На правах рукописи

Дойникова Елена Владимировна

ОЦЕНКА ЗАЩИЩЕННОСТИ И ВЫБОР ЗАЩИТНЫХ МЕР В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ ГРАФОВ АТАК И ЗАВИСИМОСТЕЙ СЕРВИСОВ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2017

Работа выполнена в федеральном бюджетном учреждении науки "Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)".

Научный руководитель:	доктор технических наук, профессор Котенко Игорь Витальевич, СПИИРАН, заведующий лабораторией проблем компьютерной безопасности.
Официальные оппоненты:	доктор технических наук, профессор Новиков Владимир Александрович, Федеральное государственное бюджетное военное образовательное учреждение высшего образования «Военно-космическая академия имени А.Ф.Можайского», профессор кафедры.
	доктор технических наук, профессор Иванов Александр Юрьевич, Федеральное государственное казенное образовательное учреждение высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации», профессор кафедры специальных информационных технологий.
Ведущая организация	АО «Научно-исследовательский институт «Рубин»

Защита диссертации состоится "25" мая 2017 г. в __:__ часов на заседании совета по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Д 002.199.01 при Федеральном государственном бюджетном учреждении науки "Санкт-Петербургский институт информатики и автоматизации Российской академии наук" (СПИИРАН) по адресу:
199178, Санкт-Петербург, 14-а линия В.О., 39, комн. 401.
Факс: (812)-328-44-50 тел: (812)-328-34-11.

С диссертацией и авторефератом можно ознакомиться на сайте Федерального государственного бюджетного учреждения науки "Санкт-Петербургский институт информатики и автоматизации Российской академии наук".
http://www.spiiras.nw.ru/dissovet/

Автореферат разослан "____"_____2017 г.

Ученый секретарь совета
Д 002.199.01

к.т.н, доц. Фаткиева Р.Р.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. Оценка защищенности и выбор защитных мер в компьютерных сетях (КС) является важной и актуальной задачей ввиду непрекращающегося роста количества и сложности киберпреступлений. Согласно ГОСТ Р ИСО/МЭК 27005-2010 оценка защищенности включает определение источников риска, количественную оценку риска и сравнение полученных оценок с заданными критериями. Защитные меры (контрмеры) применяются для избегания, оптимизации, переноса или сохранения риска.

Для оценки защищенности и выбора контрмер используется информация из различных источников. Для сбора и обработки информации, связанной с безопасностью КС, были разработаны системы мониторинга безопасности и управления инцидентами (Security Information and Events Management, SIEM). Однако, реализованные в них методики не позволяют получить всестороннюю оценку ситуации по безопасности и рекомендации по выбору защитных мер на основе адекватных количественных показателей. Аспекты определения различных характеристик атак и защитных мер широко рассмотрены в исследовательских работах. Для определения таких характеристик атаки, как вероятность ее успешной реализации в КС, и соответствующих рисков безопасности, успешно применяются графы атак. Графы атак показывают, как могут быть использованы уязвимости системы для выполнения многошаговых атак нарушителями. Для определения потенциального влияния атак на бизнес-операции применяются методики определения распространения ущерба на основе графов зависимостей сервисов. Граф зависимостей сервисов представляет собой множество сервисов КС, связанных между собой в соответствии с тем, как свойства безопасности одного сервиса зависят от свойств безопасности другого.

Существующие методики оценки, как правило, ограничиваются детальным исследованием только одного из наборов характеристик атак и защитных мер, например, уровнем навыков атакующего, вероятностью атаки, возможным ущербом. Они не позволяют сформировать полную картину информационных рисков и принять всесторонне обоснованное решение по выбору и внедрению защитных мер. Таким образом, данная задача является актуальной и на данный момент не имеет эффективного решения.

Степень разработанности темы диссертации. Вопросам оценки защищенности и анализа рисков КС посвящено большое количество стандартов и работ как отечественных исследователей: С.В. Симонова, И.В. Котенко, С.А. Петренко, И.Б. Саенко, А.М. Астахова, Д.С. Черешкина, А.Г. Остапенко, М.В. Степашкина, А.А. Чечулина, так и зарубежных: R.P. Lippmann, H. Debar, N. Kheir, M. Frigault, N. Poolsappasit, M. Jahnke, G.G. Granadillo. Анализ работ показал,

что они зачастую ограничены исследованием одного набора характеристик объектов оценки и не учитывают данных, предоставляемых SIEM-системами. Поэтому в данной работе была поставлена задача разработки комплексного подхода к оценке защищенности КС и выбору защитных мер, основанного на вычислении различных показателей и применимого для SIEM-систем, который позволит отслеживать характеристики атаки, атакующего и выбирать адекватные защитные меры.

Научная задача. Разработка модельно-методического аппарата для оценки защищенности КС и выбора защитных мер на основе совместного применения графов атак и зависимостей сервисов для SIEM-систем.

Объект исследования. КС, атаки на КС с использованием уязвимостей их программного и аппаратного обеспечения.

Предмет исследования. Модели, методики и алгоритмы оценки защищенности КС и выбора защитных мер на этапах проектирования и эксплуатации с использованием показателей защищенности.

Основной целью диссертационной работы является повышение защищенности КС за счет усовершенствования методик, моделей и алгоритмов оценки защищенности КС и выбора контрмер на основе вычисления показателей защищенности. Для достижения данной цели в диссертационной работе поставлены и решены следующие **задачи**:

1. Анализ показателей защищенности и методик их вычисления на основе моделей умышленных атак в КС в виде графов атакующих действий и моделей распространения воздействия атаки в сети в виде графов зависимостей сервисов.
2. Разработка комплекса показателей защищенности с учетом различных входных данных, таких как модели КС, атакующих действий, нарушителей и инцидентов безопасности, и на различных уровнях функционирования защищаемой системы (статическом и динамическом).
3. Разработка методики оценки защищенности КС на основе графов атак и зависимостей сервисов.
4. Разработка алгоритмов вычисления показателей защищенности.
5. Разработка методики выбора защитных мер для реагирования на компьютерные атаки с учетом доступных данных.
6. Построение архитектуры и реализация программного прототипа системы оценки защищенности КС и выбора защитных мер на основе предложенных методик.
7. Экспериментальная оценка предложенных алгоритмов и методик, и сравнение их с существующими аналогами.

Положения, выносимые на защиту:

1. Комплекс показателей защищенности компьютерных сетей на основе графов атак и зависимостей сервисов.

2. Методика оценки защищенности КС на основе графов атак и зависимостей сервисов.

3. Методика выбора защитных мер на основе графов атак и зависимостей сервисов.

4. Архитектура и программная реализация системы оценки защищенности КС и выбора защитных мер на основе предложенных методик.

