Форма 503. РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер проекта

15-07-07451

3.2. Объявленные ранее цели Проекта на 2016 год

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

3.3. Коды классификатора, соответствующие содержанию фактически проделанной работы

07-298, 07-205, 08-608

3.4. Объявленные ранее цели Проекта на 2016 год

Общей целью данного проекта является повышение защищенности информационно-телекоммуникационных систем. Для достижения этой цели в проекте решается общая задача по разработке алгоритмов построения, модификации и анализа моделей атак, позволяющих получить результат за заданное время, и способствуют достижению цели Проекта.

В 2016 году планировалось решение следующих задач:

1) разработка усовершенствованного алгоритма построения моделей атак, позволяющего формировать модели атак для нескольких нарушителей, без значительного увеличения ресурсоемкости по сравнению с построением модели атак для одного нарушителя;

2) разработка алгоритма модификации модели атак, позволяющего оперативно приводить модели компьютерной сети и атак в соответствие с измененной реальной сетью, за счет целевой модификации только тех элементов моделей, которые соответствуют измененным элементам компьютерной сети;

3) разработка алгоритма анализа моделей атак, использующего одновременно ряд различных способов анализа имеющих различные показатели точности и оперативности, и позволяющего за счет этого получить результаты анализа уже на самых ранних стадиях анализа и итеративно повышать точность анализа с течением времени;

4) разработка алгоритма, позволяющего получит список рекомендаций по изменению политики безопасности системы защиты информационно-телекоммуникационной системы на основе результатов анализа моделей атак;

5) анализ существующих и разработка новых подходов к визуализации результатов оценки защищенности информационно-телекоммуникационных систем для повышения эффективности выбора контрмер;

6) реализация программной библиотеки реализующей отдельные алгоритмы построения, модификации и анализа моделей атак для проведения сравнительного анализа разработанных и существующих алгоритмов.

3.5. Полученные в ходе выполнения Проекта важнейшие результаты

В ходе второго этапа проекта были выполнены все запланированные задачи. Так, были разработаны:

1. Усовершенствованный алгоритм построения моделей атак, позволяющий формировать модели атак для нескольких нарушителей, без значительного увеличения ресурсоемкости по сравнению с построением модели атак для одного нарушителя

Разработанный на втором этапе алгоритм построения моделей атак использует модели, предложенные на прошлом этапе, а именно, обобщенную модель информационно-телекоммуникационной системы, включающей в себя

описания хостов и связей между ними, модель нарушителя безопасности информационно-телекоммуникационных систем и модель атак.

Разработанный алгоритм содержит следующие основные шаги:

1) Построение модели компьютерной сети на основе информации из открытых баз данных программно-аппаратного обеспечения, уязвимостей, атакующих действий и контрмер, данных от активных и пассивных средств сбора информации и знаний пользователей. При этом, модель компьютерной сети позволяет сформировать максимально возможное множество атакующих действий, но для оценки защищенности необходимо построить и модель нарушителя, которая ограничит возможные атаки, на основе характеристик нарушителя. Кроме того, модель нарушителя позволяет определять цели нарушителя, на основе которых становится возможно оценить успешность смоделированных последовательностей атакующих действий. Соответственно, модель нарушителя определяет ограничения на возможные атакующие действия из общего множества.

2) Выбор основных моделей нарушителей в виде множества пар (тип нарушителя, цель).

3) Построение списков возможных атакующих действий для каждого хоста на основе возможностей нарушителя (возможностей нарушителя по эксплуатации уязвимостей и выполнению атак, начальных прав). При этом, так как возможности нарушителей часто совпадают, то списки строятся сразу для групп нарушителей.

4) Построение графов возможных многошаговых атак нарушителей на основе их возможностей (точек подключения, знаний нарушителя о компьютерной сети и т.д.). При этом, так как переходы между хостами для различных нарушителей часто совпадают, то списки строятся сразу для групп нарушителей.

Таким образом, при выполнении данного алгоритма одновременно формируются модели атак для нескольких нарушителей, без значительного увеличения ресурсоемкости по сравнению с построением модели атак для одного нарушителя.

2. Алгоритм модификации модели атак, позволяющий оперативно приводить модели информационно-телекоммуникационной системы и атак в соответствии с изменениями, происходящими в сети, за счет целевой модификации только тех элементов моделей, которые соответствуют измененным элементам информационно-телекоммуникационной системы

Одной из основных проблем аналитического моделирования является необходимость постоянного обновления моделей реальных объектов для обеспечения обоснованности получаемых при моделировании результатов. Для аналитического моделирования информационно-телекоммуникационных систем на базе компьютерных сетей эта проблема также актуальна. Для решения этой проблемы в настоящем проекте был разработан алгоритм модификации модели атак, позволяющий оперативно приводить модели информационно-телекоммуникационной системы и атак в соответствии с изменениями, происходящими в сети. Для построения данного алгоритма была построена классификация возможных изменений в компьютерной сети и для каждого из типов был разработан отдельный алгоритм, наиболее эффективно приводящий модели в соответствие с измененным реальным объектом.

