НАЗВАНИЕ ПРОЕКТА Разработка моделей, методик и алгоритмов автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности	НОМЕР ПРОЕКТА 16-37-00338
ОБЛАСТЬ ЗНАНИЯ 07	КОД КЛАССИФИКАТОРА 07-241, 07-235, 01-217
ВИД КОНКУРСА мол_а Конкурс научных проектов, выполняемых молодыми учеными (Мой первый грант)	
ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА Дойникова Елена Владимировна	ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА 8-906-251-26-02
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, предоставляющей условия для выполнения работ по Проекту физическим лицам Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук	

Форма 503 (мол). РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер Проекта
16-37-00338

3.2. Название Проекта
Разработка моделей, методик и алгоритмов автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности

3.3. Код классификатора
07-235, 07-241, 01-217

3.4. Объявленные ранее цели Проекта

Одной из фундаментальных научных задач является создание новых подходов к всестороннему оцениванию защищенности компьютерных сетей, основанных на комплексе показателей защищенности и применимых для систем управления информацией и событиями безопасности. Системы управления информацией и событиями безопасности (Security Information and Events Management, SIEM) разработаны для управления безопасностью компьютерных сетей в связи с ростом количества различных событий безопасности до объемов, невозможных для ручной обработки и в настоящее время активно развиваются и применяются в том числе в системах взаимодействующих сервисов.

Основные **цели** проекта на 2016 год определялись как разработка и совершенствование моделей, алгоритмов и методики оценки защищенности систем взаимодействующих сервисов на основе количественных показателей для последующего повышения эффективности реагирования на инциденты безопасности в рамках систем управления информацией и событиями безопасности.

Для достижения цели планировалось решение **задач**: детальный анализ состояния исследований в области автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов; анализ существующих систем управления информацией и событиями безопасности; формирование требований к методикам анализа защищенности и реагирования на инциденты для последующей разработки новых моделей и методик; разработка системы показателей защищенности; разработка моделей входных данных; разработка алгоритмов и методики вычисления показателей; разработка методики оценивания защищенности на основе предложенной системы показателей и алгоритмов их вычисления.

Обобщенной задачей на первом этапе являлась разработка моделей, алгоритмов и методики оценки защищенности систем взаимодействующих сервисов на основе количественных показателей, применимых для систем управления информацией и событиями безопасности. Система, основанная на результатах данного этапа исследования должна предоставлять оценку ситуации по защищенности даже при небольшом количестве входных данных, и уточнять оценки с поступлением новой информации. Таким образом, данный подход позволит отслеживать характеристики атаки и нарушителя в режиме проектирования и эксплуатации системы. Путем реализации разрабатываемых моделей, методик и алгоритмов планируется достичь повышения эффективности оценки защищенности компьютерных сетей в статическом и динамическом режимах работы.

3.5. Полученные в 2016 году результаты с описанием методов и подходов, использованных в ходе выполнения проекта

На первом этапе были выполнены все запланированные задачи:

1. **Проведен детальный анализ состояния исследований** в области автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов. Выделены применяемые в различных системах методики и показатели защищенности. Проведен анализ существующих систем управления информацией и событиями безопасности, сделан вывод о том, что используемые ими в настоящий момент показатели не дают полной картины информационных и бизнес-рисков, порождаемых потенциальными угрозами, и не позволяют принять всесторонне обоснованное решение по выбору и внедрению защитных мер. На основе анализа **сформированы требования** к разрабатываемой системе автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности: (1) получение адекватной и актуальной оценки защищенности системы на основе доступных входных данных в статическом (соответствует этапам проектирования и реализации информационной системы) и динамическом (соответствует режиму эксплуатации информационной системы) режимах работы; (2) учет характеристик атакующего, в том числе, его целей, положения в сети, начальных знаний о сети, навыков и возможностей по реализации атак в статическом и динамическом режимах работы; (3) учет взаимосвязей между сервисами сети для тщательного учета возможного распространения ущерба в случае успешной реализации атак, или побочного ущерба при реализации защитных мер, в статическом и динамическом режимах работы; (4) учет стоимостных характеристик атак и защитных мер, для того, чтобы определить выигрыш в случае реализации защитных мер, в статическом и динамическом режимах работы; (5) автоматизация процесса представления и обработки данных, применяемых для оценки защищенности и выбора защитных мер, в статическом и динамическом режимах работы; (6) выбор наиболее адекватного решения по реагированию с учетом стоимостных требований в статическом и динамическом режимах работы; (7) выявление слабых мест компьютерной сети в статическом режиме работы; (8) выявление возможных атак на сеть, и получение набора показателей защищенности, характеризующего их, в статическом режиме работы; (9) учет событий безопасности, происходящих в сети, и переоценка ситуации по защищенности в соответствии с полученной информацией, в динамическом режиме работы; (10) интеграция с системами управления информацией и событиями безопасности в динамическом режиме работы.