Научная новизна диссертационной работы состоит в следующем:

1. Разработанный комплекс показателей защищенности отличается иерархическим способом классификации на основе объектов оценки, этапов процесса оценки защищенности и категорий показателей (базовые, 0 дня, стоимостные), и позволяет для каждой выделенной группы показателей получить оценку защищенности системы и выбрать защитные меры.

2. Предложенная методика оценки защищенности на основе графов атак и зависимостей сервисов отличается тем, что на каждом уровне иерархии задается совокупность используемых моделей, показателей и алгоритмов оценки, и определяет взаимосвязи между разными уровнями. Методика основана на использовании входных данных о сети и ее уязвимостях, атаках, зависимостях сервисов, атакующих, событиях, контрмерах, экспертных оценках уязвимостей и контрмер, и оценках из открытых баз данных.

3. Разработанная методика выбора защитных мер отличается возможностью генерации комплекса защитных мер на основе доступных входных данных и его последующего уточнения за счет применения иерархического комплекса показателей на основе анализа событий безопасности, выделением этапов статического и динамического уровня, и совместным применением графов атак и зависимостей сервисов.

4. Разработанная архитектура и программная реализация системы оценки защищенности и выбора защитных мер отличается наличием интерфейсов взаимодействия с SIEM-системами и применением оригинальных методик оценки защищенности и выбора защитных мер.

Обоснованность и достоверность представленных научных положений обеспечивается тщательным анализом состояния исследований в области, подтверждается согласованностью результатов, полученных при экспериментах, успешной апробацией на ряде научных конференций всероссийского и международного уровня, и публикацией в ведущих рецензируемых научных изданиях.

Теоретическая и практическая значимость результатов исследования. Разработанные методики оценки защищенности КС и выбора защитных мер развивают теоретические положения в данной области и позволят снизить уровень

возможных потерь организаций в результате компьютерных атак за счет постоянного отслеживания и пересчета показателей защищенности в соответствии с поступающими данными о событиях в системе и своевременного применения адекватных контрмер. Данные методики должны стать основой компонента принятия решений активно распространяющихся SIEM-систем. Применимость результатов исследования состоит в необходимости обработки генерируемых такими системами данных для формирования текущей картины по безопасности и выработки рекомендаций по реагированию. В настоящее время КС применяются во многих критически важных коммерческих и государственных отраслях. Необходимость их дальнейшего развития и повышения уровня их защищенности определены в стратегии развития информационного общества в Российской Федерации на 2014–2020 годы. Это указывает на обширную область применения результатов исследования.

Реализация результатов работы. Отраженные в диссертационной работе исследования проведены в рамках следующих научно-исследовательских работ: грантов РФФИ № 16-37-00338-мол_а и № 13-01-00843-а, гранта РНФ № 15-11-30029, проектов Минобрнауки России № 14.604.21.0137, № 14.604.21.0033, № 14.616.21.0028 и № 11.519.11.4008, проекта 2009-2011 гг. по программе фундаментальных исследований РАН «Математические модели, методы и алгоритмы моделирования атак, анализа защищенности компьютерных систем и сетей, анализа рисков безопасности информации и принятия решений о выборе механизмов защиты в компьютерных системах и сетях»; и др. Полученные результаты использовались в рамках проекта седьмой рамочной программы (FP7) Европейского Сообщества (контракт № 257475), внедрены в учебный процесс СПб ГУТ, используются в научно-инновационной деятельности в ООО «Ароматы безопасности», применяются в рабочем процессе ГК «Омега».

Апробация результатов работы. Основные положения и результаты работы докладывались на научных конференциях: международный симпозиум по безопасности мобильного Интернета MobiSec-2016 (Тайчжун, Тайвань, 2016); 24-я международная конференция по параллельной, распределенной и сетевой обработке PDP-2016 (Ираклион, Греция, 2016); 10-ая международная конференция по рискам и безопасности Интернета и систем CRiSIS-2015 (Митилини, Греция, 2015); 22-я международная конференция по параллельной, распределенной и сетевой обработке PDP-2014 (Турин, Италия, 2014); 22-я общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2013); VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013)» (Санкт-Петербург, 2013); 8-я международная конференция по доступности, надежности и

безопасности ARES-2013 (Регенсбург, Германия, 2013); 7-я международная конференция по интеллектуальному сбору данных и передовым вычислительным системам IDAACS-2013 (Берлин, Германия, 2013); часть 5-й Российской мультиконференции по проблемам управления – конференция «Информационные технологии в управлении (ИТУ-2012)» (Санкт-Петербург, 2012); XIII Санкт-Петербургская Международная Конференция «Региональная информатика-2012 (РИ-2012)» (Санкт-Петербург, 2012); 19-я международная конференция по параллельной, распределенной и сетевой обработке PDP-2011 (Айя-Напа, Кипр, 2011); и др.

Публикации. По материалам диссертационной работы опубликовано более 40 работ, в том числе 9 – в рецензируемых изданиях из перечня ВАК («Информационно-управляющие системы», «Безопасность информационных технологий», «Проблемы информационной безопасности. Компьютерные системы», «Известия высших учебных заведений. Приборостроение», «Труды СПИИРАН»), 12 – в изданиях, индексируемых в международных базах Scopus и Web Of Science, и 5 свидетельств о государственной регистрации программ для ЭВМ.

Структура и объем диссертационной работы. Диссертационная работа включает введение, три главы, заключение, список литературы (146 наименований) и 15 приложений. Объем работы – 163 страницы машинописного текста; включает 40 рисунков и 17 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована важность и актуальность темы диссертационной работы, определена цель и сформулированы задачи, решение которых необходимо для ее достижения. Показаны научная новизна и практическая значимость работы. Дано краткое описание предложенного комплекса показателей защищенности, применяемых моделей представления анализируемых объектов, разработанных методик оценки защищенности и выбора защитных мер, а также представлены основные результаты разработки предлагаемых моделей, алгоритмов и методик в научно-исследовательских проектах.

Первая глава диссертации посвящена анализу задачи оценки защищенности и выбора контрмер для повышения уровня защищенности КС. В главе определены место и роль оценки защищенности и выбора защитных мер в задаче повышения защищенности КС. Проведен анализ существующих систем, обоснована актуальность цели исследования. Для достижения поставленной цели предложено использование методик, основанных на иерархическом комплексе показателей защищенности и алгоритмах их вычисления. Определены требования к методикам оценки защищенности и выбора контрмер: автоматизация процесса представления и обработки данных, выявление возможных атак на КС и получение характеризующего

их набора показателей, совместимость с SIEM-системами для учета событий безопасности, учет характеристик атакующего, учет взаимосвязей между сервисами КС, учет стоимостных характеристик при определении выигрыша в случае реализации защитных мер, получение адекватной и актуальной оценки защищенности КС и выбор наиболее адекватного решения по реагированию на основе доступных входных данных. Сформулирована постановка задачи исследования.

