 11 (47), С. 76-80.
53. Саенко И.Б., Куваев В.О., Бирюков М.А. Общая архитектура единой системы разграничения доступа к разнородным ресурсам в едином информационно-коммуникационном пространстве // Технические науки – от теории к практике, 2015, № 11 (47), С. 70-75.
54. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №47, 2015, С.14-18.
55. Десницкий В.А., Дойникова Е.В. Архитектура и оценка эффективности программного средства конфигурирования компонентов защиты систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №47, 2015, С.9-13.
56. Левшун Д.С., Чечулин А.А. Постановка задачи построения единого хранилища мультимедийных данных из полевых этнографических экспедиций // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №46, 2015, С. 25-30.
57. Саенко И.Б., Бирюков М.А. Методика интеграции локальных схем разграничения доступа к разнородным ресурсам единого информационного пространства // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.758-762.
58. Десницкий В.А. Выявление аномальных данных от сенсоров встроенных устройств на основе экспертных знаний // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.676-679.
59. Десницкий В.А. Реализация средства верификации сетевых информационных потоков с использованием метода «проверки на модели» // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.680-683.
60. Дойникова Е.В., Котенко И.В. Методика оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016.
61. Новожилов Д.А., Чечулин А.А. Разработка стенда для проведения экспериментов с методами классификации веб-сайтов // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.740-749.
62. Чечулин А.А. Алгоритмы построения и модификации моделей атак для анализа защищенности компьютерных сетей // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.782-785.
63. Браницкий А.А., Котенко И.В. Методики комбинирования бинарных классификаторов для выявления аномальных сетевых соединений // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.660-664.
64. Браницкий А.А. Модифицированная модель вычислительной иммунной системы на базе эволюционно-генетического подхода для обнаружения и классификации аномальных сетевых соединений // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.656-659.
65. Саенко И.Б., Куваев В.О. Модель и методика оценки и обеспечения оперативной доступности к ресурсам единого информационного пространства // Математические методы в технике и технологиях – ММТТ-29 [текст]: сб. трудов XXIX Междунар. науч. конф.: в 12 т. Т.6. / под общ. ред. А.А. Большакова. – Саратов: Саратов. гос. техн. ун-т; Санкт-Петербург: СПбГТИ(ТУ), СПбПУ, СПИИРАН; Самара: Самарск. гос. техн. ун-т, 2016. – С.139–142.
66. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа к разнородным ресурсам единого информационного пространства // Математические методы в технике и технологиях – ММТТ-29 [текст]: сб. трудов XXIX Междунар. науч. конф.: в 12 т. Т.6. / под общ. ред. А.А. Большакова. – Саратов: Саратов. гос.

техн. ун-т; Санкт-Петербург: СПбГТИ(ТУ), СПбПУ, СПИИРАН; Самара: Самарск. гос. техн. ун-т, 2016. – С.122-125.

67. Дойникова Е.В., Федорченко А.В. Методики автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов // XXIX Международная научная конференция "Математические методы в технике и технологиях - ММТТ-29", 31 мая - 3 июня 2016 года, Санкт-Петербургский государственный технологический институт, Санкт-Петербург, Россия (в печати).

68. Котенко И.В., Саенко И.Б. Генетические алгоритмы для булевой матричной факторизации применительно к задачам разграничения доступа в компьютерных сетях // Пятнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (3-7 октября 2016 года, г. Смоленск, Россия): Труды конференции. Т.3. Смоленск: Универсум, 2016. С.98-106.

69. Коломеец М.В., Котенко И.В., Чечулин А.А. Модель визуализации для интеллектуальной системы мониторинга кибербезопасности, базирующаяся на аналоге диаграмм Вороного // Пятнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (3-7 октября 2016 года, г. Смоленск, Россия): Труды конференции. Т.3. Смоленск: Универсум, 2016. С.180-187.

Прочие публикации

70. Куваев В.О., Саенко И.Б. Подход к решению задачи разграничения доступа в разнородном информационном пространстве // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.33-34.

71. Котенко И.В., Новикова Е.С. Модели и методики визуального анализа данных для решения задач компьютерной безопасности // Шестнадцатая Международная конференция «РусКрипто-2014». Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/

72. Котенко И.В., Саенко И.Б. О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта // Интеллектуальные системы на транспорте: Материалы IV международной научно-практической конференции «ИнтеллектТранс-2014». – СПб.: ПГУПС, 2014. С.196-203.

73. Котенко И.В., Новикова Е.С. Визуальная аналитика на страже информационной безопасности // Международный форум по практической безопасности Positive Hack Days. Москва. 21-22 мая 2014 г. http://www.phdays.ru

74. Котенко И.В., Саенко И.Б. Об архитектуре многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.97-98.

75. Агеев С.А., Саенко И.Б. Интеллектуальные методы управления рисками информационной безопасности мультисервисных сетей связи // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.59-60.

76. Котенко И.В., Саенко И.Б. Система логического вывода и верификации политик безопасности в автоматизированных системах железнодорожного транспорта // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT-14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.2. С.271-276. 978-5-9221-1572-8.

77. Саенко И.Б., Котенко И.В. Генетический подход к проектированию виртуальных компьютерных сетей на основе генетических алгоритмов // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT-14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.1. С.35-40. ISBN 978-5-9221-1572-8.

78. Котенко И.В., Саенко И.Б. Интеллектуальная система мониторинга и управления инцидентами кибербезопасности // Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 (24–27 сентября 2014 года, г. Казань, Россия): Труды конференции. Т.3. Казань: Изд-во РИЦ «Школа», 2014. С.219-227.

79. Дойникова Е.В., Котенко И.В. Оценивание защищенности в автоматизированных системах управления РЖД // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.132-133.

80. Дойникова Е.В. Поддержка принятия решений по выбору защитных мер в информационных системах на основе комплекса показателей защищенности // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.132.

81. Агеев С.А., Саенко И.Б. Оценка и управление рисками информационной безопасности в защищенных мультисервисных сетях на основе методов искусственного интеллекта // XIV Санкт-

Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.116-117.
82. Котенко И.В., Саенко И.Б. Поддержка принятия решений по безопасности информации в АСУ железнодорожного транспорта на основе онтологического моделирования данных // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.144.
83. Котенко И.В., Саенко И.Б. Модели и методы визуального анализа больших объемов данных и событий безопасности автоматизированных систем железнодорожного транспорта // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.143.
84. Котенко И.В., Саенко И.В., Чечулин А.А. Проактивное управление информацией и событиями безопасности в сетях NGN // Материалы семинара Международного союза электросвязи «Переход развивающихся стран с существующих сетей на сети нового поколения (NGN): технические, экономические, законодательные и политические аспекты», Санкт- Петербург, СПб ГУТ им Бонч-Бруевича. 23–25 июня 2014 года.
85. Котенко И.В., Саенко И.Б. Генетический подход к проектированию виртуальной частной сети в защищенном информационном пространстве // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT’15, 2015, Том 2. С.320-325.
86. Десницкий В.А. Модели процесса разработки комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT’15, 2015, Том 2. С. 113-118.
87. 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.
88. Саенко И.Б., Котенко И.В. Адаптивное изменение политик и схем разграничения доступа к ресурсам единого информационного пространства // 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.127-128.
89. Агеев С.А., Васильев Д.В., Саенко И.Б. Управление безопасностью защищенной мультисервисной сети специального назначения // 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.106-107.
90. 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.
91. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // 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.69-70.
92. 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.
93. 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.
94. 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.
95. Чечулин А.А., Проноза А.А. Классификация и анализ типов связей в компьютерных сетях для их последующей визуализации // 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.132-133.
96. 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.

97. 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.
98. Левшун Д.С., Чечулин А.А., Коломеец М.В., Котенко И.В. Архитектура системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 76.
99. Браницкий А.А. Методы вычислительного интеллекта для обнаружения и классификации аномалий в сетевом трафике // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 61-62.
100.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.
101.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.
102.Новожилов Д.А., Чечулин А.А. Разработка программных средств поддержки проведения экспериментов по классификации веб-сайтов // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 80-81.
103.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.
104.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/
105.Саенко И.Б., Котенко И.В., Круглов С.Н. Генетический подход к реконфигурированию схем ролевого доступа в едином информационном пространстве // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'16, 2016, Том 1. С.13-18.
106.Саенко И.Б., Котенко И.В., Круглов С.Н. Поход к решению «проблемы извлечения ролей» при формировании модели RBAC на основе генетических алгоритмов // Материалы 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 4 июля - 7 июля 2016 г. Санкт-Петербург. Издательство Политехнического университета. 2016. С.113.
107.Саенко И.Б., Котенко И.В. Модели и методы визуального анализа схем и политик разграничения доступа к ресурсам единого информационного пространства // XV Санкт-Петербургская Международная Конференция "Региональная информатика-2016" ("РИ-2016"). Материалы конференции. СПб., 2016. С. 192-193.

Свидетельства о регистрации программ для ЭВМ:
108.Саенко И.Б., Агеев С.А., Чечулин А.А. Поддержка принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи. Свидетельство № 2014660775. Зарегистрировано в Реестре программ для ЭВМ 15.10.2014.
109.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.
110.Саенко И.Б., Чечулин А.А., Куваев В.О., Барыкин Н.А. Программное средство оценки оперативности доступа к ресурсам единого информационно-коммуникационного пространства. Свидетельство № 2015662574. Зарегистрировано в Реестре программ для ЭВМ 16.11.2015.
111.Саенко И.Б., Котенко И.В., Авраменко В.С., Бобрешов-Шишов Д.И. Программное средство оценки защищенности информации от угроз несанкционированного доступа в автоматизированных системах на основе экспертных оценок. Свидетельство № 2016614484. Зарегистрировано в Реестре программ для ЭВМ 25.04.2016.

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, навигационных 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 выполнения Проекта проведен анализ состояния исследований в области построения систем контроля и разграничения доступа к информационным и телекоммуникационным ресурсам и анализ угроз единого информационно-коммуникационного пространства (ЕИКП). Анализ показал, что при построении ЕИКП необходимо ориентироваться на новую парадигму «пространство данных» (data space), которая является дальнейшим развитием парадигмы «хранилище данных» (data warehouse), а последняя в свою очередь – развитием парадигмы «база данных» (data base). Пространство данных в структурном плане отличается от хранилища тем, что интегрирует данные, содержащиеся в хранилищах, совместно с электронными информационными ресурсами, хранящимися отдельно от хранилищ и баз данных.

Сформирована общая формальная постановка задачи исследования, определяющая исходные данные, критерии и допущения. Критерии задачи определяют степень соблюдения единой системой разграничения доступа ЕИКП правил частных политик разграничения доступа, изначально установленных в каждой из интегрируемых автоматизированных систем.

Определены требования по безопасности, достоверности и производительности ЕСРД в ЕИКП. Требования по достоверности и производительности сводятся к тому, что изменение ЕСРД в случае изменения множеств пользователей, ресурсов и/или полномочий должно производиться и завершаться до наступления новых изменений в этих множествах.