Рассмотрим возможные изменения в компьютерной сети более подробно (данная классификация была представлена в прошлых работах коллектива).

1. Изменение топологии (добавление связи).
2. Изменение топологии (удаление связи).
3. Изменение состава (добавление/удаление) хостов.
4. Изменение программно-аппаратной конфигурации хоста, или параметров системы безопасности связанных с одним хостом.
5. Добавление/изменение/удаление модели нарушителя.
6. Добавление/изменение/удаление уязвимостей.

Разработанный алгоритм представляет собой часть общей методики аналитического моделирования. Применение этого алгоритма позволяет значительно повысить оперативность получения результатов за счет постоянного отслеживания текущих изменений и обновления моделей, а значит и показателей,

характеризующих состояние защищенности в режиме, близком к реальному времени.

3. Алгоритм анализа моделей атак, использующий одновременно ряд различных способов анализа, имеющих различные показатели точности и оперативности, и позволяющего за счет этого получить результаты анализа поведения системы защиты компьютерной сети уже на самых ранних стадиях и итеративно повышать точность анализа с течением времени

Для повышения оперативности получения результатов анализа моделей атак в данном проекте предлагается использовать anytime алгоритмы. Основным принципом работы данного типа алгоритмов является одновременный запуск нескольких алгоритмов анализа моделей атак с разной вычислительной сложностью и, соответственно, разной точностью. При этом достигается возможность получения результатов анализа уже на ранних стадиях анализа (с низкой точностью) и возможность повышения точности с течением времени.

При этом, нельзя не отметить, что одновременное выполнение алгоритмов повышает время работы каждого из них (это происходит из-за ограниченности ресурсов), однако, это компенсируется тем, что результат может быть получен практически в любой момент времени, причем его точность и обоснованность (в случае разного количества учитываемых параметров в разных алгоритмах) будет увеличиваться в зависимости от затраченного на анализ времени.

Таким образом, anytime-алгоритмы имеют следующие особенности:

- возможность получения решения (не всегда точного) в любой момент времени;
- повышение точности с течением времени.

Для алгоритмов анализа моделей атак ресурсоемкость анализа может варьироваться за счет изменения полноты исходных данных. Так, если сходные элементы компьютерной сети будут сгруппированы, то скорость анализа возрастет. Однако, при этом могут быть пропущенные элементы возможных атакующих действий.

4. Алгоритм, позволяющий получить список рекомендаций по изменению политики безопасности системы защиты информационно-телекоммуникационной системы на основе результатов анализа моделей атак

Основным отличием разработанного в проекте алгоритма от существующих аналогов является использование моделей атак, а также использование стандартов «Общее перечисление защитных мер» (Common Remediation Enumeration, CRE) и «Расширенная информация по защитным мерам» (Extended Remediation Information, ERI). Использование моделей и стандартов позволяет рассчитать показатели эффективности, стоимости и побочного ущерба контрмеры, а использование anytime алгоритмов позволяет предоставить оператору наилучшие (с некоторой степенью точности) контрмеры в любой момент времени в зависимости от текущей информации о состоянии защищенности и событиях безопасности.

Для формирования списка рекомендаций на уровне выбора контрмер задается модель защитной меры: C=(V, P, M, Sc, AI, SI), где V – уязвимость против которой направлена защитная мера, P – платформа или конфигурация в которой применима защитная мера, M – режим работы системы (статический или динамический), Sc – область действия (attack graph element / host / subnet / network), AI – влияние на граф атак, SI – влияние на граф зависимостей сервисов (удаление, добавление, изменение). Модель сформирована на основе стандартов протокола SCAP: CRE и ERI.

Алгоритм формирующий список рекомендаций в динамическом режиме принимает на вход результаты методики оценки защищенности динамического режима и включает следующие основные шаги: (1) определение позиции атакующего на графе атак на основе событий безопасности, поступающих от SIEM-системы; (2) определение уровня навыков атакующего на основе событий безопасности, поступающих от SIEM-системы; (3) вычисление вероятностей для путей атак, проходящих через узел, соответствующий текущей позиции атакующего, учитывая уровень навыков атакующего. Для этого применяется теорема Байеса с учетом того, что событие компрометации соответствующего

узла истинно; (4) вычисление значений риска для путей, проходящих через скомпрометированный узел на основе критичности соответствующего узла, ущерба от атаки и вероятности атаки; (5) выделение узлов, для которых значение риска больше или равно «Высокий» для реализации контрмер; (6) сортировка контрмер по количеству узлов, на которые они повлияют (в случае контрмер, влияющих на равное количество узлов, создается несколько списков контрмер); (7) определение контрмер для каждого узла на основе полученных списков: сначала выбираются контрмеры, действующие на наибольшее количество узлов графа, затем контрмеры, действующие на наибольшее число из оставшихся узлов, и так пока не будут охвачены все узлы; (8) вычисление индекса выбора контрмер для полученных на шаге (7) списков. Выбирается список с максимальным суммарным индексом выбора контрмер.