Во второй главе представлены разработанный комплекс показателей защищенности, входные данные для вычисления показателей (включая модели представления анализируемых объектов), методика оценки защищенности, алгоритмы вычисления показателей, входящие в ее состав, и методика выбора защитных мер.

Разработанный комплекс показателей представлен на рисунке 1. Он включает несколько уровней (топологический, графа атак, атакующего, событий, выбора контрмер и интегральный) и категорий (базовые показатели, показатели 0 дня и стоимостные показатели) в соответствии с используемыми входными данными. Сплошными стрелками на рисунке показаны зависимости между уровнями и входными данными, пунктирными стрелками показаны необязательные зависимости. Выделяются статические уровни: топологический, графа атак, атакующего, и динамический: событий. Комплекс позволяет на каждом уровне отразить текущий уровень защищенности.

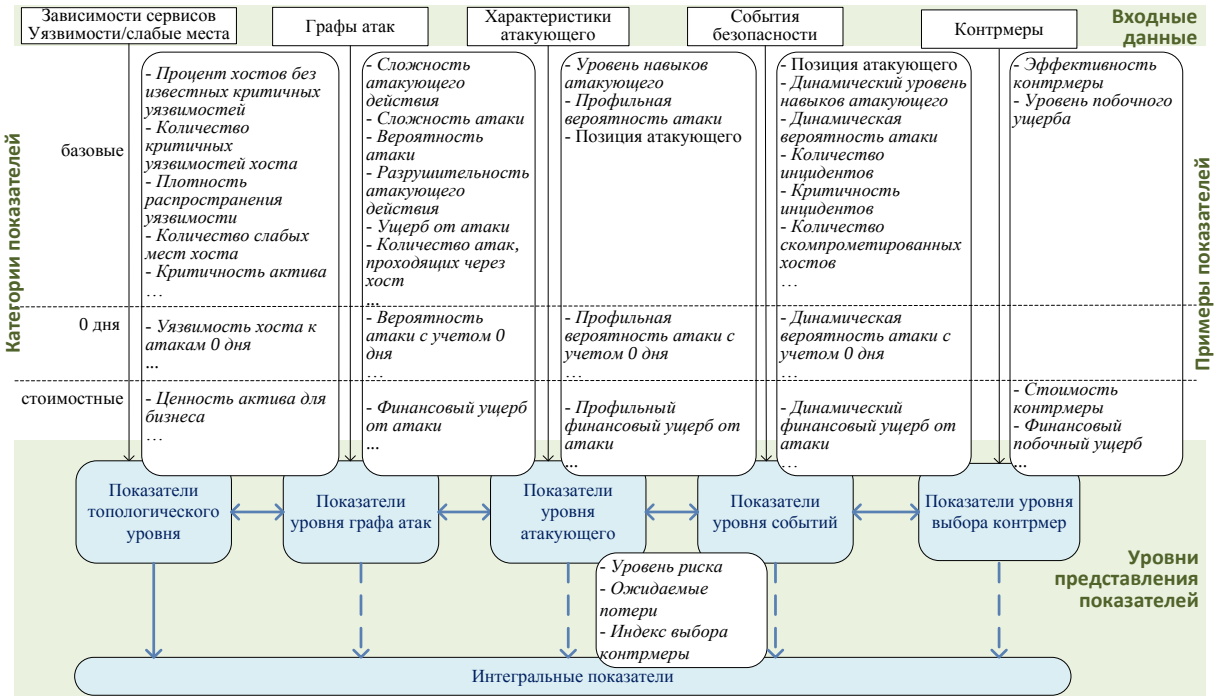


Рисунок 1 – Комплекс показателей защищенности

Под топологическими понимаются показатели, определяемые на основе конфигурации и топологии КС. Уровень графа атак позволяет определить

вероятность атаки и возможный ущерб с учетом всех путей атаки. На уровне атакующего выделяются атаки, которые может реализовать конкретный атакующий. Уровень событий позволяет отслеживать развитие атаки и профиль атакующего по событиям безопасности. Уровень выбора контрмер включает показатели, характеризующие защитные меры. Интегральный уровень включает показатели, вычисляемые на основе показателей предыдущих уровней, характеризующие защищенность системы в целом и позволяющие выбрать защитные меры.

Предложенная методика оценки защищенности включает следующие этапы (рисунок 2): (1) сбор входных данных и формирование аналитических моделей (идентификация риска); (2) вычисление показателей защищенности (установление значения риска); (3) определение уровня защищенности (сравнительная оценка риска).