Определены подходы к разработке единой системы разграничения доступа в ЕИКП, которые связаны с использованием онтологий и постановкой и решением оптимизационных задач для схем разграничения доступа. Для решения оптимизационных задач предложены усовершенствованные генетические алгоритмы, отличающиеся рядом инноваций. К их числу относятся: применение мульти-хромосомного кодирования возможных решений; использование сложных объектов в качестве генов хромосом; введение в рассмотрение дополнительных управляющих хромосом, обеспечивающих целостность решений и др.

Выполнены разработка и тестирование эволюционных алгоритмов, моделей и методов для предметных областей разграничения доступа к информационным и телекоммуникационным ресурсам в ЕИКП, каковыми являются: виртуальные локальные вычислительные сети (VLAN); виртуальные частные сети (VPN); ролевые схемы доступа (RBAC) к базам данных критических инфраструктур. Для VLAN и RBAC были разработаны эвристические алгоритмы на основе метода генетической оптимизации. При этом для скрещивания особей при RBAC применялся мульти-хромосомный подход, а для VLAN – двумерное скрещивание. Для VPN разработан генетический алгоритм, в котором функция пригодности рассчитывалась как взвешенная сумма нормированных показателей эффективности. Показатели эффективности рассчитывались на основе положений теории массового обслуживания и теории графов.

Разработаны общая архитектура и архитектуры отдельных компонентов ЕСРД. Архитектура ЕСРД включает три уровня своего построения: локальный уровень; интеграции данных; аналитический. Локальный уровень ЕСРД образуют локальные системы разграничения доступа (ЛСРД). На уровне интеграции данных ЕСРД осуществляется формирование единых схем и политик разграничения доступа. На аналитическом уровне основными компонентами ЕСРД являются компонент анализа и компонент принятия решений.

Проведены исследование и разработка моделей и методов использования онтологий для управления разграничением доступа к разнородным ресурсам ЕИКП. Предложена формальная модель управления доступом в виде онтологической модели, которая позволяет полностью описать семантику базовых понятий управления доступа к ресурсам ЕИКП. В состав онтологической модели ЕСРД включена собственная подсистема доступа, содержащая формальные записи политик доступа к сервисам, семантика которых определена моделью.

Проведено исследование и выполнена разработка моделей и методов решения задач адаптивного изменения политик и схем разграничения доступа к разнородным информационным и телекоммуникационным ресурсам ЕИКП. В качестве критерия решения задачи предложено условие минимизации трудозатрат администратора безопасности на выполнение работ по переходу к новой схеме разграничения доступа с сохранением уровней конфиденциальности и доступности информации, обеспечиваемых предыдущей схемой доступа. Сформированы формальные постановки задач реконфигурации схем доступа к ресурсам ЕИП для сценариев RBAC и VLAN, основанные на решении задач булевой матричной факторизации. Показано, что в случае реконфигурации схем доступа VLAN постановка задачи сводится к поиску минимума для

DX при заданной DA и матрице X, которые связаны друг с другом уравнением вида $X*X^T+DA=(X+DX)(X+DX)^T$. Постановка задачи реконфигурации RBAC заключается в поиске минимума (DX+DY) при заданных DA, X и Y, связанных уравнением X*Y+DA=(X+DX)(Y+DY).

Исследованы и разработаны модели и методы оценки эффективности функционирования ЕСРД к разнородным информационным и телекоммуникационным ресурсам ЕИКП, основанные на принципах имитационного моделирования попыток несанкционированного доступа, а также автоматической генерации объектов и полномочий доступа. В качестве показателей эффективности функционирования ЕСРД используются значения количества ошибок первого и второго рода, совершаемых за заданный период модельного времени, а также рассчитываемая на их основе вероятность реализации несанкционированного доступа. В ходе автоматической генерации объектов и полномочий доступа учитываются заданные плотности распределения значений последних, а также общие количественные ограничения. Разработан подход к использованию предложенных моделей и методов оценки эффективности функционирования ЕСРД, позволяющий не только проводить верификацию ЕСРД по предложенным показателям, но и обнаруживать «узкие места» формируемой системы разграничения доступа в интересах повышения обоснованности принимаемых решений по обеспечению защищенности ЕИКП от несанкционированного доступа.

Разработаны модели и методики оценки и обеспечения оперативной доступности к информационным и телекоммуникационным ресурсам, ориентированные на on-line и off-line режимы функционирования ЕИКП. При этом вид критериев оптимальности зависит от режимов функционирования ЕИКП, которыми являются on-line и off-line режимы. Сформирована постановка задача оптимизации размещения ресурсов по узлам ЕИКП с учетом имеющихся ограничений и коммуникационных возможностей. Задача в режиме on-line рассматривается как задача обеспечения, а в режиме off-line – как задача оценки оперативной доступности к ресурсам ЕИКП. В on-line режиме дополнительно в состав исходных данных включаются требования по своевременности получения ресурсов по запросам.

Предложена обобщенная методика поддержки принятия решений по разграничению доступа к ресурсам ЕИКП. На предварительном этапе методики формируется единая база знаний о разграничении доступа в формате RDF путем интеграции частных онтологий разграничения доступа отдельных автоматизированных систем. На основном этапе запускается механизм логического вывода, результат которого, с одной стороны, показывает, доступен ресурс пользователю или нет, а с другой – каковы полномочия пользователя в случае доступности ресурса. На заключительном этапе формируется визуальная модель представления данных. Разработано семейство моделей визуализации, обладающих следующими возможностями: кластеризация больших массивов данных; автоматическая классификация массивов данных; «ленивая» загрузка массивов данных при визуализации; детализация кластеризованных данных.

Проведено исследование и выполнена разработка моделей и методов использования онтологий для управления разграничением доступа к разнородным ресурсам ЕИКП. Сущность модели использования онтологий заключается в создании универсальной, кросс-платформенной информационной структуры, использующей как собственные семантические метаописания данных, так и надстройки к уже существующим разнородным базам данных.

Произведена экспериментальная оценка полученных моделей, методов, методик и алгоритмов с использованием разработанных программных прототипов, составляющих программно-инструментальный стенд для оценки и формирования ЕСРД к ресурсам ЕИКП. Проведенные на стенде эксперименты показали, что разработанные модели, методы и алгоритмы обладают высокими значениями частных показателей эффективности (точности, оперативности, достоверности). Разработанные программные средства «Поддержка принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи», «Программно-инструментальный стенд визуализации и оценки качества проектирования виртуальных компьютерных сетей для поддержки принятия решений при мониторинге и управлении информационной безопасностью», «Программное средство оценки оперативности доступа к ресурсам единого информационно-коммуникационного пространства» и «Программное средство оценки защищенности информации от угроз несанкционированного доступа в автоматизированных системах на основе экспертных оценок» зарегистрированы в Реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности (свидетельства о государственной регистрации программы для ЭВМ №№ 2014660775, 2015615772, 2015662574 и 2016614484).

Аннотации публикаций

1. Igor Kotenko, Igor Saenko. A Genetic Approach for Virtual Computer Network Design // Intelligent Distributed Computing VIII. Studies in Computational Intelligence. Springer-Verlag, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain. Springer-Verlag. P.95-105.

Одним из возможных уровней защиты информации может являться разделение компьютерной сети на логические фрагменты, которые известны как виртуальные компьютерные сети, или виртуальные подсети. Статье рассматривает новый подход к определению виртуальных подсетей, который основан на учете заданной матрицы логической связности компьютеров. Показано, что рассматриваемая проблема представляет собой одну из форм булевой матричной факторизации. Она формирует задачу проектирования виртуальных подсетей и предлагает использовать генетический алгоритм как средство ее решения. Основные усовершенствования, предложенные в статье, заключаются в использовании тривиальных решений для генерации начальной популяции, учете в функции пригодности критерия минимального числа подсетей и использовании столбцов матрицы связности в качестве генов хромосом. Эксперименты показали, что предложенный генетический алгоритм имеет высокую эффективность.

2. I.V. Kotenko and I. B. Saenko. Creating New Generation Cybersecurity Monitoring and Management Systems // Herald of the Russian Academy of Sciences, 2014, Vol.84, No.6. P.993–1001. ISSN 1019-3316.

В статье рассматривается технология управления событиями и информацией безопасности – новое интенсивно развивающееся направление в области кибербезопасности, которое обладает достаточно большим потенциалом как в отношении обнаружения угроз, так и с точки зрения выработки контрмер, обеспечивающих требуемый уровень безопасности информационных инфраструктур. Системы мониторинга и управления кибербезопасностью, ориентированные на эту технологию, предполагают оперативный сбор, хранение и последующую аналитическую обработку данных о событиях, связанных с безопасностью.

3. Igor Kotenko, Elena Doynikova. Security Evaluation Models for Cyber Situational Awareness // The 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS 2014). August 20-22, 2014, Paris, France. 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.1229-1236.

В статье рассматриваются методики измерения и вычисления показателей защищенности на основе графов атак и зависимостей сервисов. Методики основаны на нескольких уровнях оценивания (топологическом, графа атак, атакующего, событий и системы) и таких важных аспектах, как атаки нулевого дня и стоимостные характеристики атак. Они позволяют оценить текущую ситуацию по защищенности, в том числе определить уязвимые и слабые места системы, выявить опасные события, параметры проходящих и возможных кибер-атак, намерения атакующих, вычислить интегральные показатели защищенности и определить возможные защитные меры.

4. Igor Kotenko, Olga Polubelova, Igor Saenko. Logical Inference Framework for Security Management in Geographical Information Systems // V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems, Lecture Notes in Geoinformation and Cartography, DOI: 10.1007/978-3-642-31833-7_14, Springer-Verlag, Berlin, Heidelberg, 2014. P.203-218.

Разработка программных средств реализации логического вывода на основе знаний о безопасности информации и событий является перспективным направлением исследований для обеспечения безопасности в крупных информационных системах, включая распределенные геоинформационные системы. Платформы, которые используют логические языки и системы логического вывода, предоставляют администраторам мощные и гибкие средства, которые обеспечивают верификацию политик безопасности, создание эффективных контрмер против компьютерных атак и поддержание требуемого уровня безопасности. В статье излагается новый подход для разработки и осуществления системы логического вывода для управления информацией и событий безопасности. Рассматриваются общая архитектура этой системы, а также детали архитектуры и реализация конкретных модулей логического вывода, основанные на исчислении событий, методе «проверки на моделях» и онтологическом представлении данных в репозитории.

5. Igor Saenko, Igor Kotenko. Design of Virtual Local Area Network Scheme based on Genetic Optimization and Visual Analysis // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.5, No.4, December 2014. P.86-102.

