АКЦИОНЕРНОЕ ОБЩЕСТВО
“НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
“РУБИН”

а/я 359, Кантемировская, д. 5, Санкт-Петербург, 197342, тел.: (812)670-89-89, факс: (812)596-35-81, e-mail: inforubin@rubin-spb.ru
ИНН/КПП 7802776390/780201001, ОГРН 1127847043720, ОКПО 07542394

Экз. № 2

УТВЕРЖДАЮ
ральный директор
) «НИИ «Рубин»
А.Ю. Рунеев
04» мая 2017 г.

ОТЗЫВ

ведущей организации на диссертационную работу Дойниковой Елены Владимировны «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АКТУАЛЬНОСТЬ ТЕМЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

Компьютерные сети являются неотъемлемой частью инфраструктуры многих современных организаций. При этом важной особенностью является вывод ряда сервисов системы во внешние сети. Создавая новые возможности и повышая удобство для пользователей, это в тоже время ведет к появлению дополнительных точек входа для компьютерных атак. В такой ситуации особенно актуальной становится задача обеспечения защищенности компьютерных сетей организаций. Для ее выполнения необходимо корректно оценить защищенность системы, чтобы выявить наиболее слабые с точки зрения безопасности места, выбрать адекватные защитные меры и избежать серьезного материального ущерба. Однако получение адекватной оценки состояния защищенности затрудняется сложностью конфигурации

современных сетей, постоянными изменениями состава программно-аппаратного обеспечения, и появлением новых уязвимостей. При этом из-за сложности взаимосвязей между сетевыми объектами не всегда просто выявить уязвимости, которые могут нанести серьезный ущерб и выбрать защитные меры, которые не нанесут еще больший вред системе. В таких условиях для своевременного реагирования на инциденты и предотвращения развития атак в компьютерной сети процесс оценки защищенности и выбора защитных мер необходимо автоматизировать. Это можно осуществить путем автоматизированного построения и анализа моделей основных компонентов безопасности. Для определения возможных путей атак в компьютерной сети и выявления ее слабых мест применяются модели в виде графов атакующих действий. Для определения распространения ущерба в системе, в том числе от внедрения защитных мер используются графы зависимостей сервисов. При этом существующие инструменты и исследования в области оценки защищенности обычно применяют только одну из указанных моделей, используя ограниченный набор характеристик защищенности и принятия решений, что не позволяет осуществлять адекватный мониторинг ситуации и принимать всесторонне обоснованное решение по выбору защитных мер. Поэтому задача разработки моделей, методик и программного инструмента оценки защищенности и выбора защитных мер на основе совместного применения моделей атак и зависимостей сервисов является актуальной и имеет практическую ценность для мониторинга ситуации по защищенности и реагирования на инциденты безопасности.

НАУЧНАЯ НОВИЗНА РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

В диссертации Дойниковой Е.В. предложен комплекс показателей защищенности компьютерных сетей. Комплекс отличается от уже существующих способом классификации показателей. Показатели классифицируются на основе объектов оценки (в том числе, сети, атак, атакующего, инцидентов, контрмер), этапов процесса оценки защищенности (проектирования и эксплуатации) и категорий показателей (базовые,

стоимостные пр.). Это позволяет получать оценку защищенности системы и выбирать защитные меры для выделенной группы показателей в зависимости от доступных входных данных.

Разработанная методика оценки защищенности на основе совместного применения графов атак и графов зависимостей сервисов выделяет несколько уровней оценки и определяет применяемые на каждом уровне модели, показатели и алгоритмы их вычисления, а также их взаимосвязи между разными уровнями. Уровни выделены в зависимости от используемых при оценке защищенности входных данных. В качестве входных данных применяются данных о сети и ее уязвимостях, атаках, зависимостях сервисов, атакующих, событиях, контрмерах, экспертных оценках уязвимостей и контрмер, и оценках из открытых баз данных. Алгоритмы различных уровней иерархически связаны между собой: выходные данные алгоритмов каждого предыдущего уровня используются в качестве входных данных алгоритмов следующего уровня. Это позволяет уточнять показатели за счет новых входных данных. 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.

Предложенная в работе методика выбора защитных мер отличается возможностью формирования комплекса защитных мер (контрмер) на основе доступных входных данных за счет применения иерархического комплекса показателей. Выделение этапов статического и динамического уровня позволяет на первом этапе выбрать набор средств защиты, реализующих в динамике контрмеры, позволяющие остановить развитие обнаруженных атак на основе анализа инцидентов безопасности. Совместное применение графов атак и зависимостей сервисов позволяет учитывать при выборе защитных мер влияние инцидентов безопасности на защищенность и влияние защитных мер на систему с точки зрения эффективности и побочного ущерба.

Разработанная архитектура и программная реализация системы оценки

защищенности и выбора защитных мер отличается наличием интерфейсов взаимодействия с системами мониторинга безопасности и управления инцидентами и применением оригинальных методик оценки защищенности и выбора защитных мер.

Таким образом, новизна диссертационной работы заключается в том, что предлагаемые методики позволяют совместно учитывать различные показатели защищенности и уточнять их с появлением новых данных в рамках систем мониторинга безопасности и управления инцидентами для адекватной оценки защищенности компьютерных сетей и эффективного реагирования на инциденты.