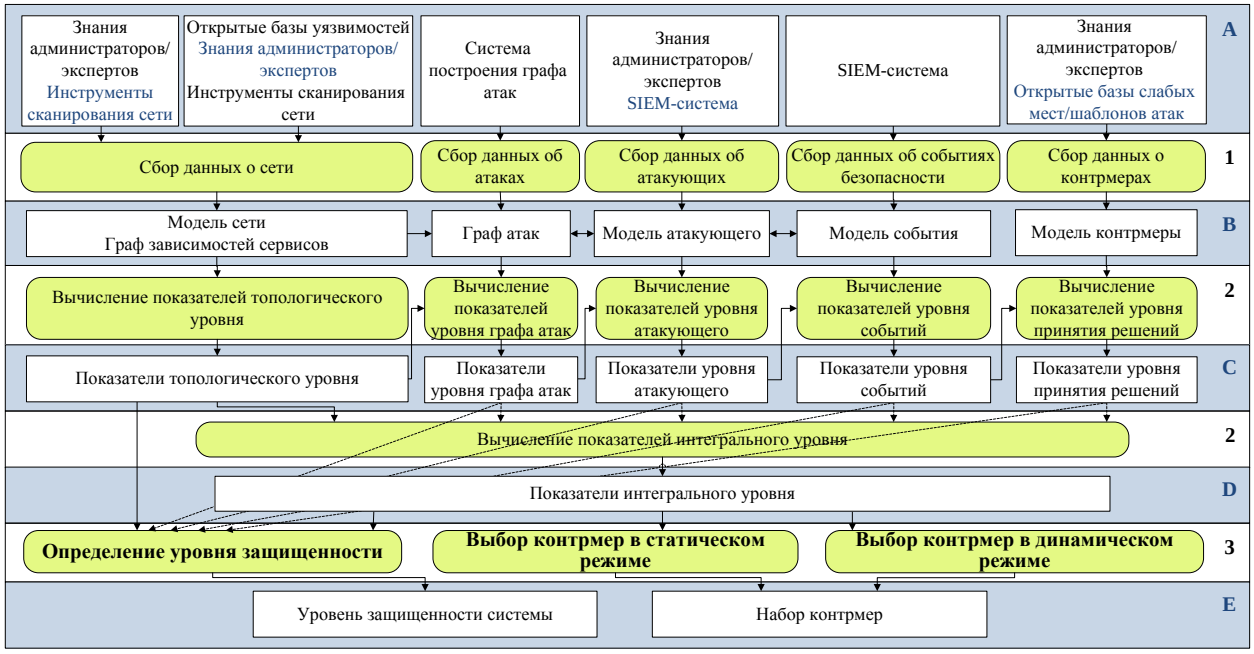


Рисунок 2 – Обобщенная схема методики оценки защищенности

На каждом этапе полученный на вход набор данных преобразуется в выходной. Стрелками показано движение данных между вычислительными модулями. На уровне **A** отображены источники входных данных, предоставляемых в формате открытых стандартов: CVE, CWE, CPE, CAPEC, CRE, ERI и CVSS, что позволяет использовать в качестве источника входных данных открытые базы, заполняемые экспертами. На основе собранных данных конкретизируются значения параметров моделей, применяемых при дальнейших вычислениях показателей (**B**). На уровне **E** отображены выходные данные. На остальных уровнях (**C**, **D**) отображены данные, применяемые на соответствующих этапах. В основе методики лежит так называемый anytime-подход: для определения уровня защищенности применяются показатели

интегрального уровня и как минимум топологического уровня. Остальные уровни являются дополнительными, что показано пунктирными стрелками.

Уровень защищенности системы определяется на основе уровня риска R по ГОСТ Р ИСО/МЭК 27005-2010: $R=P \cdot El$, где P – вероятность успешной реализации атаки, El – потери в случае успешной реализации атаки: $El=Cr \cdot Im$, где Cr – критичность активов; Im – ущерб, наносимый критичности активов.

Определение полной критичности активов осуществляется в статическом режиме с учетом зависимости от них бизнес-активов организации на основе модели зависимостей сервисов: $SG=(R, L, \varepsilon)$, где R – множество узлов графа зависимостей сервисов (сервисов), L – множество связей ($L \subseteq R \times R$), ε – множество кортежей, определяющих тип зависимости между сервисами, вида $<L_k, d_k>$, где $L_k \in L$, $d_k \in$ {И, ИЛИ}. Связь определяется как: $L = (r_i, r_j, W)$, где $r_i, r_j \in R$; $r_j \in Det(r_i)$; $Det(r_i)$ – множество всех прямых потомков сервиса r_i (то есть сервисов, от свойств безопасности которых напрямую зависят свойства безопасности r_i); W – весовая матрица, определяющая степень зависимости свойств безопасности взаимосвязанных сервисов (предка и потомка). Модель сервиса: $S=(T, Cr)$, где T – тип сервиса (*информационно-технологические (ИТ) активы, порт или программно-аппаратное обеспечение*); Cr – критичность сервиса ($Cr=[Cr(c)\ Cr(i)\ Cr(a)]$, $Cr(c)$, $Cr(i)$, $Cr(a)$ – критичность сохранения свойств конфиденциальности c, целостности i и доступности a, соответственно.

Для связи со стоимостью активов для организации в алгоритм добавлен этап организационного уровня отображения бизнес-активов на ИТ активы организации. Критичность бизнес-активов с учетом финансовой важности их защищенности для целей организации задается их владельцами в финансовых единицах, отображаемых на шкалу: {0; 0,01; 0,1; 1; 10; 100}. Итоговая критичность остальных активов (сервисов) определяется на техническом уровне при обходе графа зависимостей сервисов в виде трехмерного вектора по параметрам c, i и a: $pCr_{r_k} = wCr_{r_m} + iCr_{r_k}$, где r_k – сервис потомок, r_m – сервис предок; iCr_{r_k} и wCr_{r_m} – собственная критичность сервиса потомка и критичность, распространенная от сервиса предка, соответственно, в виде трехмерных векторов по параметрам c, i и a.

Определение критичности активов, не представляющих прямой бизнес-ценности для организации, позволяет не упустить узкие места системы при оценке защищенности и избежать побочного ущерба при реализации защитных мер. Прямая зависимость между стоимостью активов для организации и шкалой оценки критичности позволяет обосновать необходимость финансовых вложений в реализацию защитных мер.

Показатель ущерба, наносимого критичности актива r_k в результате атакующего действия a_i, задается в виде вектора: [$ConfImpact_{k,i}(c)$ $IntegImpact_{k,i}(i)$ $AvailImpact_{k,i}(a)$], где $k \in [1, l]$, l – количество всех программных активов организации; $i \in [1, m]$, m – множество всех уязвимостей актива; $ConfImpact_{k,i}(c)$, $IntegImpact_{k,i}(i)$, $AvailImpact_{k,i}(a)$ – влияние на c, i и a актива, соответственно.

$ConfImpact_{k,i}(c)$, $IntegImpact_{k,i}(i)$, $AvailImpact_{k,i}(a)$ определяются на основе одноименных показателей системы оценки уязвимостей CVSS для уязвимостей. Потери в случае успешной реализации атаки определяются по свойствам c, i и a в виде вектора: [$Impact_{k,i}(c)$ $Impact_{k,i}(i)$ $Impact_{k,i}(a)$], путем перемножения показателей критичности актива по соответствующему свойству и ущерба в результате атакующего действия. Общий ущерб определяется суммированием ущерба по трем свойствам.

Определение вероятности успешной реализации атаки осуществляется на основе Байесовского графа атак: $G=(S, L, \tau, Pc)$, где S – множество узлов графа (атакующих действий), L – множество связей ($L \subseteq S \times S$), τ – множество кортежей, определяющих тип связи между узлами, Pc – дискретные локальные распределения условных вероятностей. Модель атакующих действий: $S=(H, V, Sc, St, Pr)$, где H – атакованный хост, включает описание сервисов хоста (связь с графом зависимостей сервисов добавлена для одновременного учета распространения ущерба и вероятностного аспекта компрометации активов); V – использованная уязвимость; Sc – атака, направленная на сбор информации о хосте; Pr – вероятность того, что атакующее действие находится в состоянии St ($Pr \in [0,1]$). Выбор данной модели обусловлен тем, что Байесовские графы атак позволяют учитывать влияние событий на состояние системы и прогнозировать в соответствии с этим развитие атаки, определять предыдущие шаги атаки, делать выводы об атаке на основе субъективных знаний при отсутствии статистических данных.