В статье рассматривается подход к генетической оптимизации схемы виртуальной локальной вычислительной сети с использованием разработанного инструментария – средства проектирования схемы VLAN. Авторы предлагают формальную постановку задачи оптимизации схемы VLAN, решение которой может улучшить надежность и безопасность функционирования корпоративной компьютерной сети. В статье показано, что рассматриваемая проблема является одной из форм булевой матричной факторизации. В предложенном генетическом алгоритме был реализован ряд усовершенствований, касающихся формирования начальной популяции, вида функции пригодности, кодирования хромосом и выполнения операций скрещивания и мутации. Средство проектирования схемы VLAN позволяет решать проблему с помощью генетического алгоритма, формировать визуальное представление хода решения задачи и

обеспечивает оценку генетического алгоритма. Экспериментальные результаты подтвердили высокую эффективность предложенного генетического алгоритма.

6. Igor Kotenko, Igor Saenko. Improved genetic algorithms for solving the optimization tasks in access scheme design for computer networks // International Journal of Bio-Inspired Computation, Inderscience Enterprises Ltd., Vol. 7, No. 2, 2015, P.98-110.

Проектирование схем разграничения доступа является одной из наиболее важных задач в области обеспечения безопасности компьютерных сетей, которая должна решаться администраторами и разработчиками систем безопасности. Качество разграничения доступа очень сильно зависит от таких свойств безопасности, как конфиденциальность и доступность информации. Одним из возможных решений этой проблемы является сведение ее к форме оптимизационной задачи, решаемой математическими методами. Тем не менее, из-за высокой сложности этой задачи, применение традиционных математических методов является затруднительным. В то же время, генетические алгоритмы представляют собой новое и очень интересное направление решения такого класса задач. В статье предлагается подход для проектирования схем разграничения доступа, основанный на генетических алгоритмах. Для совершенствования генетических операций, предлагается ряд существенных усовершенствований, которые включают мульти-хромосомное представление особей в популяциях, использование сложных типов данных для представления генов в хромосомах и использование специальных управляющих хромосом. Обсуждается экспериментальная оценка этого подхода. Показано, что предложенные усовершенствованные генетические алгоритмы являются достаточно эффективными средствами для оптимизации схем разграничения доступа в компьютерных сетях.

7. Vasily Desnitsky, Igor Kotenko. Design and Verification of Protected Systems with Integrated Devices Based on Expert Knowledge // Automatic Control and Computer Sciences, Allerton Press, Inc., Vol. 49, No. 8, 2015. P.648-652.

Предложен подход к выявлению экспертных знаний в области информационной безопасности встроенных устройств для их дальнейшего использования разработчиками встроенных устройств, в том числе в качестве входных данных автоматизированных инструментов проектирования и верификации встроенных устройств. Цель работы – формирование, структуризация и уточнение экспертных знаний, характеризующие различные аспекты проектирования и верификации механизмов защиты встроенных устройств, а также поиск и адаптация существующих и разработка новых методик и автоматизированных программных инструментов для их последующего использования разработчиками устройств. Основной вклад настоящей статьи – предлагаемая методика проектирования и верификации на основе выявленных экспертных знаний в предметной области, нацеленная на разработку комбинированных механизмов защиты встроенных устройств с учетом показателей ресурсопотребления, а также возможных конфликтов и аномалий компонентов защиты и информационных потоков. Методика характеризуется заложенной в нее специфичной экспертной информацией о системных ресурсах встроенных устройств, типовых конфликтах и аномалиях. Методика включает следующие основные стадии: (1) конфигурирование компонентов защиты встроенного устройства; (2) верификация системы защиты на предмет выявления скрытых конфликтов; (3) верификации сетевых информационных потоков.

8. Andrey Chechulin, Igor Kotenko. Attack Tree-based Approach for Real-Time Security Event Processing. Automatic Control and Computer Sciences, Allerton Press, Inc., 2015, Vol. 49, No. 8, P.701-704.

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.

9. Maksim Kolomeec, Andrey Chechulin, Igor Kotenko. Methodological Primitives for Phased Construction of Data Visualization Models // Journal of Internet Services and Information Security (JISIS), 2015, Vol. 5, No. 4. P.60-84.

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.

10. Vasily Desnitsky, Igor Kotenko. Event analysis for security incident management on a perimeter access control system // XIX International Conference on Soft Computing and Measurements (SCM'2016). IEEE Xplore, 2016. P.481-483.

Работа посвящена вопросам анализа и управления инцидентами безопасности в информационно-телекоммуникационных системах Интернета вещей. Представлен общий подход к анализу событий безопасности на основе принципов проактивности, динамичности и многоаспектности. Предложены элементы программно-аппаратной реализации для системы управления инцидентами безопасности на примере кибер-физической системы контроля и управления доступом с использованием микроконтроллеров и RFID-сканеров.

11. Igor Kotenko, Dmitry Levshun, Andrey Chechulin. Event correlation in the integrated cyber-physical security system // XIX International Conference on Soft Computing and Measurements (SCM'2016). IEEE Xplore, 2016. P.484-486.

Данная статья посвящена исследованию подходов к интеграции гетерогенных источников данных для организации защиты от кибер-физических атак. В статье рассмотрена архитектура предлагаемой комплексной системы безопасности, основные этапы и методы корреляции данных, а так же примеры применения подобной системы.

12. Котенко И.В., Саенко И.Б., Чечулин А.А. Проактивное управление информацией и событиями безопасности в информационно-телекоммуникационных системах // Вопросы радиоэлектроники. Сер. СОИУ. 2014. Вып. 1. С. 170–180.

В статье рассматриваются вопросы построения проактивных систем управления и мониторинга безопасности информации для современных информационно-телекоммуникационных систем. Обсуждаются решения, полученные в ключевых областях, связанных с построением репозитория и анализом событий безопасности на основе моделирования сетевых атак

13. Котенко И.В., Саенко И.Б., Юсупов Р.М. Новое поколение систем мониторинга и управления инцидентами безопасности // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. СПбГПУ, 2014, № 3 (198), С.7-18.

Обоснована технологическая необходимость разработки нового поколения систем мониторинга и управления инцидентами безопасности, основанных на технологии управления информацией и событиями безопасности. Приведены типовая архитектура и основные решения по построению отдельных модулей таких систем, осуществляющих устойчивый сбор данных о событиях безопасности, их универсальную трансляцию, масштабируемую обработку, гибридное онтологическое хранение и многофункциональную визуализацию, а также межуровневую корреляцию событий, моделирование атак и прогностический анализ безопасности. Сформулированы предложения по применению таких систем в предметных областях, касающихся обеспечения безопасности в критических инфраструктурах.

14. Котенко И.В., Саенко И.Б. К новому поколению систем мониторинга и управления безопасностью // Вестник Российской академии наук, Том 84, № 11, 2014, С.993–1001.

В статье обобщены основные результаты по построению систем управления событиями и информацией безопасности, а также рассмотрены возможные сценарии применения этих разработок.

15. Дойникова Е.В., Котенко И.В. Отслеживание текущей ситуации и поддержка принятия решений по безопасности компьютерной сети на основе системы показателей защищенности // Изв. вузов. Приборостроение, Т.57, № 10, 2014, С.72-77.

Рассматривается подход к отслеживанию текущей ситуации по защищенности компьютерной сети и поддержке принятия решений по реагированию на инциденты безопасности, основанный на использовании предлагаемой системы показателей защищенности и разработанных моделей и алгоритмов их расчета. Ключевой особенностью подхода является учет разноплановой информации при вычислении показателей защищенности, что позволяет более точно отразить текущую ситуацию по безопасности компьютерной сети

16. Носков А.Н., Чечулин А.А. Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных // Труды СПИИРАН. Вып.6 (37). СПб.: Наука, 2014.

Анализ методик систем обнаружения сетевых атак является перспективным направлением в области защиты сетей и сетевых систем. В статье рассматривается подход к оценке алгоритмов и механизмов обнаружения атак. Новизна предлагаемой методики заключается в возможности создания самообучающихся систем для обнаружения вторжения. В статье рассмотрены основные элементы алгоритмов обнаружения атак.

17. Саенко И.Б., Котенко И.В. Применение средств генетической оптимизации и визуального анализа для формирования схем доступа в виртуальных локальных вычислительных сетях // Информационные технологии и вычислительные системы, № 1, 2015, С.33-46.

Рассматривается подход к проектированию виртуальной локальной вычислительной сети (ВЛВС), основанный на использовании программного средства генетической оптимизации и визуального анализа схемы доступа ВЛВС. Излагается формальная постановка задачи оптимизации схемы доступа ВЛВС, решение которой повышает надежность и безопасность функционирования корпоративной вычислительной сети. Показано, что рассматриваемая задача относится к одной из форм булевой матричной факторизации и является NP-полной. В разработанном генетическом алгоритме, предложенном для решения поставленной задачи, реализован ряд усовершенствований, касающихся формирования начальной популяции, вида функции пригодности, кодирования хромосом и выполнения операций скрещивания и мутации. Разработанное программное средство реализует генетический алгоритм, формирует визуальное отображение хода решения задачи и обеспечивает оценку решения задачи. Экспериментальные результаты показали высокую эффективность разработанного генетического алгоритма.

18. Куваев В.О., Чечулин А.А., Ефимов В.В., Лыжинкин К.В. Варианты построения единого информационного пространства для интеграции разнородных автоматизированных систем // Информация и космос. Научно-технический журнал, № 4, 2015. С.83-87.

В статье рассматриваются возможные варианты построения единого информационного пространства, объединяющего информационные ресурсы разнородных автоматизированных систем. Приведены классификационные признаки построения единого информационного пространства. Предложена система показателей качества, полученная при подходе, в котором на информационные средства распространяются результаты анализа стандартов и исследований в области оценки качества программных средств. Проводится анализ номенклатуры качества программного обеспечения, следующих действующих стандартов: отечественном стандарте ГОСТ Р ИСО/МЭК 9126-93 и пакете международных стандартов ISO 9126. Предложенный подход к построению системы показателей качества единого информационного пространства задает основу для анализа и синтеза вариантов построения единого информационного пространства в условиях строгого учета предъявляемых к нему требований. Предложена методика оценки качества единого информационного пространства

19. 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.

20. 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 нее аспектов. Приводится классификация примитивов и их связи между собой в соответствии с этапами построения модели. Рассматриваются библиотеки визуализации на популярных языках программирования.

21. Браницкий А.А., Котенко И.В. Построение нейросетевой и иммуноклеточной системы обнаружения вторжений // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С. 23-25.

В статье рассматриваются методы обнаружения и классификации аномальных образцов сетевых соединений с использованием аппарата искусственных нейронных сетей и эволюционной модели иммунной системы.

22. Котенко И.В., Чечулин А.А., Комашинский Д.В. Автоматизированное категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Проблемы информационной безопасности. Компьютерные системы, № 2, 2015. С.69-79.

В статье представлен подход к классификации веб-страниц с помощью методов интеллектуального анализа данных. Предложена архитектура и алгоритмы работы системы сбора, хранения и анализа данных, необходимой для классификации сайтов по определенным категориям. Разработана программная система для автоматизации классификации веб-страниц. Проведены эксперименты, выявившие основные проблемы, возникающие при построении систем классификации веб-страниц. Эксперименты, описанные в статье, показали высокую точность классификации веб-страниц, что подтверждает возможность использования разработанной технологии в системах блокирования веб-сайтов с неприемлемым содержимым.