Показатель индекс выбора контрмеры CI определяется на основе выигрыша в результате реализации контрмеры и затрат на ее реализацию (а именно, стоимости реализации контрмеры и побочного ущерба от ее реализации). При этом выигрыш должен стремиться к максимально возможному значению, а затраты – к минимальному, поэтому: , где Riska – возможные потери до реализации контрмеры, Riskb – возможные потери после, CD – побочный ущерб, CC – стоимость контрмеры.

5. Обзор существующих и новых разработанных подходов к визуализации результатов оценки защищенности информационно-телекоммуникационных систем для повышения эффективности выбора контрмер

Для визуализации результатов оценки защищенности информационно-телекоммуникационных систем существует множество подходов. Наиболее популярные подходы включают в себя модели визуализации, которые способны отображать связи между элементами системы. К таким моделям относятся:

- графы – способ представления, когда элементы представляются вершинами, а связи между ними ребрами;

- глифы – графоориентированный способ представления, в котором каждая вершина делится на сектора различного цвета в зависимости от вкладываемой метрики;
- матрицы – способ, в котором элементы представлены номерами строк и столбцов, а связи между элементами – ячейками;
- карты деревьев – иерархический способ представления, в котором каждый элемент представлен прямоугольником, содержащим в себе множество таких же элементов-прямоугольников с различной площадью.

Также существует множество других моделей, в том числе способных отображать элементы без связей. К таким моделям относятся: линейные графики, столбчатые графики, круговые графики, иерархические графики, параллельные координаты, радиальные координаты, розы ветров, пузырчатые графики, географические координаты, графики рассеивания, гистограммы, гексогональные карты, диаграммы Вороного, временные интервалы, японские свечи, диаграммы Чорда, коллизионные графики, облака тегов, графики плотности, трилинейные координаты, кластерограммы, потоковые графики, специализированные инфографики и другие.

Различные комбинации уже существующих моделей визуализации позволяют создавать новые модели, оптимальные для определенного сценария. Так, комбинация глифов и матриц позволяет отображать на порядок больше метрик безопасности, если вместо ячеек на пересечении строк и столбцов отображать глифы. Комбинация графов и временных интервалов позволяет отображать пересечение временных процессов в графоориентированном виде, и тем самым упрощает моделирование и анализ происходящих процессов. Комбинация кластерограмм и коллизионных графиков позволяет производить кластерных анализ на основе визуальной аналитики без применения методов машинного обучения, что делает кластеризацию более точной.

6. Программная библиотека, реализующая отдельные алгоритмы построения, модификации и анализа моделей атак для проведения сравнительного анализа разработанных и существующих алгоритмов

В качестве практической реализации была разработана программная библиотека, реализующая отдельные алгоритмы построения, модификации и анализа моделей атак для проведения сравнительного анализа разработанных и существующих алгоритмов.

Данная библиотека была объединена с библиотекой разработанной на первом этапе проекта. За счет этого была достигнута возможность формирования исходных данных из открытых баз данных программно-аппаратного обеспечения, уязвимостей, атакующих действий и контрмер.

Для проведения экспериментов были реализованы следующие алгоритмы, предложенные в данном проекте

1) усовершенствованный алгоритм построения моделей атак;
2) алгоритм модификации модели атак, позволяющего оперативно приводить модели компьютерной сети и атак в соответствие с измененной реальной сетью;
3) алгоритм анализа моделей атак, использующего одновременно ряд различных способов анализа имеющих различные показатели точности и оперативности;
4) алгоритм формирования списка рекомендаций по изменению политики безопасности системы защиты информационно-телекоммуникационной системы на основе результатов анализа моделей атак;
5) алгоритм построения ряда визуализационных моделей для отображения результатов оценки защищенности информационно-телекоммуникационных систем для повышения эффективности выбора контрмер.

Для обеспечения кроссплатформенности и модульности библиотека была реализована на языке Java с использованием новейших технологий.