2. **Разработана система показателей защищенности**, включающая в себя отдельные показатели и связи между ними. Основным отличием системы является иерархический способ классификации показателей на основе входных данных, применяемых для их вычисления, этапов процесса анализа рисков, и значений показателей. Были выделены уровни классификации: топологический уровень (применяемые входные данные: модель компьютерной сети, информация о хостах, сервисах, характеристики программно-аппаратного обеспечения, в том числе уязвимости, характеристики уязвимостей на основе открытых баз уязвимостей, характеристики слабых мест хоста на основе базы слабых мест, сервисы сети и зависимости между ними); уровень графа атак (входные данные: показатели защищенности и входные данные предыдущего топологического уровня, граф атак); уровень атакующего (входные данные: показатели защищенности и входные данные предыдущих уровней, модель атакующего); уровень событий (входные данные: показатели защищенности и входные данные предыдущих уровней, события безопасности); уровень выбора контрмер (входные данные: показатели защищенности и входные данные предыдущих уровней, модель

контрмеры) и интегральный уровень (входные данные: показатели защищенности и входные данные предыдущих уровней).

Каждая категория включает подкатегории: базовые характеристики, стоимостные характеристики, характеристики нулевого дня. Внутри каждой подкатегории выделяются основные показатели, используемые для вычисления значения уровня риска, и вспомогательные, не используемые для вычисления значения уровня риска.

Уровни классификации выделены в зависимости от обрабатываемых входных данных для удовлетворения требований адекватного отражения текущей ситуации на основе доступных входных данных и применения в качестве входных данных графов атак и графов зависимостей сервисов. Уровень событий введен для удовлетворения требования интеграции с системами управления информацией и событиями безопасности и выделения статического и динамического режимов оценки защищенности и выбора защитных мер. Уровень выбора контрмер добавлен для учета контрмер при оценке защищенности, а также выбора контрмер. Категория стоимостных характеристик введена учета стоимостных характеристик атак и контрмер.

Каждый уровень содержит набор показателей (как известных, так и модифицированных и вновь введенных в рамках работы над Проектом), отражающий последние исследования в данной области. Система позволяет для каждой выделенной группы показателей получить оценку защищенности системы и выбрать защитные меры.

3. **Разработаны аналитические модели входных данных**. Для этого определены основные источники входных данных, в том числе администратор, сетевые сканеры, SIEM-система, открытые базы уязвимостей, слабых мест и атак. В качестве входных данных для вычисления показателей используются данные о сети и ее уязвимостях, разработанные модели атак и зависимостей сервисов, модели атакующих, событий, и контрмер, экспертные оценки уязвимостей и контрмер, и оценки из открытых баз данных. Разработаны методы сбора и обработки данных из различных источников с применением открытых стандартов протокола SCAP (CVE для представления уязвимостей, CWE для представления слабых мест, CPE для представления программно-аппаратного обеспечения, CAPEC для представления атак, CRE и ERI для представления контрмер) для последующего использования их при заполнении формируемых моделей. Для отслеживания распространения ущерба в системе взаимодействующих сервисов разработана модель в виде направленного графа (узлы – сервисы, дуги – связи между ними, определяющие зависимость свойств безопасности сервиса предка от свойств безопасности сервиса потомка с учетом конъюнктивных и дизъюнктивных зависимостей), позволяющая определять влияние атак и контрмер на активы сети. Для определения направления развития атак, их вероятностей, и влияния событий на вероятность успешной атаки, сформирован Байесовский граф атак. Узлы графа соответствуют атакующим действиям (эксплуатация уязвимостей). При этом для последующего автоматизированного выбора контрмер, узлы графа сгруппированы по разным типам угроз. Связи между узлами определены на основе матриц доступности для хостов, и пред- и постусловий эксплуатации уязвимостей. Для совместного применения графов атак и графов зависимостей сервисов для определения уровня риска определена связь между этими двумя моделями. Для определения влияния событий на вероятность атаки, выделены типы событий, поступающих от системы управления информацией и событиями безопасности, и определена их связь с графом атак. Определена модель атакующего и ее связь с графом атак.

4. **Разработаны алгоритмы вычисления показателей** с использованием разработанных моделей. Алгоритмы разделены на группы в зависимости от используемых при вычислениях моделей и входных данных. Алгоритмы различных групп иерархически связаны между собой: выходные данные алгоритмов группы каждого предыдущего уровня используются в качестве входных данных алгоритмов группы следующего уровня.