23. Браницкий А.А., Котенко И.В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейро-нечетких классификаторов // Информационно-управляющие системы, 2015, № 4, С.69-77.

В статье предложена обобщенная схема комбинирования классификаторов для обнаружения сетевых атак. На ее основе разработано программное средство, которое позволяет анализировать сетевой трафик на наличие аномальной сетевой активности.

24. Десницкий В.А., Котенко И.В. Формирование экспертных знаний для разработки защищенных систем со встроенными устройствами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С.35-41.

Раскрывается подход к формированию экспертных знаний для разработки защищенных систем со встроенными устройствами. Комбинирование компонентов защиты, выявление аномальных данных в системе и структурных несовместимостей компонентов защиты производится на основе знаний о целевой системе, требованиях и компонентах защиты. Настоящая работа нацелена на формирование, структуризацию и уточнение экспертных знаний, характеризующих различные аспекты проектирования, верификации и тестирования механизмов защиты систем со встроенными устройствами, а также поиск и адаптацию существующих и разработку новых методик и автоматизированных программных инструментов для их последующего использования разработчиками устройств. Основной вклад настоящей статьи – методика проектирования, верификации и тестирования на основе выявленных экспертных знаний в предметной области в части комбинирования компонентов защиты с использованием эвристики, верификации системы для выявления известных видов несовместимостей компонентов защиты и тестирования системы на предмет выявления аномальных данных в них.

25. 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.

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.

26. Дойникова Е.В., Котенко И.В., Чечулин А.А. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах // Безопасность информационных технологий, № 3, 2015. С. 33-42.

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.

27. Саенко И.Б., Котенко И.В., Скорик Ф.А. Мониторинг и прогнозирование состояния компьютерных сетей на основе применения гибридных нейронных сетей // Изв. вузов. Приборостроение, Т.59, № 10, 2016, С.795-800.

Для мониторинга и прогнозирования состояния компьютерных сетей необходимо использовать средства, имеющие высокую адаптивность и устойчивость к внешним шумам. Такими возможностями обладают гибридные нейронные сети. В статье рассматриваются модели для оценки и прогнозирования состояния компьютерных сетей, основанные на гибридных нейронных сетях. Результаты проведенных экспериментов показали, что предложенные модели обладают достаточно высокой точностью классификации текущего и прогнозируемого состояния компьютерной сети.

28. Саенко И. Б., Лаута О. С., Котенко И. В. Применение метода преобразования стохастических сетей для моделирования мобильных банковских атак // Изв. вузов. Приборостроение, Т.59, № 11, 2016, С.928-933.

Предложен подход к моделированию мобильных банковских атак, основанный на методе преобразования стохастических сетей. Достоинствами предложенного метода являются достаточно высокая скорость моделирования, а также высокая достоверность и чувствительность результатов к изменению исходных данных. Проведена экспериментальная оценка метода, которая подтвердила его достаточно высокую эффективность.

29. Коломеец М.В., Чечулин А.А., Котенко И.В. Методика визуализации топологии компьютерной сети для мониторинга безопасности // Изв. вузов. Приборостроение, Т.59, № 10, 2016, С.807-812.

Разработана методика визуализации данных топологии компьютерной сети для мониторинга безопасности, применяемого в SIEM-системах, а также системах мониторинга компьютерных сетей и сетевой активности. Методика основана на использовании соотношения эффективности восприятия и информативности отображаемых данных. Методика учитывает возможные модели визуализации, которые могут быть применены для отображения данных мониторинга безопасности, особенности когнитивного аппарата оператора, которые были рассмотрены коллективом авторов в предыдущих работах. Методика включает в себя все этапы процесса визуализации, что позволяет рассматривать отдельные компоненты системы визуализации данных безопасности на уровне архитектуры разрабатываемого или анализируемого программного средства. Представленные результаты могут быть использованы при разработке систем визуализации, для повышения эффективности уже реализованных систем, а также для оценки их эффективности. Приводится пример использования методики для повышения эффективности визуализации топологии компьютерных сетей с использованием древовидных и графовых структур.

30. Дойникова Е.В., Котенко И.В. Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности // Информационно-управляющие системы, 2016, № 5, С.54-65.

Проблема реагирования на компьютерные атаки остается актуальной, так как количество компьютерных угроз год от года не уменьшается, информационные технологии применяются повсеместно, а сложность и размер сетевых инфраструктур растет. Соответственно растет и необходимость в усовершенствовании механизмов оценки защищенности и выбора мер реагирования. Для адекватного реагирования на атаки необходим грамотный всесторонний анализ рисков системы, дающий значимую и

реально отражающую ситуацию по защищенности оценку. Хотя исследователями были предложены различные подходы, универсального решения найти не удалось. Цель исследования: разработка методик оценки риска, адекватно отражающих текущую ситуацию по защищенности на основе автоматизированной обработки доступных данных по безопасности, разработка реализующего их программного средства и оценка эффективности методик на основе экспериментов. Результаты: разработаны и реализованы в рамках программного средства методики оценки рисков, основанные на ранее предложенной авторами комплексной системе показателей защищенности. Уточнены некоторые аспекты вычисления показателей для оценки рисков, отличающие предложенные методики от аналогичных работ. Разработанный программный компонент позволяет гибко выбирать методику в зависимости от текущей ситуации и требований пользователя программного средства. На экспериментах показана реализация методик в программном средстве, результаты их работы, выделены достоинства и недостатки. Практическая значимость: разработанные методики и программный компонент позволят повысить защищенность информационных систем за счет предоставления значимой и адекватной оценки защищенности системы.

31. Новожилов Д.А., Чечулин А.А., Котенко И.В. Улучшение категорирования веб-сайтов для блокировки неприемлемого содержимого на основе анализа статистики html-тэгов // Информационно-управляющие системы, 2016 (в печати)

В статье рассматривается проблема улучшения качества категорирования веб-сайтов методами Data Mining для автоматизированных систем родительского контроля, целью которых является защита от нежелательной или неприемлемой информации. Приведена архитектура системы категорирования и алгоритм ее работы, представлены результаты экспериментов, проведена оценка качества классификации по основным метрикам тэгов. Новизна предложенного подхода заключается в использовании статистики html-тэгов веб-страниц для улучшения категоризации сайтов, сходных по своему текстовому содержанию, но различающихся по структурным особенностям.

32. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных кибер-физических устройств // Труды СПИИРАН. 2016. Вып. 5(48). С.5-31.

С точки зрения информационной безопасности встроенные устройства представляют собой элементы сложных кибер-физических систем, работающих в потенциально враждебном окружении. Поэтому разработка таких устройств является сложной задачей, часто требующей экспертных решений. Сложность задачи разработки защищенных встроенных устройств обуславливается различными типами угроз и атак, которым может быть подвержено устройство, а также тем, что на практике вопросы безопасности встроенных устройств обычно рассматриваются на финальной стадии процесса разработки в виде добавления дополнительных функций защиты. В статье предлагается методика проектирования, применение которой будет способствовать разработке безопасных и энерго-эффективных кибер-физических и встроенных устройств. Данная методика организует поиск наилучших комбинаций компонентов защиты на основе решения оптимизационной задачи. Работоспособность предлагаемой методики демонстрируется на основе разработки прототипа защищенной системы охраны периметра помещения.

33. Новикова Е.С., Котенко И.В. Выявление аномальной активности в сервисах мобильных денежных переводов с помощью RADViz-визуализации // Труды СПИИРАН. 2016. Вып. 5(48). С.32-51.

В настоящее время широкое распространение получили сервисы мобильных денежных переводов (СМДП), в которых ключевая роль принадлежит оператору мобильной связи. В работе авторы предлагают новый подход к анализу транзакций для выявления аномальной активности в СМДП, в основе которого лежит RadViz-визуализация ее пользователей. Особенностями данной методики визуализации являются возможность разбиения пользователей на группы, имеющих одинаковое поведение, и низкая вычислительная сложность. В работе представляются и обсуждаются результаты применения разработанной методики визуального анализа транзакций для выявления различных сценариев финансовых мошенничеств, характерных для сервисов мобильных денежных переводов.

34. Проноза А.А., Чечулин А.А., Котенко И.В. Математические модели визуализации в SIEM-системах // Труды СПИИРАН. 2016. Вып. 3(46). С.90-107.

В статье предложены математические модели визуализации данных в SIEM-системах. Модели визуализации служат для формализации трех основных этапов процесса визуализации. На первом этапе предлагаются модели, с помощью которых происходит унификация сведений об объектах компьютерной сети, имеющих разнородные структуры и различные источники. На втором этапе, на базе построенных моделей формируется многомерная матрица связей. На третьем этапе предлагается унифицированный подход к визуализации различных аспектов безопасности компьютерной сети на основе построенной матрицы.

35. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2(45). С.207-244.

В работе рассматриваются различные методы обнаружения сетевых атак. Основное внимание уделяется построению обобщенной классификационной схемы методов обнаружения сетевых атак, представлению сущности каждого из рассмотренных методов и их сравнительному анализу в рамках предложенной классификационной схемы.

36. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В., Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. 2016. Вып. 4 (47). С. 5-27.

Статья посвящена анализу методов корреляции событий безопасности в системах управления информацией и событиями безопасности (SIEM-системах). Процесс корреляции событий безопасности рассматривается в виде многоуровневой иерархии этапов, цель каждого из которых заключается в выполнении определенных операций над обрабатываемыми данными безопасности. На основе результатов проведенного анализа в работе приводится описание каждого этапа процесса корреляции и схемы их взаимодействия.

37. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В., Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 // Труды СПИИРАН. 2016. Вып. 6(49). С.208-225.

Статья является продолжением описания исследований, посвященных анализу методов корреляции событий безопасности в системах управления информацией и событиями безопасности (SIEM-системах). В данной части рассматриваются методы непосредственной корреляции событий безопасности, применяемых на этапах, описанных в предыдущей статье. Приводится классификация рассматриваемых методов корреляции и результаты анализа их достоинств и недостатков, а также оценивается эффективность их применения на различных этапах процесса корреляции.

38. Новикова Е.С., Котенко И.В., Федотов Е.С. Визуальный анализ данных для обнаружения аномалий в сервисах мобильных денежных переводов // Защита информации. Инсайд, № 4, 2016. С.40-47; № 5, 2016. С.72-82.