3.6. Сопоставление полученных результатов с мировым уровнем

Научные и практически результаты, полученные в рамках проведенного в 2016 году исследования, соответствуют мировому уровню. Это подтверждается успешной апробацией на ряде российских и иностранных конференциях и публикациями в российских и иностранных рецензируемых журналах. Авторы проекта изложили основные результаты в 2 статьях, опубликованных в изданиях, индексируемых в международных базах цитирования (сборники трудов конференций «XIX International Conference on Soft Computing and Measurements (SCM'2016) » и «The 2016 International Symposium on Mobile Internet Security (MobiSec’16)») и в 6 статьях, опубликованных в журналах, входящих в список ВАК Минобрнауки России (журналы «Информационно-управляющие системы», «Известия вузов. Приборостроение», «Труды СПИИРАН»), а также в прочих журналах и трудах конференций. Кроме публикаций в журналах, результаты также были апробированы на множестве различных российских и международных конференций, в частности, на 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.; Восемнадцатой международной конференции “РусКрипто’2016”. Московская область, г.Солнечногорск, 22-25 марта 2016 г.; 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, июль 2015 года; XXIX Международной научной конференции "Математические методы в технике и технологиях - ММТТ-29", 31 мая - 3 июня 2016 года; Международном конгрессе по интеллектуальным системам и информационным технологиям (IS-IT’16), Дивноморское, Россия, сентябрь 2016 года.

3.7. Методы и подходы, использованные в ходе выполнения Проекта (описать, уделив особое внимание степени оригинальности и новизны)

Для достижения поставленных в 2016 году целей использовались следующие методы и подходы:

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

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

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

4) методы оценки защищенности и анализа рисков;

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

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

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

3.8. Вклад каждого члена коллектива в выполнение Проекта в 2016 году (указать работу, выполненную каждым членом коллектива по Проекту в 2016 году с новой строки)

Браницкий Александр Александрович

- разработка алгоритма, позволяющего получит список рекомендаций по изменению политики безопасности системы защиты информационно-телекоммуникационной системы на основе результатов анализа моделей атак;
- анализ существующих и разработка новых подходов к визуализации результатов оценки защищенности информационно-телекоммуникационных систем для повышения эффективности выбора контрмер;
- реализация программной библиотеки реализующей отдельные алгоритмы построения, модификации и анализа моделей атак.

Десницкий Василий Алексеевич

- разработка усовершенствованного алгоритма построения моделей атак, позволяющего формировать модели атак для нескольких нарушителей;
- разработка алгоритма модификации модели атак, позволяющего оперативно приводить модели компьютерной сети и атак в соответствие с измененной реальной сетью;
- реализация программной библиотеки реализующей отдельные алгоритмы построения, модификации и анализа моделей атак.

Дойникова Елена Владимировна

- разработка алгоритма анализа моделей атак, использующего одновременно ряд различных способов анализа имеющих различные показатели точности и оперативности;

- разработка алгоритма, позволяющего получит список рекомендаций по изменению политики безопасности системы защиты информационно-телекоммуникационной системы на основе результатов анализа моделей атак.

Саенко Игорь Борисович

- - разработка усовершенствованного алгоритма построения моделей атак, позволяющего формировать модели атак для нескольких нарушителей;
- - разработка алгоритма анализа моделей атак, использующего одновременно ряд различных способов анализа имеющих различные показатели точности и оперативности;
- - анализ существующих и разработка новых подходов к визуализации результатов оценки защищенности информационно-телекоммуникационных систем для повышения эффективности выбора контрмер.

Федорченко Андрей Владимирович

- разработка алгоритма анализа моделей атак, использующего одновременно ряд различных способов анализа имеющих различные показатели точности и оперативности;
- реализация программной библиотеки реализующей отдельные алгоритмы построения, модификации и анализа моделей атак.

Чечулин Андрей Алексеевич

- разработка усовершенствованного алгоритма построения моделей атак, позволяющего формировать модели атак для нескольких нарушителей;
- разработка алгоритма модификации модели атак, позволяющего оперативно приводить модели компьютерной сети и атак в соответствие с измененной реальной сетью;

- разработка алгоритма анализа моделей атак, использующего одновременно ряд различных способов анализа имеющих различные показатели точности и оперативности;
- разработка алгоритма, позволяющего получит список рекомендаций по изменению политики безопасности системы защиты информационно-телекоммуникационной системы на основе результатов анализа моделей атак;
- анализ существующих и разработка новых подходов к визуализации результатов оценки защищенности информационно-телекоммуникационных систем для повышения эффективности выбора контрмер;
- реализация программной библиотеки реализующей отдельные алгоритмы построения, модификации и анализа моделей атак.

Шоров Андрей Владимирович

- разработка алгоритма модификации модели атак, позволяющего оперативно приводить модели компьютерной сети и атак в соответствие с измененной реальной сетью.