Алгоритм определения вероятности атаки включает шаги: определение локальных вероятностей компрометации узлов графа (то есть вероятностей того, что атакующий сможет и проэксплуатирует уязвимость, соответствующую данному узлу, если все предусловия выполнены), определение условных вероятностей компрометации узлов графа (дискретных локальных распределений условных вероятностей), определение безусловных вероятностей компрометации узлов (вероятностей атаки).

Локальная вероятность $p(a_i)$ компрометации узла графа S_i в случае атакующего действия a_i определяется на основе индексов CVSS *AccessComplexity* (*AC*) – сложность доступа к уязвимости, *Authentication* (*Au*) – параметры аутентификации, *AccessVector* (*AV*) – вектор доступа к уязвимости. Для корневых узлов графа $p(a_i)$ определяется по формуле:

$$p(a_i)=2\times AV\times AC\times Au. \quad (1)$$

Для узлов, не являющихся корневыми, $p(a_i)$ определяется по формуле:

$$p(a_i)=2\times AC\times Au. \quad (2)$$

Вектор доступа к уязвимости учитывается только для корневых узлов графа, поскольку переход из состояния в состояние на графе атак возможен только в случае наличия доступа к соответствующему узлу.

Дискретные локальные распределения условных вероятностей *Pc* определяются с учетом типов связей между узлами. В случае связей типа «И» (для успешной компрометации узла потомка S_i необходимо, чтобы все узлы предки $Pa(S_i)$ были скомпрометированы):

$$Pc(S_i \mid Pa(S_i)) = \begin{cases} 0, & \exists S_i \in Pa(S_i) \mid S_i = 0 \\ p(S_i), & \text{иначе} \end{cases}. \quad (3)$$

В случае связей типа «ИЛИ» (для успешной компрометации узла потомка необходимо, чтобы хотя бы один узел предок был скомпрометирован):

$$Pc(S_i \mid Pa(S_i)) = \begin{cases} 0, & \forall S_i \in Pa(S_i) \mid S_i = 0 \\ p(S_i), & \text{иначе} \end{cases}. \quad (4)$$

Безусловные вероятности компрометации узлов графа определяются путем обхода графа на основе локальных вероятностей и распределений условных вероятностей по формуле полной вероятности.

Дополнительные данные об атакующем и событиях позволяют уточнить оценку путем пересчета показателя вероятности атаки. Алгоритм уровня событий включает отображение события на граф атак, переопределение уровня навыков атакующего, и переопределение вероятности атаки. Алгоритм отображения события на граф атак заключается в поиске узла графа по хосту, которому соответствует событие безопасности и последствиям атакующего действия, сгенерировавшего событие. Алгоритм переопределения уровня навыков атакующего включает шаги: переопределение вероятности атаки для узла, для которого поступило событие безопасности; определение наиболее вероятного пути атакующего до данного узла на основе теоремы Байеса; выбор узлов пути с максимальным значением индекса CVSS *сложность доступа*. Уровень навыков атакующего *AttackerSkillLevel* определяется равным этому значению (на шкале «Высокий»/«Средний»/«Низкий»). Алгоритм переопределения вероятности атаки включает шаги: переопределение вероятности атаки для узла, для которого поступило событие безопасности; вычисление вероятностей для путей атак, проходящих через данный узел на основе формулы

полной вероятности и с учетом новых значений локальных вероятностей. Локальные вероятности для корневых узлов графа переопределяются по формуле:

$$p(a)=AV\times(AC+AttackerSkillLevel)\times Au. \quad (5)$$

Локальные вероятности для узлов графа, не являющихся корневыми, переопределяются по формуле:

$$p(a)=0{,}5\times(AC+AttackerSkillLevel)\times Au. \quad (6)$$

Методика выбора защитных мер основана на модели защитной меры, которая концептуально описывается как: $C=(V, P, M, Sc, AI, SI)$, где V – уязвимость против которой направлена мера, P – платформа или конфигурация в которой применима мера, M – режим работы системы, Sc – область действия (элемент графа атак/сети), AI – влияние на граф атак, SI – влияние на граф зависимостей сервисов (удаление, добавление, изменение). V и P позволяют автоматизировано определить узлы графа атак, к которым применима мера. AI и SI определяют перестроение графов для пересчета показателей после реализации контрмер.

Методика выбора защитных мер в динамическом режиме начинает работу, когда новое значение риска для узлов графа атак превышает пороговое значение. Основные этапы методики: выделение узлов, для которых значение риска больше порогового; сортировка контрмер, применимых к выделенным узлам, по количеству узлов, на которые они повлияют (в случае контрмер, влияющих на равное количество узлов, создается несколько списков контрмер); определение контрмер для каждого узла на основе полученных списков: сначала выбираются контрмеры, действующие на наибольшее количество узлов графа, затем контрмеры выбираются по максимальному несовпадению покрытий (при полном совпадении контрмера исключается), пока не будут охвачены все узлы; вычисление *индекса выбора контрмер* для полученных на предыдущем шаге списков. Выбирается список с максимальным суммарным индексом выбора контрмер.

В третьей главе приведена архитектура и общее описание программного прототипа, разработанного для проведения экспериментов. Представлены результаты экспериментов и сравнение предложенной методики с существующими аналогами. Описаны возможности практического применения основных результатов исследования.

Для проведения экспериментов был дополнительно разработан генератор сценариев атак на основе открытых шаблонов атак CAPEC. Обобщенная архитектура генератора представлена на рисунке 3.

Генератор работает следующим образом: (1) выбор модели атакующего; (2) случайный выбор шаблона из группы разведывательных шаблонов с учетом модели атакующего и конфигурации сети; (3) формирование списка шаблонов атак

для доступных хостов, на основе модели атакующего и конфигурации сети; (4) случайный выбор шаблона из сформированного списка; (5) повторение шагов (2)-(4) с учетом нового положения атакующего в сети. Цепочка событий формируется на шагах (2)-(4) на основе информации из шаблонов.