Сервисы мобильных денежных переводов (СМДП) широко используются для совершения внутренних и международных денежных переводов. Как и традиционные финансовые системы они могут быть использованы для выполнения нелегальной финансовой деятельности, включая схемы по отмыванию денег, использованию вредоносного ПО для получения доступа к мобильным деньгам. В работе описывается новый подход к изучению транзакций СМДП и обнаружению аномалий в них на основе группы взаимосвязанных интерактивных моделей визуализации данных, которые позволяют всесторонне проанализировать поведение пользователей в системе. Авторы предложили метафорическое представление пользователей СМДП на основе модели визуализации RadViz, которое позволяет выявить группы пользователей со схожим поведением и пользователей, отличающихся от других своим поведением. Анализ изменений характеристик транзакций пользователей осуществляется при помощи тепловых карт. В работе предложен сценарий использования разработанной методики для выявления схем по отмыванию денежных средств и поведенческих мошенничеств, представлены результаты оценки эффективности разработанной методики визуального анализа транзакций СМДП.

39. Саенко И.Б., Котенко И.В. Основы построения перспективных систем мониторинга и управления безопасностью для защиты критически важных объектов информатизации // Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности». 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014. С.368-373.

В статье рассматриваются основы построения перспективных систем мониторинга и управления безопасностью для защиты критически важных объектов информатизации. Приводятся основные требования к таким системам. Рассматривается обобщенная архитектура такой системы и ее компонентов. Подробнее обсуждается порядок функционирования компонента анализа защищенности и моделирования атак.

40. Нестерук Ф.Г. Специфика двухуровневой организации адаптивных систем защиты информации // Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности». 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.С. 227-231.

В статье рассмотрены особенности организации двухуровневой организации адаптивных систем защиты информации на базе средств интеллектуального анализа данных, являющиеся базой построения многоуровневой системы адаптивной защиты. Рассмотрена специфика использования интеллектуального анализа данных при организации адаптивных уровней системы защиты информации.

41. Саенко И.Б., Кушнеревич А.Г., Котенко И.В. Реализация платформы распределенных параллельных вычислений для сбора и предварительной обработки больших данных мониторинга в кибер-физических системах // Международный конгресс по информатике: информационные системы и технологии (CSIST-2016). Материалы международного научного конгресса. Республика Беларусь, Минск, 24–27 октября 2016 г., 641-645.

В статье рассматриваются вопросы построения программной системы сбора и предварительной обработки больших массивов гетерогенных данных в кибер-физических системах. Система основана на платформе распределенных параллельных вычислений Hadoop и функционирующей на ее основе системе Spark. Реализация платформы позволяет реализовать потоковую обработку собираемых данных мониторинга на основе технологии Complex Event Processing и способствует преодолению ограничений при обработке Больших Данных. Экспериментальная оценка показала высокую производительность платформы.

42. Igor Saenko, Oleg Lauta, Igor Kotenko. Analytical modeling of mobile banking attacks based on a stochastic network conversion technique // The 2016 International Symposium on Mobile Internet Security (MobiSec'16). Taichung, Taiwan. July 14-15, 2016. 10 p.

Мобильные банковские атаки сильно возрастают в настоящее время. Это приносит большой экономический ущерб и требует повышения уровня мобильной безопасности. Для эффективной защиты от мобильных банковских атак необходимо разработка достоверных аналитических моделей, адекватно отображающих реальные процессы реализации атак в различных условиях. В статье представлен подход к аналитическому моделированию мобильных банковских атак, основанный на методе преобразования стохастической сети. Сущность данного метода заключается в замене множества элементарных ветвей стохастической сети одной эквивалентной ветвью и последующим определением эквивалентной функции сети, а также начальных моментов и функции распределения случайного времени реализации компьютерной атаки. Достоинствами предложенного метода являются высокая скорость моделирования, а также высокая достоверность и высокая чувствительность результатов к изменению исходных данных. Экспериментальная оценка предложенного метода подтвердила его высокую эффективность.

43. Куваев В.О., Саенко И.Б. Концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве // Проблемы экономики и управления в торговле и промышленности, № 7 (007), 2014. С. 101-104.

В статье излагаются концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве. Формулируются формализованные постановки задач, необходимые для эффективной интеграции информационных ресурсов.

44. Саенко И.Б., Куваев В.О., Алышев С.В. Подход к построению системы показателей качества единого информационного пространства // Естественные и математические науки в современном мире, 2014. № 14. С. 51-56.

В статье приводится описание системы показателей качества, предназначенной для оценки единого информационного пространства. Выделяются наиболее существенные характеристики и предлагаются показатели для их оценки.

45. Котенко И.В., Саенко И.Б. Предложения по реализации логического вывода для управления кибербезопасностью в АСУ железнодорожного транспорта // Естественные и математические науки в современном мире. 2014. № 14. Новосибирск: Изд. «СибАК», С. 46-50.

В статье приводится описание обобщенной архитектуры системы логического вывода для управления кибербезопасностью в АСУ железнодорожного транспорта. Приводится характеристика отдельных модулей данной системы и реализованных в ней механизмов логического вывода – исчисления событий и метода «проверки на модели». Обсуждаются входные данные и этапы алгоритма реализации метода «проверки на модели».

46. Котенко И.В., Саенко И.Б. Методика верификации политик безопасности в многоуровневой интеллектуальной системе обеспечения комплексной безопасности железнодорожного транспорта // Технические науки - от теории к практике. Новосибирск: Изд. «СибАК», 2014. № 30. С. 18-22.

В статье приводится описание методики верификации политик безопасности, применяемых в многоуровневой интеллектуальной системе обеспечения комплексной безопасности железнодорожного транспорта. Рассматриваются этапы методики, основанной на методе «проверки на модели». Обсуждаются вопросы построения модели компьютерной сети, модели аномалий и модели переходов, используемых в методике верификации.

47. Десницкий В.А., Чечулин А.А. Обобщенная модель нарушителя и верификации информационно-телекоммуникационных систем со встроенными устройствами // Технические науки - от теории к практике. Новосибирск: Изд. «СибАК», 2014. №38, С.7-21.

Сложность разработки и реализации требований к защите информационно-телекоммуникационных систем и встроенных устройств обуславливает необходимость построения моделей и методов проектирования и верификации механизмов защиты с учетом угроз информационной безопасности, целей и ресурсов возможных нарушителей, а также функциональных особенностей устройств. Предложены обобщенная модель нарушителя на основе анализа существующих классификаций нарушителей и верификация спецификаций в качестве метода тестирования защищенности устройств в процессе проектирования. Тестирование позволяет разработчику выявить потенциальные угрозы и осуществить отбор возможных типов нарушителей в зависимости от функциональности устройств и ожидаемых сценариев использования, после чего формируется список возможных атак на это устройство. Верификация включает анализ спецификаций на предмет проверки условий, необходимых для выполнения выявленных видов атак, в том числе проверку наличия определенных аппаратных компонентов и коммуникационных интерфейсов, которые могут использоваться в качестве стартовой точки для проведения атаки

48. Саенко И.Б., Куваев В.О. О применении методов искусственного интеллекта для разграничения доступа к ресурсам единого информационного пространства разнородных автоматизированных систем // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.631-637.

Рассматриваются основные подходы к применению методов искусственного интеллекта с целью разграничения доступа к ресурсам единого информационного пространства разнородных автоматизированных систем. Анализируется состояние исследований в данной предметной области. Выделяются четыре группы задач по реализации этих подходов, и дается их краткая характеристика.

49. Котенко И.В., Саенко И.Б. О задачах обеспечения кибербезопасности в инфраструктурах «электронного города» на основе методов искусственного интеллекта // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.618-622.

В работе рассматривается концепция «Электронный город», его особенности и основные задачи. А также выделяются основные проблемы, решение которых необходимо для обеспечения кибербезопасности его инфраструктур. Авторы рассматривают возможные подходы к решению этих проблем и обсуждают отдельные результаты, полученные в ходе их решения.

50. Десницкий В.А. Верификация сетевых информационных потоков систем со встроенными устройствами на основе экспертных знаний // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.596-600.

Ограничения на системные ресурсы встроенных устройств определяют сложность применения существующих методов и алгоритмов, используемых традиционно для защиты персональных компьютеров и серверных станций. В результате разработка защищенных встроенных устройств требует специализированных подходов к проектированию механизмов защиты, которые могли бы обеспечить стойкость системы к атакам не только за счет дополнительных средств защиты, но и за счет особенностей архитектуры системы. Верификация информационной системы со встроенными устройствами на всех этапах проектирования, как один из путей достижения этой цели, позволяет избежать архитектурных ошибок, которые, в свою очередь, снижают уровень защищенности всей системы. В работе предложена методика верификации информационных потоков, которая построенная на основе экспертных знаний об известных видах аномалий сетевых информационных потоков. Методика нацелена на проведение оценки защищенности разрабатываемой информационной системы со встроенными устройствами, проверки корректности политики безопасности этой системы и определение уровня соответствия информационных потоков в реальной системе заданным политикам.

51. Агеев С.А., Саенко И.Б. Управление рисками информационной безопасности защищенной мультисервисной сети специального назначения на основе интеллектуальных мультиагентов // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.556-562.

Рассматриваются основные подходы построения интеллектуальных методов и алгоритмов, синтезированных на их основе, оценки и управления рисками информационной безопасности защищенных мультисервисных сетей (ЗМС). Показана необходимость применения интеллектуальных методов управления ЗМС СН. Разработана и исследована математическая модель оценки риска информационной безопасности ЗМС СН.

52. Саенко И.Б., Куваев В.О., Бирюков М.А. Использование онтологий для управления разграничением доступа к разнородным ресурсам единого информационно-коммуникационного пространства // Технические науки – от теории к практике, 2015, № 11 (47), С. 76-80.

Приводится описание онтологического подхода для управления разграничением доступа к разнородным ресурсам в едином информационно-коммуникационном пространстве. Выделяются преимущества решения поставленной проблемы с использованием онтологической модели. Предлагается архитектура построения системы управления разграничением доступа с использованием онтологии.

53. Саенко И.Б., Куваев В.О., Бирюков М.А. Общая архитектура единой системы разграничения доступа к разнородным ресурсам в едином информационно-коммуникационном пространстве // Технические науки – от теории к практике, 2015, № 11 (47), С. 70-75.

В статье предлагается общая архитектура единой системы разграничения доступа к разнородным ресурсам в едином информационно-коммуникационном пространстве. Дается формальное описание условий построения единой системы разграничения доступа. Рассматриваются задачи, решаемые отдельными компонентами предлагаемой архитектуры.

54. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №47, 2015, С.14-18.

В работе предложена методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами. Методика базируется на определениях и методологическом аппарате, предложенным в рамках методологии моделирования встроенных устройств и систем реального времени MARTE. MARTE задает следующие наиболее важные виды аппаратных ресурсов, которые учитываются в процессе комбинирования системы: вычислительные ресурсы, коммуникационные ресурсы, ресурсы хранения и энергоресурсы. Каждый ресурс характеризуется численным показателем ресурсопотребления – нефункциональным ресурсным свойством, определяющим величину его расхода в процессе функционирования устройства.

55. Десницкий В.А., Дойникова Е.В. Архитектура и оценка эффективности программного средства конфигурирования компонентов защиты систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №47, 2015, С.9-13.