3.8.1. Количество научных работ по Проекту, опубликованных в 2016 году (цифрами) (пункт заполняется автоматически, выводится количество заполненных 509 форм)

22

3.8.1.1. Из них в изданиях, включенных в перечень ВАК

8

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

13

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

0

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

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

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

Страница содержащая о руководителе проекта (на английском языке): http://www.comsec.spb.ru/chechulin/

Страница содержащая о руководителе проекта (на русском языке): http://www.comsec.spb.ru/ru/staff/chechulin/

Страница содержащая информацию о публикациях коллектива (на английском языке): http://www.comsec.spb.ru/en/papers

Страница содержащая информацию о публикациях коллектива (на русском языке): http://www.comsec.spb.ru/ru/papers/

Отчет за первый этап работы по проекту: http://comsec.spb.ru/ru/projects/43/getfile

Отчет за второй этап работы по проекту: http://comsec.spb.ru/ru/projects/50/getfile

3.11. 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, 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. DOI: 10.1109/SCM.2016.7519820.

2. 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 по перечню ВАК:

3. 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.

4. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2(45). С.207-244. DOI: http://dx.doi.org/10.15622/sp.45.13

5. Проноза А.А., Чечулин А.А., Котенко И.В. Математические модели визуализации в SIEM-системах // Труды СПИИРАН. 2016. Вып. 3(46). С.90-107. DOI: http://dx.doi.org/10.15622/sp.46

6. 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. DOI: http://dx.doi.org/10.15622/sp.47.1

7. 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. 49. С. 208-225.

8. 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.

В изданиях, индексируемых в базе РИНЦ:

9. 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.

10. 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. С. 694-699. НАПЕЧАТАЛИ 2 РАЗА

11. Проноза А.А., Чечулин А.А., Копчак Я.М. Подход к оценке методов визуализации защищенности компьютерных сетей на основе соотношения показателей информативности и простоты восприятия // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.750-757.

12. 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.

13. 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.

14. Дойникова Е.В., Котенко И.В. Методика и программное средство выбора контрмер в компьютерных сетях на основе динамического перерасчета показателей защищенности // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'16, 2016, Том 2. С.271-276.

15. 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

16. Чечулин А.А., Коломеец М.В. Применение новых методов визуализации для отображения метрик безопасности компьютерной сети // Восемнадцатая Международная конференция “РусКрипто’2016”. Московская область, г.Солнечногорск, 22-25 марта 2016 г. http://www.ruscrypto.ru/

17. Федорченко А.В., Котенко И.В. Методики корреляции событий безопасности для обнаружения целевых атак // Восемнадцатая Международная конференция “РусКрипто’2016”. Московская область, г.Солнечногорск, 22-25 марта 2016 г. http://www.ruscrypto.ru/

18. Левшун Д.С., Чечулин А.А., Котенко И.В. Архитектура комплексной системы безопасности // Материалы 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 4 июля - 7 июля 2016 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.53-54.

19. Дойникова Е.В. Модели, методики и алгоритмы вычисления показателей защищенности информационных систем в рамках иерархической системы показателей защищенности // Материалы 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 4 июля - 7 июля 2016 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.45-47.

20. Федорченко А.В. Корреляция событий безопасности для обнаружения целевых атак // 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.32-33.

21. Чечулин А.А. Основные типы происходящих в компьютерной сети изменений, учитываемых при построении аналитической модели атак // 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.114-115.

22. Дойникова Е.В. Оценка защищенности на основе графов и открытых стандартов для сетей с мобильными компонентами // XV Санкт-Петербургская Международная Конференция “Региональная информатика-2016” (“РИ-2016”). Материалы конференции. СПб., 2016. С 158 - 159.

Свидетельства о регистрации программ для ЭВМ:

23. Саенко И.Б., Чечулин А.А., Агеев С.А., Богданов А.В. Программное средство адаптивной оценки трафика в мультисервисных компьютерных сетях для анализа рисков угроз информационной безопасности. Свидетельство № 2016614488. Зарегистрировано в Реестре программ для ЭВМ 25.04.2016.

24. Котенко И.В., Коломеец М.В., Чечулин А.А. Компонент формирования паттернов и извлечения информационных объектов и связей между ними для визуализации неформализованных данных разнородной структуры. Свидетельство № 2016663182. Зарегистрировано в Реестре программ для ЭВМ 29.11.2016.

25. Федорченко А.В., Чечулин А.В. Компонент экспертной оценки качества визуализации неформализованных данных разнородной структуры. Свидетельство № 2016663861. Зарегистрировано в Реестре программ для ЭВМ 19.12.2016.

26. Дойникова Е.В., Котенко И.В. Компонент динамического выбора контрмер на основе анализа инцидентов безопасности для предотвращения

развития атаки в компьютерной сети. Свидетельство № 2016663492. Зарегистрировано в Реестре программ для ЭВМ 08.12.2016.

