ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора ИВАНОВА Александра Юрьевича
на диссертационную работу ДОЙНИКОВОЙ Елены Владимировны
«Оценка защищенности и выбор защитных мер в компьютерных сетях
на основе графов атак и зависимостей сервисов»,
представленную на соискание ученой степени кандидата технических наук
по специальности 05.13.19 – методы и системы защиты информации,
информационная безопасность

АКТУАЛЬНОСТЬ ТЕМЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

В настоящее время существует объективная необходимость дальнейшего совершенствования методов, средств и технологий защищенности компьютерных сетей. Это вызвано, с одной стороны, значительным расширением пространства киберугроз, а с другой стороны – довольно большим числом уязвимостей узловой составляющей крупномасштабных сетей. Рациональное распределение усилий и ограниченных ресурсов, выделяемых на организацию системы защиты компьютерных сетей, невозможно без реализации научного подхода к решению проблемы обеспечения требуемого уровня их информационной безопасности. Такой подход подразумевает, в том числе, достоверную оценку защищенности компьютерных сетей и выработку адекватных мер их защиты.

Применяемые в настоящее время системы управления информацией о безопасности и текущих событиях (SIEM-системы) являются центральным звеном мониторинга информационной безопасности для большинства крупных сетей, однако они не в состоянии полноценно противодействовать информационным угрозам. Это объясняется рядом причин, в основном следующих. Во-первых, невысокой эффективностью при решении конкретной задачи, не предназначенной для какого-либо обобщения. Во-вторых, малой степенью гибкости, что требует их существенной модификации при использовании конкретным клиентом в определенных условиях: настройка правил вычисления корреляций между событиями, сопряжение с новыми источниками информации и т.д. Также можно назвать высокие требования к профессиональным знаниям и навыкам пользователей системы, трудности освоения, большое количество ложных извещений, хранение больших объемов информации.

В этом контексте представляется интересным и перспективным замысел автора диссертационной работы, направленный на теоретическое обоснование надстройки над SIEM-системами. Такой модельно-методический аппарат позволит всесторонне исследовать защищенность компьютерных сетей при реализации конкретных атак с учетом протекающих в сетях процессов, что служит основой формирования комплекса защитных мер, направленных на нейтрализацию атак или снижение ущерба от их реализации.

Этим в полной мере определяется своевременность и актуальной темы диссертационной работы и полученных в ней результатов.

АНАЛИЗ НАУЧНЫХ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

К числу основных научных результатов, выносимых на защиту, в диссертационной работе отнесены следующие.

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

2. Методика оценки защищенности компьютерных сетей 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 защищенности компьютерных сетей и выбора защитных мер на основе предложенных методик.

Первый результат включает в себя оригинальную классификацию показателей согласно объектам и категориям оценки, что дает ему полное право претендовать на научную новизну.

В свою очередь, основная новизна второго результата – методики оценки защищенности – заключается в интеграции разнородных показателей защищенности и алгоритмов их вычисления. Предложенные алгоритмы отличаются в зависимости от доступных входных данных и режимов работы системы. В рамках разработанной методики взаимосвязи между ними и условия их функционирования определены таким образом, чтобы от разрозненных исходных данных перейти к значимой, выраженной количественно оценке защищенности.

Предложенная методика выбора защитных мер (третий результат) отличается тем, что введенная модель контрмеры тесно связана с моделями оценки защищенности, в том числе моделью атак и зависимостей сервисов, позволяющими одновременно отследить влияние защитной меры на уровень защищенности системы и возможный побочный ущерб от негативного влияния на сервисы системы. Методика позволяет автоматизировать процесс оперативного реагирования на изменения в системе за счет выделения динамического режима работы и связи между моделью события и моделью атак, а также количественно оценить выигрыш от реализации доступных защитных мер для снижения риска до приемлемого уровня и с приемлемым уровнем затрат.

Четвертый результат – архитектура и программная реализация системы защищенности компьютерных сетей и выбора защитных мер на основе предложенных методик – характеризуется ярко выраженной практической направленностью. Новизна этого результата состоит в реализации разработанных автором методик количественной оценки защищенности и выбора контрмер. Проведенные эксперименты подтверждают, что выносимые на защиту методики позволяют снизить потери организации в случае компьютерных атак и удовлетворяют заявленным требованиям.

ОБОСНОВАННОСТЬ НАУЧНЫХ ПОЛОЖЕНИЙ И ВЫВОДОВ

Обоснованность и достоверность полученных автором результатов подтверждаются строгой аргументацией основных положений и выводов, теоретическим анализом разработанных алгоритмов, экспериментальным исследованием алгоритмов, моделей и методик, сравнительным анализом предложенных методик с существующими аналогами, а также доказательным и корректным использованием апробированных методов исследований.