В работе исследуется программный прототип средства компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами на основе оптимизационного подхода к выбору комбинаций компонентов защиты (конфигурирование). Прототип реализует функцию конфигурирования, которая по установленным функциональным требованиям и нефункциональным ограничениям, а также перечню заданных альтернатив компонентов защиты определяет на выходе наиболее эффективную (оптимальную) конфигурацию защиты. Прототип содержит функцию проверки эффективности заданной конфигурации защиты в соответствии с заданным критерием. Целью работы является разработка архитектуры для программной реализации средства конфигурирования компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами. Предложенная архитектура базируется на использовании средств языка моделирования UML, принципах объектно-ориентированного программирования и теории принятия решений. Произведена оценка эффективности разработанного средства путем сравнения результатов конфигурирования с альтернативными путями комбинирования компонентов защиты.

56. Левшун Д.С., Чечулин А.А. Постановка задачи построения единого хранилища мультимедийных данных из полевых этнографических экспедиций // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №46, 2015, С. 25-30.

Данная работа посвящена исследованию существующих решений для построения единого хранилища мультимедийных данных из полевых этнографических экспедиций. Объектом исследования являются как специализированные системы, так и системы управления содержимым. В статье рассматриваются достоинства и недостатки существующих решений, выделяются требования к построению единого хранилища мультимедийных данных из полевых этнографических экспедиций.

57. Саенко И.Б., Бирюков М.А. Методика интеграции локальных схем разграничения доступа к разнородным ресурсам единого информационного пространства // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.758-762.

Предложена методика интеграции локальных схем разграничения доступа к разнородным ресурсам единого информационного пространства, основанная на применении онтологий. Описана структура онтологии для разграничения доступа. Обоснована проблема интеграции локальных схем разграничения доступа в едином информационном пространстве. Представлена архитектура единой системы разграничения доступа единого информационного пространства. Рассмотрены модель и метод использования онтологий для управления разграничением доступа к разнородным ресурсам единого информационного пространства. Раскрыто содержание этапов разработанной методики.

58. Десницкий В.А. Выявление аномальных данных от сенсоров встроенных устройств на основе экспертных знаний // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.676-679.

В работе исследуются экспертные знания в области информационно-телекоммуникационных систем для выявления аномальных данных от сенсоров встроенных устройств в результате атакующих воздействий на компоненты устройства. К таким атакам относятся физическое воздействие на сенсор, атака подмены сенсора, воздействия на коммуникационные интерфейсы устройства, подмена данных на устройстве с использованием злонамеренного программного обеспечения и др. Предложен подход к выявлению аномальных данных путем проверки ограничений на значения данных в соответствии с паттернами, задаваемыми для каждого из устройств системы. Реализован прототип системы «Умный дом» с использованием Raspberry Pi, реализующий предложенный подход и проведена его экспериментальная оценка. Проведены эксперименты и проанализированы их результаты. В качестве будущих исследований по данному направлению планируется построение комплексной среды тестирования готовых встроенных устройств на основе выявления конкретных знаний для разработки наборов тестов с учетом специфики систем Интернета вещей на некорректных, неполных и неожиданных входных данных, а также разработка системы правил для выявления таких атак в рамках компонента мониторинга.

59. Десницкий В.А. Реализация средства верификации сетевых информационных потоков с использованием метода «проверки на модели» // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.680-683.

В работе реализован подход к верификации информационных потоков в части проверки корректности политики контроля сетевых информационных потоков в информационно-телекоммуникационных системах со встроенными устройствами. Подход базируется на применении метода «проверки на модели» путем последовательного перебора правил разрешения и запрета информационных потоков в системе в порядке уменьшения их приоритета до факта первого срабатывания. Воспроизведение в динамике процесса контроля политики на модели некоторой системы позволяет выявлять аномальные правила политики, которые могу приводить к некорректной работе целевой системы. Программный прототип средств верификации

реализован на языке Promela и использован для обоснования практической действенности и применимости предложенного подхода на практике.

60. Дойникова Е.В., Котенко И.В. Методика оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016.

В работе описывается методика оценки защищенности компьютерных сетей. Методика основана на комплексе показателей защищенности, вычисляемых на основе графов атак и графов зависимостей сервисов. Основным отличием методики является ее многоуровневая структура, объединяющая несколько уровней оценки и позволяющая оценить защищенность на каждом уровне в зависимости от имеющихся входных данных. Оценка защищенности основана на определении рисков компрометации компьютерной сети. В состав методики традиционно входит идентификация источников риска, анализ риска и сравнительная оценка риска. Для идентификации риска применяется модельно-методический аппарат, включающий представление входных данных в виде моделей сети (граф зависимости сервисов), атак (граф атак), атакующего, событий и контрмер, и ряд стандартов унифицированного представления данных по безопасности. На этапе анализа риска применяется комплекс показателей защищенности на основе графов атак и графов зависимостей сервисов и алгоритмы вычисления данных показателей. В том числе логический вывод на основе графа зависимостей сервисов и матричные вычисления для определения критичности активов сети, Байесовский вывод для определения вероятности компрометации ресурсов сети и влияния событий на развитие атаки. Вычисляемые показатели определяются в зависимости от доступных входных данных. Сравнительная оценка результатов проводится путем сопоставления полученных количественных оценок риска качественной шкале. В докладе показано применение методики для оценки защищенности различных сетей и разных наборов входных данных.

61. Новожилов Д.А., Чечулин А.А. Разработка стенда для проведения экспериментов с методами классификации веб-сайтов // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.740-749.

Методы классификации занимают важное место в интеллектуальном анализе данных (Data Mining). Будучи примененными к веб-сайтам, они позволяют повысить защищенность Интернет-пользователей от нежелательной информации. Данная проблема включает в себя два основных направления: ограждение несовершеннолетних от нежелательной информации и блокировку контента, нарушающего законодательство. Сложность проводимых в настоящее время исследований, их трудоемкость и значительные временные затраты потребовали создания специального стенда для проведения экспериментов, отличительной чертой которого является полная автоматизация процесса на всех его стадиях. В статье приводится обзор существующих решений, архитектура предлагаемой системы, раскрываются детали ее реализации, а также описываются эксперименты, демонстрирующие работу стенда.

62. Чечулин А.А. Алгоритмы построения и модификации моделей атак для анализа защищенности компьютерных сетей // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.782-785.

В работе рассматриваются алгоритмы построения и модификации моделей атак для оценки защищенности компьютерных сетей. Для повышения скорости работы алгоритмов предлагается разбить общую последовательность действий, выполнение которых необходимо в зависимости от анализируемой компьютерной сети, изменений, происходящих в этой сети, и типов возможных нарушителей.

63. Браницкий А.А., Котенко И.В. Методики комбинирования бинарных классификаторов для выявления аномальных сетевых соединений // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.660-664.

Рассматриваются несколько приемов гибридизации методов вычислительного интеллекта применительно к задаче обнаружения сетевых атак.

64. Браницкий А.А. Модифицированная модель вычислительной иммунной системы на базе эволюционно-генетического подхода для обнаружения и классификации аномальных сетевых соединений // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.656-659.

Описывается новая модель искусственной иммунной системы, построенной на основе эволюционного подхода с применением усовершенствованного конкурентного обучения.

65. Саенко И.Б., Куваев В.О. Модель и методика оценки и обеспечения оперативной доступности к ресурсам единого информационного пространства // Математические методы в технике и технологиях – ММТТ-29 [текст]: сб. трудов XXIX Междунар. науч. конф.: в 12 т. Т.6. / под общ. ред. А.А. Большакова. – Саратов: Саратов. гос. техн. ун-т; Санкт-Петербург: СПбГТИ(ТУ), СПбПУ, СПИИРАН; Самара: Самарск. гос. техн. ун-т, 2016. – С.139–142.

Рассматриваются аналитические модели оценки и обеспечения оперативной доступности ресурсов к единому информационному пространству. Приводятся постановки задач оптимизации для различных

режимов функционирования системы. Обсуждаются методики решения этих задач на основе применения генетических алгоритмов.

66. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа к разнородным ресурсам единого информационного пространства // Математические методы в технике и технологиях – ММТТ-29 [текст]: сб. трудов XXIX Междунар. науч. конф.: в 12 т. Т.6. / под общ. ред. А.А. Большакова. – Саратов: Саратов. гос. техн. ун-т; Санкт-Петербург: СПбГТИ(ТУ), СПбПУ, СПИИРАН; Самара: Самарск. гос. техн. ун-т, 2016. – С.122-125.

Предложен подход к управлению разграничением доступа в едином информационном пространстве, основанный на использовании онтологий. Описана структура онтологии для разграничения доступа. Рассмотрены модель и метод использования онтологий для управления разграничением доступа к разнородным ресурсам единого информационного пространства.

67. Дойникова Е.В., Федорченко А.В. Методики автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов // XXIX Международная научная конференция "Математические методы в технике и технологиях - ММТТ-29", 31 мая - 3 июня 2016 года, Санкт-Петербургский государственный технологический институт, Санкт-Петербург, Россия.

Рассмотрены и классифицированы существующие подходы к автоматизированному реагированию на атаки. Выявлены недостатки существующих подходов. Предложен подход к автоматизированному реагированию на инциденты на основе графов атак и открытых стандартов по представлению информации по безопасности.

68. Котенко И.В., Саенко И.Б. Генетические алгоритмы для булевой матричной факторизации применительно к задачам разграничения доступа в компьютерных сетях // Пятнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (3-7 октября 2016 года, г. Смоленск, Россия): Труды конференции. Т.3. Смоленск: Универсум, 2016. С.98-106.

В работе описываются постановки задач разграничения доступа в компьютерных сетях, которые являются задачами булевой матричной факторизации. Приводится описание ключевых вопросов по разработке генетических алгоритмов для решения этих задач. Обсуждаются результаты экспериментальной оценки разработанных алгоритмов.

69. Коломеец М.В., Котенко И.В., Чечулин А.А. Модель визуализации для интеллектуальной системы мониторинга кибербезопасности, базирующаяся на аналоге диаграмм Вороного // Пятнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (3-7 октября 2016 года, г. Смоленск, Россия): Труды конференции. Т.3. Смоленск: Универсум, 2016. С.180-187.

В работе предлагается подход к разработке компонента визуализации, используемого в интеллектуальной системе мониторинга кибербезопасности. Предлагается концептуально новая графическая модель визуализации, подобная диаграмме Вороного. Работа содержит описание новой графической модели и примеры ее применения наряду с традиционными графовыми и другими моделями. Приведена оценка предлагаемой графической модели.

70. Куваев В.О., Саенко И.Б. Подход к решению задачи разграничения доступа в разнородном информационном пространстве // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.33-34.