ДОСТОВЕРНОСТЬ, ОБОСНОВАННОСТЬ И НАУЧНАЯ ЗНАЧИМОСТЬ РЕЗУЛЬТАТОВ ДИССЕРТАЦИОННОГО ИССЛЕДОВАНИЯ

Достоверность и обоснованность результатов диссертационной работы подтверждается тщательным анализом разработанных методик и предшествующих исследований в области, согласованностью полученных экспериментах результатов, апробацией на ряде ведущих научных конференций, и публикацией в рецензируемых научных изданиях.

Основным научным достижением автора является разработка методик оценки и выбора защитных мер, основанных на комплексном учете показателей различных объектов оценки, применимых в разных режимах работы системы, и совместимых с системами мониторинга безопасности и управления инцидентами. Теоретические выводы исследования были экспериментально подтверждены с помощью разработанного программного прототипа.

Полученные результаты позволят повысить качество систем управления безопасностью организаций за счет постоянного отслеживания и пересчета показателей защищенности в соответствии с поступающими данными о событиях в системе и своевременного применения адекватных контрмер, и таким образом позволят снизить уровень возможных потерь организаций в результате компьютерных атак. Результаты исследования рекомендуется

использовать в рамках компонента принятия решений активно распространяющихся систем мониторинга безопасности и управления инцидентами в организациях, деятельность которых связана с использованием компьютерных сетей, критичных к требованиям безопасности, в том числе в организации ООО «Ароматы безопасности», организации ГК «Омега» и ЗАО «НПП ТЕЛДА» при разработке систем управления безопасностью, а также в СПб ГУТ и университете ИТМО при формировании программы подготовки специалистов в данной области. На применимость результатов исследования указывает то, что необходимость повышения уровня защищенности компьютерных сетей организаций разной направленности определена в стратегии развития информационного общества в Российской Федерации на 2014–2020 годы.

Научный уровень полученных результатов подтверждается актами о внедрении, полученными от координатора европейского проекта MASSIF, а также использованием в деятельности организаций ООО «Ароматы безопасности» и ГК «Омега», и в учебном процессе в СПБ ГУТ.

ХАРАКТЕРИСТИКА СОДЕРЖАНИЯ ДИССЕРТАЦИИ. ПОЛНОТА ОПУБЛИКОВАННОСТИ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Диссертационная работа состоит из введения, трех глав, заключения, списка литературы и 15 приложений. Объем работы составляет 163 страницы машинописного текста без учета приложений; включает 40 рисунков и 17 таблиц.

Тема диссертации, направленность проведенных исследований и полученных результатов соответствует п. 9 паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Содержание автореферата соответствует основным положениям работы. В нем изложены все основные результаты, выносимые на защиту, и дано достаточно полное представление о научно-практической значимости результатов исследования.

По теме диссертации опубликовано 9 статей в рецензируемых изданиях

из перечня ВАК, 12 статей – в изданиях, индексируемых в международных базах Scopus и Web Of Science, и 5 свидетельств о государственной регистрации программ для ЭВМ.

Основные результаты работы в достаточной мере докладывались и обсуждались на международных и всероссийских научных конференциях.

Полученные в диссертационной работе результаты рекомендуется использовать в организациях, деятельность которых связана с использованием компьютерных сетей, критичных к требованиям безопасности.

Представленная диссертационная работа не лишена недостатков, к которым следует отнести следующие:

описанный во второй главе комплекс показателей защищенности включает категорию показателей нулевого дня, однако, данная группа показателей не учитывается в предложенной методике;

при определении локальной вероятности атаки в рамках методики оценки защищенности соискатель основывается на показателе системы оценки уязвимостей CVSS *Exploitability*, при этом меняя значение коэффициента в исходной формуле без должной аргументации, в результате чего теряется физический смысл цифры 2, используемой в формуле расчета показателя: $p=2\times AV\times AC\times Au$;

одним из важных элементов методики оценки защищенности является определение критичности активов компьютерной сети, при этом соискателем учитываются сервисы компьютерной сети, зависимости между ними и веса этих зависимостей. Однако в работе не раскрыто, как именно определяются веса зависимостей между сервисами системы;

при описании архитектуры прототипа, реализующего предложенную методику, не раскрыты используемые интерфейсы взаимодействия с SIEM-системой, хотя этот аспект является существенным для понимания практической значимости заявленного исследования;

в работе не проводится оценка уровня доверия к входным данным из открытых источников, используемым в методике оценки защищенности, хотя

это является одним из важнейших аспектов.

Однако следует отметить, что вышеуказанные недостатки не снижают общую положительную оценку диссертационной работы.

ВЫВОДЫ

Диссертация Дойниковой Е.В. на соискание ученой степени кандидата технических наук является законченной научно-исследовательской работой, в которой решена актуальная и практически значимая научная задача – разработка модельно-методического аппарата для оценки защищенности компьютерных сетей и выбора защитных мер для систем мониторинга безопасности и управления инцидентами. Диссертационное исследование соответствует критериям, изложенным в п. 9 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемых к кандидатским диссертациям, а его автор Дойникова Елена Владимировна заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Отзыв ведущей организации был обсужден и одобрен на заседании секции №1 научно-технического совета АО «НИИ «Рубин» (протокол №8 от 21.04.2017 г.).

Отзыв составили:

Заместитель начальника центра специальных работ,
кандидат технических наук Д.А. Котенко

Главный конструктор комплексной безопасности
систем связи,
кандидат технических наук, доцент В.В. Таран