Кроме того, достоверность научных результатов подтверждается довольно полной апробацией и публикацией основных положений диссертации.

ТЕОРЕТИЧЕСКАЯ И ПРАКТИЧЕСКАЯ ЗНАЧИМОСТЬ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Теоретическая значимость результатов работы связана как с введением новой классификации показателей защищенности, так и с синтезом ориги-

нальных методик оценки защищенности и выбора контрмер, развивающих существующие теоретические результаты в данной области.

Практическая значимость результатов вытекает из актуальности темы исследования и связана с существующей необходимостью в предоставлении организациям инструмента адекватной оценки риска и рационального выбора контрмер. Кроме того, представлен интересный практический результат применения опыта мирового сообщества по созданию ряда стандартов и источников данных безопасности в рамках реального прототипа оценки защищенности и выбора защитных мер.

Общая значимость результатов также подтверждается внедрением в деятельность организаций ряда организаций (ООО «Ароматы безопасности», ГК «Омега») и в учебный процесс одного из ведущих ВУЗов в области инфотелекоммуникаций (СПб ГУТ), а также их применением в рамках проекта Европейского Сообщества MASSIF (№ 257475).

ОЦЕНКА СОДЕРЖАНИЯ ДИССЕРТАЦИИ И ЕЕ НЕДОСТАТКИ

Диссертация состоит из введения, трех глав, заключения и приложений. Она написана строгим научным языком, ее материал в полном объеме соответствует цели и научным задачам диссертационного исследования.

Автореферат концентрирует сущность диссертации и дает полное представление о ее содержании, несмотря на имеющийся дисбаланс объема излагаемого материала по главам диссертации. Количество публикаций по теме диссертации соответствует установленным критериям, а изложенный в них материал отражает научные результаты исследования.

Вместе с этим в диссертации имеются отдельные недостатки, а именно:

1. В первой главе довольно развернуто проанализированы многочисленные исследования в области оценки защищенности и выбора контрмер, но практически не описываются существующие коммерческие инструменты, реализующие (или частично реализующие) схожую функциональность, например, MaxPatrol SIEM от компании Positive Technologies, CAULDRON от компании CyVision и SecurITree от компании Amenaza Technologies.

2. При оценке защищенности и выборе контрмер в явном виде не учитывается время, необходимое для реализации атак и защитных мер, хотя это один из ключевых аспектов при реагировании на инциденты безопасности.

3. Интерфейсы взаимодействия системы мониторинга безопасности и управления инцидентами и разработанного компонента представлены в недостаточной степени. Их следовало бы рассмотреть подробнее, так как данная система является старшей по отношению к компоненту, реализующему разработанные методики.

4. Определение списка возможных контрмер, их эффективности и стоимости возлагается на экспертов. Этот вопрос является существенным при выборе контрмер, поэтому для полноты описания методики ему следовало уделить большее внимание.

5. Кроме того, в работе есть некоторые неточности, в числе которых следующие. В списке литературы и электронных ресурсов дата обращения к некоторым ссылкам слишком давняя (2015 г.). На странице 82 диссертации отмечено, что описанные показатели измеряются в процентах, однако, судя по формулам, показатели измеряются в долях. Там же на странице 83 не указана шкала для измерения показателя сложности атаки.

Названные недостатки носят частный характер и в целом не влияют на значимость и ценность полученных научных результатов, их новизну, обоснованность и достоверность.

ЗАКЛЮЧЕНИЕ

1. Диссертация Дойниковой Е.В. представляет собой единолично написанную автором научно-квалификационную работу, в которой содержится решение задачи разработки методик, моделей и алгоритмов оценки защищённости компьютерных сетей и выбора защитных мер для SIEM-систем, имеющей значение для развития теории и практики информационной безопасности. Область исследования соответствует паспорту специальности 05.13.19 – методы и системы защиты информации, информационная безопасность.

2. Результаты диссертационного исследования отвечают критериям пункта 9 Положения о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемым к кандидатским диссертациям.

3. Дойникова Елена Владимировна заслуживает присуждения ей ученой степени кандидата технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
Профессор кафедры специальных информационных технологий
Федерального государственного казенного образовательного учреждения
высшего образования «Санкт-Петербургский университет Министерства
внутренних дел Российской Федерации»
доктор технических наук,
профессор Иванов Александр Юрьевич

«28» апреля 2017 года

Сведения о составителе отзыва:
ФИО: Иванов Александр Юрьевич
Ученая степень: доктор технических наук
Ученое звание: профессор
Место работы: Федеральное государственное казенное образовательное учреждение высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»
Должность: профессор кафедры специальных информационных технологий
Почтовый адрес: ул. Летчика Пилютова, д. 1, г. Санкт-Петербург, 198206.
Телефон: (921) 7578239
Адрес электронной почты: alexandr.y@mail.ru