В современных исследованиях концепция «единого информационного пространства» (ЕИП) рассматривается как направление, определяющее дальнейшее развитие информационного обеспечения в целях создания сетеориентированных гетерогенных информационных систем коллективного пользования. Гетерогенность означает, что данные ресурсы ЕИП являются разнородными по содержанию и форматам представления и, кроме того, они могут отличаться по критериям и методам обеспечения безопасности. В результате разграничение доступа в разнородном информационном пространстве становится достаточно сложной задачей. Для ее решения предлагается подход, основанный на двухэтапном моделировании системы разграничения доступа к ресурсам ЕИП. На первом этапе формируется концептуальная модель системы разграничения доступа в ЕИП, в которой отражаются основные понятия данной предметной области и отношения между ними. Концептуальная модель обеспечивает понятийный базис системы управления доступа. На втором этапе модель насыщается формальной семантикой за счет использования онтологического представления правил разграничения доступа в ЕИП.

71. Котенко И.В., Новикова Е.С. Модели и методики визуального анализа данных для решения задач компьютерной безопасности // Шестнадцатая Международная конференция «РусКрипто-2014». Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/

Анализируются различные модели и методики визуального анализа, разработанные для мониторинга сетевого трафика, анализа таблиц маршрутизации, оценки политик безопасности и уровня защищенности компьютерных сетей. Формулируются основные требования к подсистеме визуального анализа как составной части автоматизированных систем мониторинга и управления информационной безопасностью,

предлагается общий подход к ее проектированию. Демонстрируются возможности разработанной системы визуального анализа для моделирования атак и оценки уровня защищенности.

72. Котенко И.В., Саенко И.Б. О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта // Интеллектуальные системы на транспорте: Материалы IV международной научно-практической конференции «ИнтеллектТранс-2014». – СПб.: ПГУПС, 2014. С.196-203.

В статье предлагается в основу построения многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем (АС) ЖТ положить технологию мониторинга и управления информационной безопасностью. Рассматриваются архитектура такой системы, исходные данные, методы и алгоритмы функционирования системных компонентов.

73. Котенко И.В., Новикова Е.С. Визуальная аналитика на страже информационной безопасности // Международный форум по практической безопасности Positive Hack Days. Москва. 21-22 мая 2014 г. http://www.phdays.ru

Методы визуальной аналитики позволяют значительно повысить эффективность администратора безопасности, так как они сочетают мощность интеллектуальных методов обработки данных и особенности зрительного восприятия информации человеком. В докладе рассматриваются существующие методы визуального анализа данных для решения различных задач защиты от компьютерных атак. Эффективность применения визуального анализа демонстрируется на примере работы разработанных авторами средств визуальной аналитики, в том числе для анализа трафика, моделирования атак, оценки защищенности, обнаружения финансовых нарушений в системе мобильных денежных переводов и др.

74. Котенко И.В., Саенко И.Б. Об архитектуре многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.97-98.

В настоящее время на первое место в противодействии новым угрозам безопасности на железнодорожном транспорте (ЖТ) выдвигаются не разработка новых механизмов защиты информации, а эффективное и комплексное применение этих механизмов. Решение данной задачи предполагается возможным на основе создания и применения многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем (АС) ЖТ. В основу построения такой системы предлагается положить технологию «управления информацией и событиями безопасности» (Security Information and Event Management, SIEM). В архитектуре предлагаемой многоуровневой интеллектуальной системы обеспечения информационной безопасности АС ЖТ выделяются три уровня: 1) уровень традиционных средств защиты (нижний); 2) уровень интеллектуальных сервисов сбора, предварительной обработки и хранения данных (средний); 3) уровень интеллектуальных сервисов анализа данных (высший).

75. Агеев С.А., Саенко И.Б. Интеллектуальные методы управления рисками информационной безопасности мультисервисных сетей связи // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.59-60.

Важнейшей проблемой при использовании защищенной мультисервисной сети (ЗМС) является проблема обеспечения ее безопасного функционирования и безопасности циркулирующей в ней информации. В докладе показывается, что оперативное оптимальное управление затрудняется вследствие больших размерностей совокупности решаемых задач по управлению ЗМС. Обосновывается, что многообразие, разнородность, неполнота и нечеткость исходных данных, учитываемых в задачах управления ЗМС, включая управление безопасностью, предопределяют необходимость использовать средства и методы искусственного интеллекта для выработки рациональных (оптимальных) управленческих решений. Для решения проблемы управления безопасностью ЗМС управление рисками ЗМС и процедуры их оценки предлагается строить на основе технологии интеллектуальных мультиагентов (ИМА), основой которых является технология «агент-менеджер». Один агент отвечает за часть задания, а общее решение возникает в результате их совместного выполнения. Программное средство «менеджер/агент» управляет действиями функциональной группой агентов и может передавать агрегированную информацию на верхний уровень иерархии, которую обрабатывает программное средство «менеджер».

76. Котенко И.В., Саенко И.Б. Система логического вывода и верификации политик безопасности в автоматизированных системах железнодорожного транспорта // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT-14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.2. С.271-276.

В работе рассматривается архитектура системы логического вывода и верификации политик безопасности в автоматизированных системах железнодорожного транспорта. Обсуждаются вопросы построения модулей верификации политик безопасности, основанные на Model checking и исчислении событий, а также онтологического хранилища данных. Раскрываются аспекты реализации компонентов системы, сущность методов верификации и вопросы тестирования онтологического хранилища.

77. Саенко И.Б., Котенко И.В. Генетический подход к проектированию виртуальных компьютерных сетей на основе генетических алгоритмов // Труды Конгресса по интеллектуальным

системам и информационным технологиям «IS&IT-14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.1. С.35-40.

В работе представлен новый подход к проектированию виртуальных компьютерных сетей, который принимает во внимание заданную матрицу логической связности компьютеров. Показано, что задача относится к классу булевой матричной факторизации. Для ее решения предлагается усовершенствованный генетический алгоритм. Основные новшества алгоритма связаны с использованием тривиальных решений для создания начальной популяции, учетом критерия минимального количества виртуальных подсетей в функции полезности и использованием столбцов матрицы связности в качестве генов хромосом.

78. Котенко И.В., Саенко И.Б. Интеллектуальная система мониторинга и управления инцидентами кибербезопасности // Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 (24–27 сентября 2014 года, г. Казань, Россия): Труды конференции. Т.3. Казань: Изд-во РИЦ «Школа», 2014. С.219-227.

В работе представлена формальная система интеллектуальных методов мониторинга и управления инцидентами кибербезопасности, позволяющая обосновать состав и содержание данных методов. Приведено формальное описание методов, используемых на начальных этапах мониторинга кибербезопасности, и дан пример их реализации.

79. Дойникова Е.В., Котенко И.В. Оценивание защищенности в автоматизированных системах управления РЖД // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.132-133.

Предлагается подход, основанный на отражении текущего уровня защищенности системы в виде набора показателей защищенности. При разработке подхода к оцениванию защищенности учитывались следующие требования, основанные на общих требованиях к системам оценивания защищенности и особенностях промышленных систем: показатели должны быть значимыми, объективными и повторяемыми; показатели должны указывать на уязвимые места системы; показатели должны определять вероятность успешной атаки и ее возможные последствия; показатели должны определять профиль нарушителя, его цели, местоположение в системе и возможности; показатели должны учитывать текущую ситуацию на основе событий, поступающих от системы управления информацией и событиями безопасности; подход к оцениванию защищенности должен помогать принимать эффективные решения по безопасности; подход должен учитывать требования действующих стандартов и протоколов безопасности; алгоритмы вычисления показателей должны быть эффективными (вычисление должно производиться во времени, близком к реальному, что особенно важно для промышленных систем) и отражать реальное состояние защищенности информационной системы.

80. Дойникова Е.В. Поддержка принятия решений по выбору защитных мер в информационных системах на основе комплекса показателей защищенности // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.132.

В рамках работы предлагается проактивный подход к выбору защитных мер, основанный на системе показателей защищенности. Подход позволяет учитывать информацию о событиях безопасности, обнаруженных в системе, и на основе спрогнозированного профиля атаки выбрать из списка защитных мер наиболее эффективные меры ее предотвращения. Данный подход является расширением предыдущей работы по анализу защищенности, в рамках которой был предложен подход к оцениванию защищенности на основе многоуровневой системы показателей. В систему показателей защищенности добавляется новый уровень принятия решений, содержащий различные показатели оценки эффективности защитных мер.

81. Агеев С.А., Саенко И.Б. Оценка и управление рисками информационной безопасности в защищенных мультисервисных сетях на основе методов искусственного интеллекта // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.116-117.

Важнейшей проблемой при создании и эксплуатации защищенных мультисервисных сетей (ЗМС) является проблема обеспечения их безопасного функционирования и безопасности циркулирующей в них информации. Одной из основных проблем управления безопасностью ЗМС является задача оценки и управления рисками информационной безопасности (ИБ). Оценивание риска является итерационным процессом, который заключается в оценке величины рисков, выработке мер по их уменьшению и убеждении, что риски допустимы. На начальном этапе методом экспертной оценки решаются общие вопросы проведения оценивания риска. Вначале производится синтез модели угроз ИБ ЗМС. Далее выбираются компоненты ЗМС и степень детальности их рассмотрения. Выбираются методологии оценки рисков как процесса получения количественной или качественной оценки ущерба, который может произойти в случае реализации угроз безопасности ЗМС.

82. Котенко И.В., Саенко И.Б. Поддержка принятия решений по безопасности информации в АСУ железнодорожного транспорта на основе онтологического моделирования данных // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.144.

В работе описывается одно из направлений решения проблемы обеспечения безопасности информации (БИ) в АСУ железнодорожного транспорта, которое заключается в создание развитой системы управления и

мониторинга комплексной безопасностью ЖТ, в частности, на концепции«управления информацией и событиями безопасности» (Security Information and Event Management). Одной из важнейших задач, решаемых в такой системе, является поддержка принятия решений на основе анализа данных о событиях безопасности, в ходе которого проводится оценке метрик защищенности, оценка издержек, связанных с реализацией возможных контрмер и выбор наиболее приемлемых решений по обеспечению информационной безопасности. Предлагается для этой цели использовать онтологическое моделирование данных, заключающееся в построении и использовании онтологии.

83. Котенко И.В., Саенко И.Б. Модели и методы визуального анализа больших объемов данных и событий безопасности автоматизированных систем железнодорожного транспорта // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.143.

В работе рассматривается одно из направлений решения проблемы обеспечения безопасности информации (БИ) в АСУ железнодорожного транспорта, которое заключается в создание развитой системы управления и мониторинга комплексной безопасностью ЖТ, в частности, на концепции «управления информацией и событиями безопасности» (Security Information and Event Management). Одной из важнейших задач, решаемых в такой системе, является поддержка принятия решений на основе анализа данных о событиях безопасности, в ходе которого проводится оценке метрик защищенности, оценка издержек, связанных с реализацией возможных контрмер и выбор наиболее приемлемых решений по обеспечению информационной безопасности. Предлагается для этой цели использовать онтологическое моделирование данных, заключающееся в построении и использовании онтологии.