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

Информационно-телекоммуникационные системы

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

3.14. 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

Разработанный на втором этапе алгоритм построения моделей атак использует модели, предложенные на прошлом этапе, а именно, обобщенную модель информационно-телекоммуникационной системы, включающей в себя описания хостов и связей между ними, модель нарушителя безопасности информационно-телекоммуникационных систем и модель атак.

При этом, одной из основных проблем аналитического моделирования является необходимость постоянного обновления моделей реальных объектов для обеспечения обоснованности получаемых при моделировании результатов. Для аналитического моделирования информационно-телекоммуникационных систем на базе компьютерных сетей эта проблема также актуальна. Для решения этой проблемы в настоящем проекте был разработан алгоритм модификации модели атак, позволяющий оперативно приводить модели информационно-телекоммуникационной системы и атак в соответствии с изменениями, происходящими в сети. Для построения данного алгоритма была построена классификация возможных изменений в компьютерной сети и для каждого из типов был разработан отдельный алгоритм, наиболее эффективно приводящий модели в соответствие с измененным реальным объектом.

Для повышения оперативности получения результатов анализа моделей атак в данном проекте предлагается использовать anytime алгоритмы. Основным принципом работы данного типа алгоритмов является одновременный запуск нескольких алгоритмов анализа моделей атак с разной вычислительной сложностью и, соответственно, разной точностью. При этом достигается возможность получения результатов анализа уже на ранних стадиях анализа и возможность повышения точности с течением времени. При этом, нельзя не отметить, что одновременное выполнение алгоритмов повышает время работы каждого из них (это происходит из-за ограниченности ресурсов), однако, это компенсируется тем, что результат может быть получен практически в любой момент времени, причем его точность и обоснованность (в случае разного количества учитываемых параметров в разных алгоритмах) будет увеличиваться в зависимости от затраченного на анализ времени.

Для алгоритмов анализа моделей атак ресурсоемкость анализа может варьироваться за счет изменения полноты исходных данных. Так, если сходные элементы компьютерной сети будут сгруппированы, то скорость анализа возрастет. Однако, при этом могут быть пропущенные элементы возможных атакующих действий.

Основным отличием разработанного в проекте алгоритма, позволяющего получить список рекомендаций по изменению политики безопасности системы защиты информационно-телекоммуникационной системы на основе результатов анализа моделей атак от существующих аналогов является использование моделей атак, а также использование стандартов «Общее перечисление защитных мер» (Common Remediation Enumeration, CRE) и «Расширенная информация по защитным мерам» (Extended Remediation Information, ERI). Использование моделей и стандартов позволяет рассчитать показатели эффективности, стоимости и побочного ущерба контрмеры, а использование anytime алгоритмов позволяет предоставить оператору наилучшие (с некоторой степенью точности) контрмеры в любой момент времени в зависимости от текущей информации о состоянии защищенности и событиях безопасности.

Для визуализации результатов оценки защищенности информационно-телекоммуникационных систем существует множество подходов. Наиболее популярные подходы включают в себя модели визуализации, которые способны отображать связи между элементами системы. Также существует множество других моделей, в том числе способных отображать элементы без связей. К таким моделям относятся: линейные графики, столбчатые графики, круговые графики, иерархические графики, параллельные координаты, радиальные координаты, розы ветров, графики рассеивания, гистограммы, гексогональные карты, диаграммы Вороного, временные интервалы, японские свечи, диаграммы Чорда, коллизионные графики, трилинейные координаты, кластерограммы, потоковые графики, специализированные инфографики и другие.

Различные комбинации уже существующих моделей визуализации позволяют создавать новые модели, оптимальные для определенного сценария. Так, комбинация глифов и матриц позволяет отображать на порядок больше метрик безопасности, если вместо ячеек на пересечении строк и столбцов отображать глифы. Комбинация графов и временных интервалов позволяет отображать пересечение временных процессов в графоориентированном виде, и тем самым упрощает моделирование и анализ происходящих процессов. Комбинация кластерограмм и коллизионных графиков позволяет производить кластерных анализ на основе визуальной аналитики без применения методов машинного обучения, что делает кластеризацию более точной.

В качестве практической реализации была разработана программная библиотека, реализующая отдельные алгоритмы построения, модификации и анализа моделей атак для проведения сравнительного анализа разработанных и существующих алгоритмов.

Аннотации публикаций

1. 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. DOI: 10.1109/SCM.2016.7519820.

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.

2. 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.

3. 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.

4. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2(45). С.207-244. DOI: http://dx.doi.org/10.15622/sp.45.13

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.

5. Проноза А.А., Чечулин А.А., Котенко И.В. Математические модели визуализации в SIEM-системах // Труды СПИИРАН. 2016. Вып. 3(46). С.90-107. DOI: http://dx.doi.org/10.15622/sp.46

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.

