Экз. № 1

ОТЗЫВ

официального оппонента на диссертацию Дойниковой Елены Владимировны, выполненную на тему «Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов» и представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»

1. Актуальность темы диссертации

В современных компьютерных сетях постоянно генерируется большое число разнородных событий, формируемых преимущественно, в результате взаимодействия программ, функционирующих на различных логических уровнях. Автоматизированное выявление событий приводящих к изменению безопасного состояния компьютерной сети и своевременное реагирование на возможные вредоносные последствия, возможно только при оперативной обработке большого массива регистрируемых и накапливаемых данных. Регистрируемые события характеризуются не всегда предсказуемой динамикой изменения контролируемых параметров, разнородностью и разноуровневым представлением накапливаемых данных. Используемые на практике системы (SIEM-системы) обычно реализуют относительно простые методики оценки защищенности, не учитывая такие аспекты безопасности, как вектор атаки, его адаптивность к контрмерам или влияние возможных контрмер на работоспособность сети. Выбор защитных мер остаётся на усмотрение оператора системы, что требует высокой квалификации оператора, а также повышает стоимость ошибки за неправильно принятое решение.

Таким образом, разработка новых компонентов SIEM-систем, позволяющих автоматизировать процесс получения комплексной оценки защищенности и выбор контрмер с поддержанием компьютерных сетей в работоспособном и безопасном состоянии, является актуальной и своевременной научно-технической задачей требующей своего решения, чему и посвящены диссертационные исследования выполненные соискателем.

2. Обоснованность научных положений, выводов и рекомендаций сформулированных в диссертации, их достоверность и новизна

К основным научным результатам, определяющим новизну и значимость представленной диссертационной работы, можно отнести следующие результаты:

– оригинальный комплекс показателей защищенности, объединяющий как уже существующие, так и предложенные автором показатели. Комплекс

отличается от существующих иерархической классификацией показателей защищенности на основе объектов оценки и тем, что каждая отдельная группа показателей позволяет получить интегральную оценку защищенности системы и выбрать защитные меры. Отмечаю, что соискателем, впервые предложено выделение внутри каждой группы показателей отдельных категорий: базовые, стоимостные и показатели нулевого дня, что позволяет оперативнее и точнее принимать решение при оценке защищенности и в последующем реализовать автоматизированное ситуационное управление при выработке контрмер.

– методика оценки защищенности. Методика объединяет ряд показателей, моделей и алгоритмов, и отличается от аналогов тем, что позволяет получить адекватную оценку защищенности с разной степенью точности в зависимости от доступных входных данных в разных режимах функционирования анализируемой системы. Впервые в рамках предложенной методики применяются в комплексе различные аналитические модели объектов оценки, которые в известных исследованиях используются отдельно. Так, предложена связь модели атак и модели зависимостей сервисов системы через их уязвимости, модели атак и модели события – через последствия эксплуатации уязвимостей, модели зависимостей сервисов и модели события – через скомпрометированный сервис. Для определения конкретных значений параметров моделей и расчета показателей защищенности используются открытые стандарты и базы данных, содержащие, в том числе, экспертные оценки уязвимостей. В частности, в работе введены новые метрики вычисления ряда показателей на основе указанных оценок. Предложенные алгоритмы и формулы вычисления показателей учитывают особенности взаимосвязанных моделей, отличаются в зависимости от используемых при вычислениях данных, и позволяют уточнять оценку защищенности при поступлении новых данных.

– методика выбора защитных мер, которая позволяет не только снизить риск до приемлемого уровня на этапе проектирования системы, но и своевременно реагировать на изменяющуюся ситуацию по защищенности при эксплуатации системы, и выбирать эффективные контрмеры в зависимости от текущего состояния по защищенности. Основной особенностью разработанной методики, отличающей ее от аналогов, является лежащий в ее основе, так называемый “any-time” подход, позволяющий при необходимости принимать решение на основе доступных входных данных, или уточнять его при получении новых данных. Впервые введённые соискателем связи между моделями контрмер, атак и зависимостей сервисов системы позволяют, с одной стороны, определить эффективность контрмеры, с точки зрения предотвращения развития атаки, а с другой стороны, определить влияние контрмеры на функционирование системы. Таким образом, методика

позволяет выбрать контрмеры, оптимальные с точки зрения выигрыша по стоимости.

– теоретические положения работы подтверждены компьютерными экспериментами с программным прототипом, в рамках которого впервые реализованы предложенные методики, модели и алгоритмы.