84. Котенко И.В., Саенко И.В., Чечулин А.А. Проактивное управление информацией и событиями безопасности в сетях NGN // Материалы семинара Международного союза электросвязи «Переход развивающихся стран с существующих сетей на сети нового поколения (NGN): технические, экономические, законодательные и политические аспекты», Санкт- Петербург, СПб ГУТ им Бонч-Бруевича. 23–25 июня 2014 года.

Рассмотрены особенности сетей NGN как объектов мониторинга и управления безопасностью. Приведена общая архитектура системы проактивного управления информацией и событиями безопасности. Обсуждались вопросы построения и функционирования основных компонентов системы, к числу которых относятся репозиторий данных о событиях безопасности, компонента анализа защищенности и компонент визуализации.

85. Котенко И.В., Саенко И.Б. Генетический подход к проектированию виртуальной частной сети в защищенном информационном пространстве // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С.320-325.

Технология виртуальных частных сетей является практически единственным средством, позволяющим осуществлять защищенный обмен данными через открытые сети в рамках защищенного информационного пространства. В работе представлен подход к проектированию виртуальных частных сетей, основанный на использовании генетического алгоритма оптимизации. Существенной особенностью предлагаемого генетического подхода является то, что функция пригодности формируется на основе аналитических выражений, позволяющих оценить свойства пропускной способности, устойчивости и стоимости для каждого возможного решения задачи. Для расчета показателей пропускной способности и устойчивости использованы положения теории массового обслуживания. Для различных вариантов функционирования виртуальной частной сети приведена оценка предлагаемого подхода, показавшая его высокую эффективность.

86. Десницкий В.А. Модели процесса разработки комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С. 113-118.

В работе предложены модели для проектирования, верификации и тестирования комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами на основе знаний о существующих системах и компонентах защиты. Модели предназначены для разработки на их основе автоматизированных методик и программных средств, используемых в процессе проектирования, верификации и тестирования компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами. Под встроенным устройством понимается набор взаимосвязанных программно-аппаратных и программных модулей, процесс выполнения непосредственно связан с реакцией на различные процессы физического окружения. Примерами таких устройств являются устройства считывания текстовой, звуковой и другой информации с различных носителей, устройствами отображения, разнообразными коммуникационными устройствами, бытовыми и промышленными устройствами нагревания, вентиляции, устройствами мониторинга и диагностики, насосными станциями, системами поддержки навигации и другими. Цель работы – выявление экспертных знаний в области проектирования, верификации и тестирования систем со встроенными устройствами и разработка на их основе специализированных моделей, которые направлены на повышение защищенности целевых систем и автоматизацию процесса разработки таких систем.

87. 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.

88. Саенко И.Б., Котенко И.В. Адаптивное изменение политик и схем разграничения доступа к ресурсам единого информационного пространства // 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.127-128.

Рассматривается задача своевременной адекватной корректировки (реконфигурации) политик и схем разграничения доступа к ресурсам единого информационного пространства. Сформированы формальные постановки задач для двух сценариев ролевой модели доступа и схемы организации виртуальной локальной вычислительной сети. Обсуждаются программные прототипы для решения поставленных задач методом генетических алгоритмов и результаты их экспериментальной оценки.

89. Агеев С.А., Васильев Д.В., Саенко И.Б. Управление безопасностью защищенной мультисервисной сети специального назначения // 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.106-107.

Работа посвящена методам управления безопасностью 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.

90. 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.

Рассматривается комплекс решений по созданию систем управления информацией и событиями безопасности нового поколения, который обеспечивает реализацию ряда новых функциональных возможностей. Обсуждаются особенности построения отдельных компонентов данной системы. Показано, что новые компоненты в совокупности реализуют более высокий уровень защищенности от несанкционированного доступа и вредоносных воздействий (атак).

91. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // 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.69-70.

Цель работы – построение методики оценки ресурсопотребления компонентов защиты систем со встроенными устройствами. Методика используется в процессе конфигурирования встроенных устройств для нахождения наиболее эффективных конфигураций защиты. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем базируется на определениях и методологическом аппарате MARTE, разработанном в рамках международной рабочей группой OMG в области объектно-ориентированных технологий и стандартов. MARTE определяет в частности, следующие наиболее важные виды системных ресурсов: вычислительные ресурсы, коммуникационные ресурсы, ресурсы хранения и энергоресурсы с определенным численным нефункциональным показателем ресурсопотребления, который определяет величину расхода заданного ресурса в процессе работы встроенного устройства. В качестве примера можно привести следующие показатели «объем оперативной памяти устройства» и «объем передаваемых данных». Для определения значений этих показателей используется понятие так называемого «сценария наихудшего выполнения». При этом выборка и максимизация расхода ресурса осуществляется путем программного моделирования функций компонента защиты на физических реализациях встроенных устройств. Ограничения на ресурсные показатели встроенного устройства задают на основе данных, полученных из формальных спецификаций и значений, заданных производителем конкретного программно-аппаратного компонента.

92. 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.

93. 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.

94. 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.

95. Чечулин А.А., Проноза А.А. Классификация и анализ типов связей в компьютерных сетях для их последующей визуализации // 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.132-133.

В работе приведено описание непротиворечивой и достаточной системы знаний, описывающей все необходимые для построения визуального представления текущего состояния защищенности компьютерной сети. При визуализации компьютерной сети в большинстве случаев необходимо отображать узлы данной сети – рабочие станции, сервера, коммутационное оборудование и т.п. При этом хосты, входящие в состав этой сети отображаются при помощи различных пиктограмм, изображающих тип сетевого объекта.

96. 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.

97. 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.

98. Левшун Д.С., Чечулин А.А., Коломеец М.В., Котенко И.В. Архитектура системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 76.

Данная работа посвящена разработке архитектуры системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт. В статье рассматриваются основные функциональные требования к системам такого типа, на основе которых формируются альтернативные компонентные составы встроенных устройств. Также, на основе нефункциональных требований к системам такого типа был выбран оптимальный компонентный состав, который стал основой системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт.

99. Браницкий А.А. Методы вычислительного интеллекта для обнаружения и классификации аномалий в сетевом трафике // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 61-62.

В работе рассматривается задача обнаружения и классификации сетевых атак с применением методов вычислительного интеллекта и различных способов их комбинирования.

100. 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.

101. 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.

102. Новожилов Д.А., Чечулин А.А. Разработка программных средств поддержки проведения экспериментов по классификации веб-сайтов // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 80-81.

В публикации рассматривается архитектура системы проведения экспериментов по классификации веб-сайтов в виде набора программных модулей с четко определенными входами и выходами, последовательная работа которых и будет обеспечивать весь процесс подготовки экспериментов.

103. 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.

104. 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/

Описана архитектура распределенной системы предназначенной для корреляции событий безопасности от встроенных устройств, представляющих собой элементы сети «Интернет вещей».

105. Саенко И.Б., Котенко И.В., Круглов С.Н. Генетический подход к реконфигурированию схем ролевого доступа в едином информационном пространстве // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'16, 2016, Том 1. С.13-18.

Ролевая схема доступа широко распространена в автоматизированных системах, объединенных в единое информационное пространство. В работе формулируется постановка задачи реконфигурирования ролевой схемы доступа. Предлагается использовать генетический алгоритм для решения этой задачи. Новизна разработанного генетического алгоритма заключается в скрещивании особей, имеющих не одну, а две хромосомы, и учете в функции пригодности критерия минимальных затрат на изменение схемы доступа. Результаты экспериментов показывают достаточно высокую эффективность предлагаемого алгоритма.

106. Саенко И.Б., Котенко И.В., Круглов С.Н. Поход к решению «проблемы извлечения ролей» при формировании модели RBAC на основе генетических алгоритмов // Материалы 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 4 июля - 7 июля 2016 г. Санкт-Петербург. Издательство Политехнического университета. 2016. С.113.

Целью настоящей работы является разработка универсального подхода к решению «проблемы извлечения ролей» при формировании модели RBAC. Данный подход основан на применении генетических алгоритмов. Разработанные генетические алгоритмы имеют ряд отличительных особенностей, которые касаются следующих аспектов: формирования хромосом для кодирования решений; формирования начальной популяции особей; формирования функции пригодности; разработки операторов скрещивания и мутации.

107. Саенко И.Б., Котенко И.В. Модели и методы визуального анализа схем и политик разграничения доступа к ресурсам единого информационного пространства // XV Санкт-Петербургская Международная Конференция "Региональная информатика-2016" ("РИ-2016"). Материалы конференции. СПб., 2016. С. 192-193.

Одной из составляющих проблемы построения системы разграничения доступа к ресурсам единого информационного пространства является необходимость разработки моделей и методов их анализа, в

частности, их визуального анализа. Специфика данных моделей и методов обусловлена тем, что визуальный анализ позволяет значительно быстрее обнаружить конфликты или противоречия в политиках безопасности, чем формальные модели и методы, за счет использования возможностей человека по обработке информации, воспринимаемой зрительным путем. К разработанным моделям и методам визуализации предъявлялись следующие требования: 1) возможность кластеризации больших массивов данных; 2) возможность автоматической классификации массивов данных; 3) возможность «ленивой» загрузки массивов данных при визуализации; 4) возможность детализации кластеризованных данных (Drill-down); 5) возможность микширования данных (mesh-up) при их визуализации. Модели и методы были реализованы следующими способами: 1) визуализация с использованием GIS-систем; 2) инфографика; 3) табличные способы; 4) иерархические способы. Экспериментальная оценка предложенных моделей и методов визуализации показала их достаточно высокую эффективность.

108. Саенко И.Б., Агеев С.А., Чечулин А.А. Поддержка принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи. Свидетельство № 2014660775. Зарегистрировано в Реестре программ для ЭВМ 15.10.2014.

Приводится листинг и краткое описание работы программного средства поддержки принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи.

109. 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.

Приводится листинг и краткое описание работы программно-инструментального стенда визуализации и оценки качества проектирования виртуальных компьютерных сетей, предназначенный для поддержки принятия решений при мониторинге и управлении информационной безопасностью.

110. Саенко И.Б., Чечулин А.А., Куваев В.О., Барыкин Н.А. Программное средство оценки оперативности доступа к ресурсам единого информационно-коммуникационного пространства. Свидетельство № 2015662574. Зарегистрировано в Реестре программ для ЭВМ 16.11.2015.

Приводится листинг и краткое описание работы программного средства оценки оперативности доступа к ресурсам единого информационно-коммуникационного пространства.

111. Саенко И.Б., Котенко И.В., Авраменко В.С., Бобрешов-Шишов Д.И. Программное средство оценки защищенности информации от угроз несанкционированного доступа в автоматизированных системах на основе экспертных оценок. Свидетельство № 2016614484. Зарегистрировано в Реестре программ для ЭВМ 25.04.2016.

Приводится листинг и краткое описание работы программного средства оценки защищенности информации от угроз несанкционированного доступа в автоматизированных системах на основе экспертных оценок.