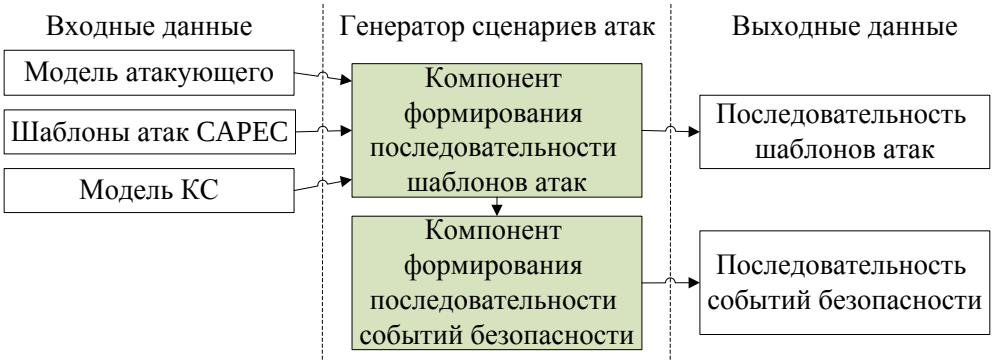


Рисунок 3 – Обобщенная архитектура генератора сценариев атак

Обобщенная архитектура прототипа системы оценки защищенности и выбора контрмер представлена на рисунке 4. Основные функциональные подсистемы прототипа: подсистема обработки исходных данных; компонент оценки защищенности, работающий в статическом и динамическом режимах; компонент выбора контрмер.

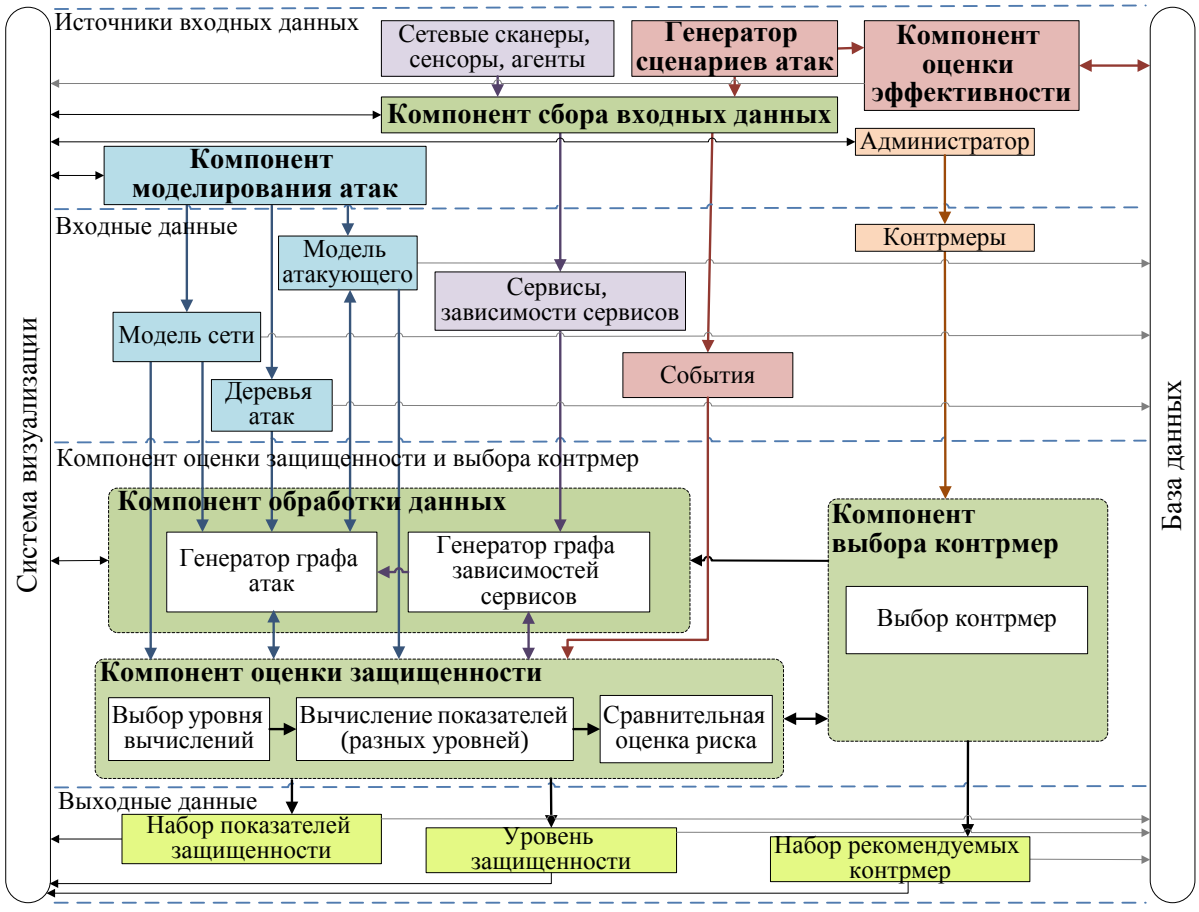
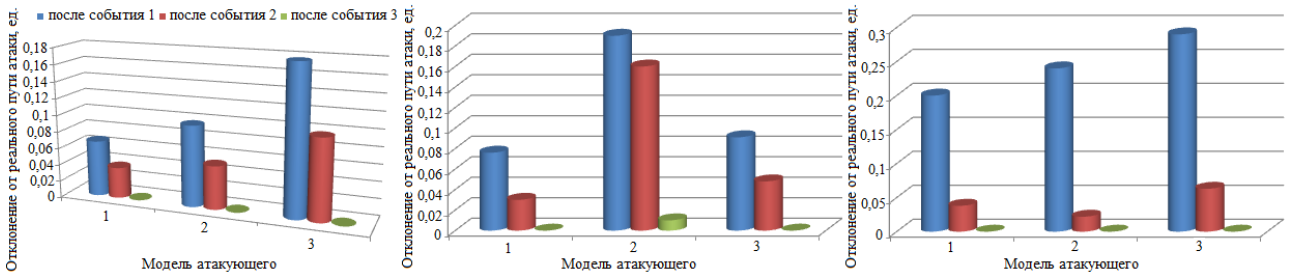


Рисунок 4 – Обобщенная архитектура прототипа, реализующего предложенные методики, в рамках тестового стенда

Эксперименты проводились для трех реальных сетей разного размера (10, 20 и 40 хостов) с добавлением случайных элементов, и трех разных типов атакующих (атакующий 1 – с низкими навыками, атакующий 2 – со средними, атакующий 3 – с высокими). По очереди выполнялись этапы предложенных методик оценки защищенности и выбора контрмер для сценариев атак, сформированных генератором. Защищенность КС оценивалась в статическом и динамическом режимах, в динамическом режиме выбирались контрмеры для противодействия соответствующему сценарию атаки.