6. 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. DOI: http://dx.doi.org/10.15622/sp.47.1

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.

7. 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. 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.

8. 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.

9. 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.

10. 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. С. 694-699.

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.

11. Проноза А.А., Чечулин А.А., Копчак Я.М. Подход к оценке методов визуализации защищенности компьютерных сетей на основе соотношения показателей информативности и простоты восприятия // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.750-757.

В современной компьютерной сети ежесекундно появляется огромное количество информации о состоянии безопасности ее узлов. Для реагирования на инциденты безопасности и принятия своевременных решений данная информация должна быть представлена пользователю в наиболее развернутой и, в то же время, читаемой форме. В настоящей работе предлагается поход к оценке различных методов визуализации защищенности компьютерной сети, задачей которого является установление уровней ее информативности и простоты восприятия.

12. 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.

13. 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.

14. Дойникова Е.В., Котенко И.В. Методика и программное средство выбора контрмер в компьютерных сетях на основе динамического перерасчета показателей защищенности // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'16, 2016, Том 2. С.271-276.

В настоящее время информационные технологии применяются повсеместно, сложность и размер сетевых инфраструктур растет, а количество компьютерных угроз год от года не уменьшается. Поэтому важной задачей является разработка и усовершенствование методик реагирования на компьютерные атаки. Хотя существует большое количество исследований в данной области, универсальное решение проблемы все еще не найдено. В данной работе предлагается методика, которая учитывает характеристики различных объектов оценки защищенности, интегрируется с системами мониторинга и управления инцидентами безопасности и позволяет автоматизировать процесс обработки данных по безопасности путем применения открытых стандартов и баз

данных. Методика основана на модели контрмер, определенной с использованием открытых стандартов, комплексной системе показателей защищенности, и алгоритмах их вычисления на основе графов атак и графов зависимостей сервисов. Методика реализована в рамках прототипа системы оценки защищенности и выбора контрмер. Разработанная система позволяет выбирать контрмеры в зависимости от доступной информации по безопасности и тем самым повышать уровень защищенности компьютерной сети.

15. 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.

16. Чечулин А.А., Коломеец М.В. Применение новых методов визуализации для отображения метрик безопасности компьютерной сети // Восемнадцатая Международная конференция “РусКрипто’2016”. Московская область, г.Солнечногорск, 22-25 марта 2016 г. http://www.ruscrypto.ru/

Представляется подход к применению диаграммы Вороного для визуализации метрик защищенности компьютерной сети. Данный подход позволяет объединить достоинства таких моделей визуализации, как карты деревьев и графов атак. В докладе представлены основные этапы построения

визуализационной модели и описан программный прототип, реализующий данный подход.

17. Федорченко А.В., Котенко И.В. Методики корреляции событий безопасности для обнаружения целевых атак // Восемнадцатая Международная конференция “РусКрипто’2016”. Московская область, г.Солнечногорск, 22-25 марта 2016 г. http://www.ruscrypto.ru/

Рассматриваются исследования целевых атак с целью разработки методов их обнаружения. Предлагается определение теоретических свойств и практических особенностей атак данного класса. Основу методик составляют различные способы корреляции получаемых событий безопасности. Описываются программный стенд испытаний разработанных методик и результаты оценки их результативности.

18. Левшун Д.С., Чечулин А.А., Котенко И.В. Архитектура комплексной системы безопасности // Материалы 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 4 июля - 7 июля 2016 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.53-54.

Данная публикация посвящена описанию архитектуры разрабатываемой комплексной системы безопасности, построение которой осуществляется в рамках комплексного подхода к обеспечению безопасности. Предполагается, что данная система позволит снизить риски, связанные с проведением сложных, растянутых во времени и происходящих на разных уровнях киберфизических атак, за счет применения корреляции данных, поступающих от гетерогенных источников.

19. Дойникова Е.В. Модели, методики и алгоритмы вычисления показателей защищенности информационных систем в рамках иерархической системы показателей защищенности // Материалы 25-й научно-технической конференции «Методы и технические средства

обеспечения безопасности информации». 4 июля - 7 июля 2016 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.45-47.

Рассмотрены объекты оценки защищенности и требования к системам оценки защищенности. Описывается иерархическая система показателей защищенности, разработанная с учетом поставленных требований и классифицирующая показатели по применяемым входным данным. А также соответствующие модели и алгоритмы вычисления показателей.

20. Федорченко А.В. Корреляция событий безопасности для обнаружения целевых атак // 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.32-33.

В работе рассматриваются существующие проблемы обработки разнородных информационных событий для мониторинга и управления безопасностью в кибер-физических системах. Данные проблемы прямо влияют на уровень обеспечения безопасности критически важных объектов, и как следствие, на распространение целевых атак. Приводится подход к обнаружению атак данного класса за счет применения сегментирования защищаемой инфраструктуры по заданным критериям, например: физическое и логическое расположение, тип операционной системы, должность обслуживающего сотрудника и пр. Также предлагается осуществлять интеллектуальный анализ поступающих событий на основе раннего разбиения на сегменты.