Это позволяет уточнять показатели за счет новых входных данных (в том числе от систем управления информацией и событиями безопасности). При этом показателей каждой отдельной группы достаточно для получения интегральных показателей, определяющих оценку защищенности и выбор защитных мер. Первичные показатели, характеризующие модели различных входных данных задаются как вручную экспертами (например, критичность основных сервисов, или уровень навыков атакующего), так и на основе открытых баз данных (например, локальные вероятности атакующих действий, определяемые на основе индексов системы оценки уязвимостей CVSS), или определяются на основе характеристик системы управления информацией и событиями безопасности (например, надежность информации о событиях, поступающей от системы). Алгоритмы вычисления показателей топологического уровня включают, в том числе, иерархическое вычисление показателей для различных объектов сети, от уязвимостей до сети в целом. А также оригинальный алгоритм вычисления критичности не основных активов сети на основе графа зависимостей сервисов путем обхода графа, с применение матричных вычислений для учета распространения критичности на зависимые сервисы по свойствам конфиденциальности, целостности и доступности. Алгоритмы вычисления показателей уровня графа атак основаны на байесовском выводе для определения вероятности компрометации различных узлов графа. Связь с топологическим уровнем системы показателей (через связь графа атак и графа зависимостей сервисов) позволяет уточнить показатели риска топологического уровня путем учета вероятностей атак. Также разработаны алгоритмы определения наиболее вероятных путей атаки на графе, определения самых слабых узлов графа (самых критичных уязвимостей), определения ущерба от атак, на основе обхода графа атак с применением стандартных оптимизационных алгоритмов, и с учетом характеристик уязвимостей, соответствующих узлам графа. Разработан алгоритм отображения событий безопасности на граф атакующих действий, использующий связь между моделью событий и моделью атак, и позволяющий уточнить показатели вероятности уровня графа атак на основе алгоритмов переопределения вероятностей на основе теоремы Байеса и определения характеристик конкретного атакующего (чьи действия привели к генерации события безопасности).

5. **Разработана иерархическая методика оценки защищенности** на основе графов атак и графов зависимостей сервисов, определяющая применяемые на каждом уровне иерархии модели, показатели и алгоритмы их вычисления, и их взаимосвязи между разными уровнями. Методика относится к так называемым any-time подходам. Основным отличием методики является то, что она позволяет получить оценку текущей ситуации по защищенности в форме адекватных количественных показателей на основе имеющихся в наличии входных данных, и уточнять ее с появлением новых данных. Что достигается за счет мониторинга поступающих входных данных и перерасчета показателей защищенности на основе алгоритмов соответствующего уровня при поступлении новых данных, таким образом формируется гибкая система, позволяющая реагировать на изменения состава и качества данных по безопасности, режима функционирования системы и временных характеристик. Методика включает три этапа: (1) сбор и обработка входных данных (на основе которых строятся модели, которые потом применяются для вычисления показателей); (2) вычисление показателей защищенности; (3) определение уровня защищенности. Выделяются этапы работы методики в статическом и динамическом режиме. Статическому режиму работы соответствуют топологический уровень системы показателей защищенности, уровень графа атак и уровень атакующего. В статическом режиме работы методика включает этапы: (1) сбор и обработка входных данных, (2) проверка уровня системы показателей, которому соответствуют входные данные, и выбор соответствующих показателей и алгоритмов их вычисления, (3) вычисление показателей соответствующего уровня, (4) вычисление показателей интегрального уровня, (5) определение уровня защищенности системы (сравнение показателей интегрального уровня с заданными критериями). Результат работы методики

в статическом режиме: уровень риска системы и комплекс показателей защищенности. Для динамического режима работы дополнительно введен уровень событий. В динамическом режиме работы методика включает этапы: (1) ожидание поступления событий, (2) при поступлении события, оно отображается на граф атак, (3) запуск вычисления показателей уровня событий, (4) вычисление показателей интегрального уровня, (5) определение уровня защищенности системы. Результат работы в динамическом режиме: путь атаки, цель атаки, характеристики атакующего, ожидаемые потери в случае успешной реализации атаки (уровень риска).

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

Федорченко Андрей Владимирович:

- детальный анализ состояния исследований в области автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов;
- анализ существующих систем управления информацией и событиями безопасности;
- формирование модели события безопасности.

Дойникова Елена Владимировна:

- формирование требований к разрабатываемой системе автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности;
- разработка системы показателей защищенности;
- разработка модели зависимостей сервисов и ее связи с моделью атак;
- разработка алгоритмов вычисления показателей защищенности;
- разработка методики оценки защищенности (этапов вычисления показателей и оценки уровня защищенности).

Чечулин Андрей Алексеевич:

- формирование требований к разрабатываемой системе;
- разработка моделей предметной области;
- разработка методики оценки защищенности (этапов сбора и обработки данных).

Браницкий Александр Александрович:

- разработка показателей защищенности, характеризующих атаки и атакующих, и алгоритмов их вычисления.