Достоверность и обоснованность результатов работы подтверждается:

– корректностью предложенных аналитических и концептуальных моделей, методик и алгоритмов, теоретической оценкой их качества;

– результатами экспериментов, проведенных с использованием разработанного программного прототипа;

– положительными результатами внедрения основных результатов исследования в практику;

– детальным сравнением с существующими исследованиями в области оценки защищенности и выбора контрмер;

– апробацией основных теоретических результатов работы на ведущих российских и международных конференциях, и в рецензируемых печатных трудах.

3. **Практическая значимость результатов исследования и рекомендации по их использованию**

Результаты исследования, реализованные в форме программного прототипа, могут применяться для управления безопасностью компьютерных сетей организаций, а также использоваться в качестве компонента перспективных систем мониторинга безопасности и управления инцидентами для поддержки принятия решений по реагированию. Теоретические результаты исследования могут применяться при разработке систем мониторинга и управления безопасностью для повышения эффективности управления безопасностью, что подтверждается представленными актами о реализации и участием в тематических проектах.

4. **Оценка содержания диссертационной работы**

Диссертационная работа включает 163 страницы машинописного текста и состоит из введения, трех глав, заключения, списка литературы и 15 приложений, написана самостоятельно с корректными ссылками по тексту на источники. Оформление диссертации соответствует предъявляемым требованиям. Содержание автореферата диссертации соответствует содержанию диссертации. Диссертационная работа написана научным языком, хорошо структурирована и представляет собой законченную научно-квалификационную работу.

Содержание диссертации соответствует пункту 9 «Модели и методы оценки защищенности информации и информационной безопасности объекта» паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

5. Замечания по диссертационной работе

1. В явном виде не обосновывается обобщённая структура и полнота элементов комплекса показателей защищенности. Не понятно, сколько таких показателей еще необходимо разработать, чтобы достигнуть максимально точной оценки защищенности и сколько их всего может быть?

2. Предложенная в работе методика учитывает уязвимости программного и аппаратного обеспечения из открытых источников, при этом в работе не рассматриваются специализированные системы, уязвимости которых невозможно найти в открытых источниках информации.

3. В диссертации не поясняется выбор методик для сравнения с предложенной методикой оценивания защищенности по показателям обоснованности.

4. В методике оценки защищенности и выбора контрмер, соискатель не обоснованно ограничился рассмотрением только атак связанных с эксплуатацией уязвимостей программно-аппаратного обеспечения, однако, существуют и другие виды атак (атаки, связанные со сканированием сети, с подбором пароля, и другие).

5. В диссертации описано проведение экспериментов для сетей размером 10, 20 и 40 хостов с фиксированной топологией сети для расчета показателей обоснованности. Указанное ограничение размера и вида анализируемой компьютерной сети для расчета показателей не обосновано, так как реальные сети обычно имеют больший размер и комбинированный характер построения.

Отмеченные выше недостатки принципиально не влияют на полученные автором в диссертационной работе научные результаты и не снижают ее ценности.

6. Выводы

Диссертационная работа Дойниковой Е.В. является законченной научно-квалификационной работой, обладает новизной и практической значимостью полученных результатов. В работе автором решена задача разработки модельно-методического аппарата для оценки защищенности компьютерных сетей и выбора защитных мер для систем мониторинга безопасности и управления инцидентами, значимая для организаций, чья деятельность

зависит от защищенности компьютерных сетей и развития сетевой инфраструктуры.

Диссертация выполнена единолично, содержит совокупность новых научных результатов и положений, выдвигаемых автором для публичной защиты, имеет внутреннее единство и свидетельствует о личном вкладе автора в науку.

По научному содержанию, глубине и полноте выполненных исследований, а также значимости и ценности полученных результатов, выводов и рекомендаций диссертация соответствует критериям пунктов п. 9, 10 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, предъявляемым к диссертационным работам, представленным на соискание ученой степени кандидата технических наук, а её автор Дойникова Елена Владимировна, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент
Профессор кафедры Систем сбора и обработки информации
197198, г. Санкт-Петербург, ул. Ждановская, д. 13, тел. (812) 347-96-87, e-mail: novikov1978@ya.ru

Новиков Владимир Александрович

Подпись официального оппонента профессора кафедры Систем сбора и обработки информации доктора технических наук, Военно-космической академии имени А.Ф.Можайского Новикова Владимира Александровича удостоверяю

Ученый секретарь специального
диссертационного совета ДС 215.013.08
кандидат технических наук, профессор

Медведев Владимир Михайлович