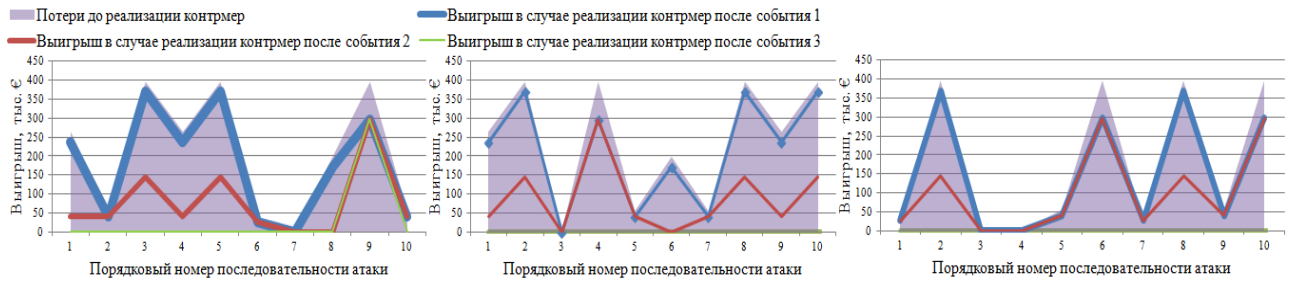
Эксперименты показали, что учет дополнительной информации (событий безопасности) в динамическом режиме, позволяет повысить точность локализации последовательности атаки (т.е. снизить отклонение спрогнозированной последовательности атаки от реальной, рисунок 5) с ростом количества обработанных событий безопасности и, соответственно, рационально реагировать на атаку (рисунок 6).



а) б) в)

Рисунок 5 – Усредненная точность локализации пути атаки для атакующего 1, 2 и 3 после поступления событий для: а) сети 1; б) сети 2; в) сети 3

Из графиков на рисунке 6 видно, что наибольший финансовый выигрыш достигается в случае реализации контрмер после поступления события 1. Это связано с тем, что уровень риска превышает пороговое значение уже после события 1, в случае, если в этот момент не реализовать контрмер, атакующий успевает нанести ущерб системе и выигрыш при реализации контрмер после события 2 уже значительно ниже.



а) б) в)

Рисунок 6 – Уровень потерь до и финансовый выигрыш после реализации контрмер для сети 1 для: а) атакующего 1; б) атакующего 2; в) атакующего 3

Оценка разработанных методик производилась на основе проверки выполнения свойств своевременности, обоснованности и ресурсопотребления. Основными в работе были названы свойства обоснованности: (1) количество анализируемых сценариев атак; (2) количество учитываемых параметров; (3) точность выявления сценария атаки; (4) выигрыш в случае реализации контрмер.

Количество анализируемых сценариев атак зависит от количества учитываемых уязвимостей. Предлагаемая методика учитывает все известные уязвимости программно-аппаратного обеспечения из открытых баз данных и по данному параметру не уступает существующим аналогам. Результаты оценки количества параметров, учитываемых разработанной методикой представлены в таблице 1 («-» – параметр не учитывается, «+» – учитывается, «+/-» – частично учитывается). Из нее видно, что по количеству учитываемых параметров методика превосходит существующие аналоги.

Таблица 1 – Сравнение предложенной методики с существующими

Методика оценки защищенности	**Параметры, учитываемые при оценке**								
	Базовые показатели (множество дополнительных показателей, рассчитываемых на основе параметров КС)	Характеристики атаки (вероятность)	Характеристики атакующего (уровень навыков, положение, мотивация)	Ущерб от атаки (потери)	Общая оценка защищенности (уровень риска или уровень защищенности, поверхность атаки)	Затраты на контрмеры	Побочный ущерб от реализации контрмер	Эффективность контрмер	События безопасности
Poolsappasit и др., 2012	-	+	-	+-	+	+-	+-	+	+
Dantu и др., 2009	-	+-	+	-	+	-	-	+	-
Kheir и др., 2010	-	-	-	+	-	+-	+	+	-
Wu и др., 2007	-	+-	-	+	-	-	+	+	+
Степашкин, 2007	-	+	+-	+-	+	-	-	-	-
Jahnke и др., 2009	-	+-	-	+-	-	-	+-	+-	+-
Lippmann и др., 2006	-	+	-	+-	-	-	-	+-	-
Granadillo и др., 2012	-	+	-	+	+	-	+	+	-
Разработанная методика	+	+	+-	+	+	+-	+	+-	+

Точность выявления сценариев атаки определяется на основе отклонения выявленного сценария атаки от реального *AC*: $AC \to \min$. Результаты оценки соответствия разработанной системы данному требованию представлены на рисунке 5, из которого видно, что требование удовлетворяется. Финансовый выигрыш в случае реализации контрмер определяется на основе индекса *AL*: $AL \to EL$, где *EL* – потери, в случае успешной реализации атаки. Результаты оценки соответствия разработанной системы данному требованию представлены на рисунке 6, из которого видно, что требование $AL \to EL$ удовлетворяется.

Финансовый выигрыш в случае реализации контрмер говорит о повышении уровня защищенности системы при реализации компьютерных атак.

Результаты экспериментов, проведенных с использованием разработанного прототипа, показали, что значения свойств обоснованности методики удовлетворяют предъявляемым требованиям. Разрабатываемая система обнаруживает не меньше сценариев атак, чем существующие аналоги, и учитывает большее количество параметров. При этом точность выявления сценариев атаки и выигрыш в случае реализации контрмер стремятся к максимуму. Это позволяет говорить о том, что новая система превосходит существующие аналоги по функциональности и качеству анализа. Своевременность оценивалось путем последовательного выполнения этапов методик для сетей различного размера. Ресурсопотребление оценивалось с теми же параметрами, которые использовались для оценки выигрыша в случае реализации контрмер. Результаты экспериментов показали, что своевременность и ресурсопотребление соответствуют требованиям, предъявляемым к подобным системам. Таким образом, применение предложенной методики позволяет повысить защищенность КС, при этом соблюдаются требования к обоснованности, своевременности и ресурсопотреблению, и цель, поставленная в данном диссертационном исследовании, достигнута.

В заключении представлены основные научные результаты проведенного исследования.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

Комплекс предложенных в диссертационной работе показателей, методик и алгоритмов, и их практическая реализация, представляют собой решение актуальной задачи разработки модельно-методического аппарата для оценки защищенности КС и выбора защитных мер для SIEM-систем. Их внедрение вносит значительный вклад в развитие систем управления безопасностью КС. При решении данной задачи были получены следующие результаты:

1. Разработан комплекс показателей защищенности КС на основе графов атак и зависимостей сервисов, позволяющий отражать текущую ситуацию по защищенности на основе доступных входных данных. Выбор общепринятых стандартов для представления входных данных позволил использовать как источник информации открытые базы уязвимостей, шаблонов атак и т.д.

2. Предложена методика оценки защищенности КС на основе графов атак и зависимостей сервисов, включающая несколько групп взаимосвязанных алгоритмов вычисления показателей, и позволяющая формировать оценку защищенности при различных наборах входных данных и уточнять ее при поступлении новых данных.