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

10

3.8.1.1. Из них в изданиях, включенных в перечень ВАК

5

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

5

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

1

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

0

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

1. 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, секционный доклад

2. 25-я научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», 4 июля - 7 июля 2016 г., Санкт-Петербург, секционный доклад

3. 9-я конференция "Информационные технологии в управлении" (ИТУ-2016), 4-6 октября 2016 г., СПб., секционный доклад

4. XV Санкт-Петербургская Международная Конференция “Региональная информатика-2016” (“РИ-2016”), секционный доклад

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

Нет

3.11. Финансовые средства, полученные в 2016 году от Фонда

450000

3.12. Адреса ресурсов в Интернете, подготовленных авторами по данному проекту

http://comsec.spb.ru/doynikova/

http://comsec.spb.ru/ru/staff/doynikova

http://comsec.spb.ru/ru/papers

http://comsec.spb.ru/en/papers

3.13. Библиографический список всех публикаций по Проекту, опубликованных в 2016 году, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.

1. 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.
2. 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
3. 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
4. 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.
5. 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.
6. 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, С.210-213.
7. 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.
8. 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.
9. 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.

10. 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.

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

Информационно-телекоммуникационные системы

3.15. Критическая технология РФ, которой, по мнению исполнителей, соответствуют результаты данного проекта

Технологии информационных, управляющих, нвигационных систем

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

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

Основные результаты Проекта

1. **Проведен детальный анализ состояния исследований** в области автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в повсеместно использующихся системах взаимодействующих сервисов. Выделены применяемые в различных системах методики и показатели защищенности. Проведен анализ существующих систем управления информацией и событиями безопасности, активно развивающихся в настоящее время ввиду увеличения объемов информации по безопасности, генерируемой различными устройствами. Сделан вывод о том, что используемые ими в настоящий момент показатели не дают полной картины информационных и бизнес-рисков, порождаемых потенциальными угрозами, и не позволяют принять всесторонне обоснованное решение по выбору и внедрению защитных мер. На основе анализа **сформированы требования** к разрабатываемым моделям, методикам и алгоритмам.

2. **Разработана система показателей защищенности,** применяемых для оценки защищенности и выбора контрмер при реагировании на инциденты безопасности. Система включает взаимосвязанные группы показателей, выделенные в зависимости от применяемых для их вычисления разнородных входных данных. Каждая группа включает ряд показателей защищенности, характеризующих определенные объекты оценки защищенности и позволяет получить на их основе оценку уровня защищенности системы взаимодействующих сервисов и выбирать меры для реагирования на инциденты безопасности, поступающие от системы управления информацией и событиями безопасности.

3. **Разработаны аналитические модели входных данных**. Для этого определены основные источники входных данных (администратор, сетевые сканеры, система управления информацией и событиями безопасности, открытые базы уязвимостей, слабых мест и атак) и сами входные данные, необходимые для вычисления показателей защищенности, применяемых для оценки защищенности и выбора контрмер при реагировании на инциденты безопасности (данные о сети, ее сервисах и уязвимостях, характеристики атак и зависимостей сервисов, атакующих, событий, и контрмер, экспертные оценки уязвимостей и контрмер, и оценки из открытых баз данных). **Разработаны методы сбора и обработки данных** из различных источников с применением открытых стандартов. **Разработаны модели**: модель сети, модель зависимостей сервисов, модель атак, модель событий, модель атакующего, модель контрмер. Определены связи между различными моделями предметной области.

4. **Разработаны алгоритмы вычисления показателей защищенности** с использованием разработанных моделей. Алгоритмы разделены на группы в зависимости от используемых при вычислениях моделей и входных данных. Алгоритмы различных групп иерархически связаны между собой: выходные данные алгоритмов группы каждого предыдущего уровня используются в качестве входных данных алгоритмов группы следующего уровня. Это позволяет уточнять показатели за счет новых входных данных (в том числе от систем управления информацией и событиями безопасности). При этом показателей каждой отдельной группы достаточно для получения интегральных показателей, определяющих оценку защищенности и выбор защитных мер.

5. **Разработана иерархическая методика оценки защищенности** на основе графов атак и графов зависимостей сервисов, определяющая применяемые на каждом уровне иерархии модели, показатели и алгоритмы их вычисления, и их взаимосвязи между разными уровнями. Методика относится к так называемым any-time подходам. Основным отличием

методики является то, что она позволяет получить оценку текущей ситуации по защищенности в форме адекватных количественных показателей на основе имеющихся в наличии входных данных, и уточнять ее с появлением новых данных. Что достигается за счет мониторинга поступающих входных данных и перерасчета показателей защищенности на основе алгоритмов соответствующего уровня при поступлении новых данных, таким образом формируется гибкая система, позволяющая реагировать на изменения состава и качества данных по безопасности, режима функционирования системы и временных характеристик.

Аннотации публикаций

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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, С.210-213.

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.

7. 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.

8. 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.

9. 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.

10. 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.