21. Чечулин А.А. Основные типы происходящих в компьютерной сети изменений, учитываемых при построении аналитической модели атак // 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.114-115.

Для анализа защищенности компьютерных сетей часто применяются методы аналитического моделирования, позволяющие не только оценить текущее состояние защиты, но и предсказать возможные направления его изменения. При этом, одним из основных недостатков данного подхода является его высокая ресурсоемкость. Например, если в компьютерной сети происходят изменения (добавление/удаление хостов, добавление/удаление связей, и т.д.), существующие методы часто требуют полного обновления аналитических моделей. Это обуславливает важность разработки алгоритма модификации аналитических моделей, позволяющего оперативно приводить модели компьютерной сети и атак в соответствие с измененной реальной сетью, за счет целевой модификации только тех элементов моделей, которые соответствуют измененным элементам компьютерной сети. Для построения такого алгоритма необходимо определить список основных типов возможных изменений. К этому списку относятся:

1. Изменение топологии (добавление связи).
2. Изменение топологии (удаление связи).
3. Изменение состава (добавление/удаление) хостов.
4. Изменение программно-аппаратной конфигурации хоста, или параметров системы безопасности связанных с одним хостом.
5. Добавление/изменение/удаление модели нарушителя.
6. Добавление/изменение/удаление уязвимостей.

22. Дойникова Е.В. Оценка защищенности на основе графов и открытых стандартов для сетей с мобильными компонентами // XV Санкт-Петербургская Международная Конференция “Региональная информатика-2016” (“РИ-2016”). Материалы конференции. СПб., 2016. С 158 - 159.

В работе предлагается методика оценки рисков компьютерных сетей с учетом мобильных компонентов, основанная на применении графов атак, открытых стандартов для представления входных данных и оценки уязвимостей системы, применении открытых баз уязвимостей и шаблонов атак, и применении количественных метрик для оценки защищенности.

23. Саенко И.Б., Чечулин А.А., Агеев С.А., Богданов А.В. Программное средство адаптивной оценки трафика в мультисервисных компьютерных сетях для анализа рисков угроз информационной безопасности. Свидетельство № 2016614488. Зарегистрировано в Реестре программ для ЭВМ 25.04.2016.

Программа предназначена для обработки значений показателей компьютерной сети, полученных от подконтрольных узлов, и установления их принадлежности к заданным классам, каждому из которых соответствует определенное состояние сети. Результаты используются для анализа рисков информационной безопасности.

24. Котенко И.В., Коломеец М.В., Чечулин А.А. Компонент формирования паттернов и извлечения информационных объектов и связей между ними для визуализации неформализованных данных разнородной структуры. Свидетельство № 2016663182. Зарегистрировано в Реестре программ для ЭВМ 29.11.2016.

Данная программа представляет собой элемент программного комплекса визуализации параметров безопасности компьютерных сетей. Программа позволяет формировать паттерны на основе пользовательского ввода соответствия значений полей и данных в текстовых файлах формата csv. На основе сформированных паттернов происходит извлечение информационных объектов и связей между ними из текстовых csv файлов.

25. Федорченко А.В., Чечулин А.В. Компонент экспертной оценки качества визуализации неформализованных данных разнородной структуры. Свидетельство № 2016663861. Зарегистрировано в Реестре программ для ЭВМ 19.12.2016.

Данная программа предназначается для осуществления экспертной оценки качества визуализации данных. В качестве входных данных выступает профиль опроса экспертов. Пользовательский интерфейс подразумевает выполнение таких действий, как: (1) выбор опроса (файла опроса); (2) заполнение результатов

опроса; (3) вывод результата по указанному профилю опроса, являющегося выходными данными в результате работы программы.

26. Дойникова Е.В., Котенко И.В. Компонент динамического выбора контрмер на основе анализа инцидентов безопасности для предотвращения развития атаки в компьютерной сети. Свидетельство № 2016663492. Зарегистрировано в Реестре программ для ЭВМ 08.12.2016.

Данная программа предназначена для автоматического выбора контрмер для предотвращения развития атаки в компьютерной сети. Входными данными являются следующие данные: характеристики инцидента безопасности, поступившего от SIEM-системы (системы мониторинга безопасности и управления инцидентами), в предопределенном формате; граф атакующих действия для компьютерной сети (отражающий все возможные шаги атакующего в сети); список доступных контрмер в предопределенном формате; набор метрик безопасности. Результатом работы программы является список контрмер, рекомендуемых для предотвращения развития атаки на компьютерную сеть.