3. Разработана методика выбора защитных мер на основе графов атак и зависимостей сервисов, позволяющая в статическом и динамическом режимах работы системы выбирать защитные меры на основе доступных входных данных и корректировать результат при поступлении новых данных.

4. Разработана архитектура системы и реализация программного прототипа на основе предложенных методик. Проведенные эксперименты показали улучшение уровня защищенности тестовых КС при реализации различных сценариев атак, при сохранении показателей ресурсопотребления, оперативности и обоснованности по сравнению с существующими системами.

Результаты соответствуют п. 9 Паспорта специальностей ВАК (технические науки) «Модели и методы оценки защищенности информации и информационной безопасности объекта» по специальности 05.13.19. Дальнейшее направление исследований может быть связано как с совершенствованием полученных результатов (расширение комплекса показателей, повышение оперативности методик выбора контрмер, учет временного и исторического аспектов при выборе контрмер), так и с развитием в сторону полноценных SIEM-систем, что включает разработку дополнительных компонентов (хранилища данных, системы корреляции и др.) и связей между ними.

СПИСОК ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых изданиях из списка ВАК:

Дойникова, Е. В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов / Е. В. Дойникова // Труды СПИИРАН. – 2013. – Вып. 3 (26). – С. 54–68.

Котенко, И. В. Вычисление и анализ показателей защищенности на основе графов атак и зависимостей сервисов / И. В. Котенко, Е. В. Дойникова // Проблемы информационной безопасности. Компьютерные системы. – 2014. – № 2. – С. 19–36.

Котенко, И. В. Динамический перерасчет показателей защищенности на примере определения потенциала атаки / И. В. Котенко, Е. В. Дойникова, А. А. Чечулин // Труды СПИИРАН. – 2013. – Вып. 7 (30). – С. 26–39.

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

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

Котенко, И. В. Анализ защищенности автоматизированных систем с учетом социо-инженерных атак / И. В. Котенко, М. В. Степашкин, Е. В. Дойникова // Проблемы информационной безопасности. Компьютерные системы. – 2011. – № 3. – С. 40–57.

Котенко, И. В. Оценка защищенности информационных систем на основе построения деревьев социо-инженерных атак / И. В. Котенко, М. В. Степашкин, Д. И. Котенко, Е. В. Дойникова // Изв.вузов.Приборостроение. –2011. –Т. 54, № 12. –С. 5–9.

Котенко, И. В. Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности / И. В. Котенко, Е. В. Дойникова // Информационно-управляющие системы. – 2015. – № 3. – С. 60–69.

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

Публикации из баз данных Web Of Science и Scopus:

Kotenko, I. Security metrics for risk assessment of distributed information systems / I. Kotenko, E. Doynikova // Proceedings of the IEEE 7th International Conference on “Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications”. – 2013. P. 646–650.

Kotenko, I. The ontology of metrics for security evaluation and decision support in SIEM systems / I. Kotenko, I. Saenko, O. Polubelova, E. Doynikova // Proceedings of the 8th International Conference on Availability, Reliability and Security. – 2013. P. 638–645.

Kotenko, I. Security metrics based on attack graphs for the Olympic Games scenario / I. Kotenko, E. Doynikova, A. Chechulin // Proceedings of the 22th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing. – 2014. – P. 561–568.

Kotenko, I. Dynamical calculation of security metrics for countermeasure selection in computer networks / I. Kotenko, E. Doynikova // Proceedings of the 24th International Conference on Parallel, Distributed and network-based Processing. – 2016. – P. 558–565.

Kotenko, I. Security analysis of information systems taking into account social engineering attacks / I. Kotenko, M. Stepashkin, E. Doynikova // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing. – 2011. – P. 611–618.

Kotenko, I. Evaluation of computer network security based on attack graphs and security event processing / I. Kotenko, E. Doynikova // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. – 2014. – Vol.5, No.3. – P. 14–29.

Kotenko, I. Security assessment of computer networks based on attack graphs and security events / I. Kotenko, E. Doynikova // Lecture Notes in Computer Science. – Vol. 8407. – Springer. – 2014. – P. 462–471.

Kotenko, I. Security evaluation for cyber situational awareness / I. Kotenko, E. Doynikova // Proceedings of the 16th IEEE International Conference on High Performance Computing and Communications, 11th IEEE International Conference on Embedded Software and Systems and 6th International Symposium on Cyberspace Safety and Security. – 2014. P.1229–1236.

Kotenko, I. Countermeasure selection in SIEM systems based on the integrated complex of security metrics / I. Kotenko, E. Doynikova // Proceedings of the 23rd Euromicro International Conference on Parallel, Distributed and Network-based Processing. – 2015. – P. 567–574.

Doynikova, E. Countermeasure selection based on the attack and service dependency graphs for security incident management / E. Doynikova, I. Kotenko // Lecture Notes in Computer Science. – Volume 9572. – Springer, 2016. – P.107–124.

Kotenko, I. The CAPEC based generator of attack scenarios for network security evaluation / I. Kotenko, E. Doynikova // Proceedings of the IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – 2015. – P. 436–441.

Kotenko, I. Combining of scanning protection mechanisms in GIS and corporate information systems / I. Kotenko, A. Chechulin, E. Doynikova // Lecture Notes in Geoinformation and Cartography. – 2011. – Springer. – P. 45–58.

Свидетельства о государственной регистрации программ для ЭВМ:

Дойникова, Е. В. Компонент определения рисков информационной безопасности активов компьютерной сети на основе полученных событий безопасности. Свидетельство № 201614489 от 25.04.2016 / Е. В. Дойникова, И. В. Котенко.

Дойникова, Е. В. Генератор случайных последовательностей атакующих действий для тестирования сетей Интернета вещей. Свидетельство № 2015615368 от 15.05.2015 / Е. В. Дойникова, А. А. Чечулин.

Дойникова, Е. В. Компонент оценивания критичности ресурсов на основе построения модели зависимостей сервисов при тестировании компонентов защиты в сетях Интернета вещей. Свидетельство № 2015615374 от 24.03.2015 / Е. В. Дойникова, И. В. Котенко.

Чечулин, А. А. Компонент анализа моделей атак для защиты информационно-телекоммуникационных систем. Свидетельство № 2015619151 от 16.11.2015 / А. А. Чечулин, Е. В. Дойникова.

Котенко, И. В. Вычисление показателей защищенности для анализа текущего состояния информационно-телекоммуникационных систем и поддержки принятия решений по реагированию на инциденты информационной безопасности. Свидетельство № 2014661026 от 22.10.2014 / И. В. Котенко, Е. В. Дойникова, А. А. Чечулин.