ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертацию Новохрестова Алексея Константиновича «Модель угроз информационной безопасности программного обеспечения компьютерных сетей на основе атрибутивных метаграфов», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертации

Несмотря на то, что в настоящее время специалистами коммерческих и государственных учреждений, а также учеными, занимающимися вопросами обеспечения информационной безопасности, уделяется большое внимание противодействию сетевым атакам и защите информации, обрабатываемой в компьютерных сетях, количество успешных атак на информационные системы продолжает увеличиваться. Во многом это обусловлено тем, что при обеспечении безопасности компьютерных сетей специалисты по защите информации руководствуются только личным опытом. Так, уже на одном из самых ранних этапов обеспечения безопасности систем – на этапе определения существующих угроз специалисту приходится опираться на множество различных подходов к классификации и идентификации угроз, которые часто противоречат друг другу.

Работа Новохрестова А.К. посвящена решению проблемы составления максимально полного перечня угроз безопасности компьютерной и снижению влияния личного опыта специалиста, осуществляющего идентификацию угроз, что несомненно имеет существенное значение для решения задач информационной безопасности. Таким образом, тема диссертации Новохрестова А.К. является актуальной.

Структура и содержание диссертации

Диссертационная работа Новохреста А.К. состоит из введения, трех глав, заключения, списка источников и 1 приложения. Общий объем диссертационной работы: 114 страниц, в том числе 14 таблиц и 14 рисунков.

Во введении автором обоснована актуальность темы исследования, поставлены цель и задачи, приведены научная новизна, практическая и теоретическая значимость полученных результатов, а также положения, выносимые на защиту.

В первой главе приведен обор современного состояния предметной области. Приведены недостатки существующих подходов, на устранение которых направлено диссертационное исследование.

Вторая глава посвящена описанию разработанных Новохрестовым А.К. модели компьютерной сети, модели угроз информационной безопасности компьютерной сети с подходом к классификации угроз, методики определения перечня угроз, использующей разработанные модели.

В третьей главе автор приводит сравнение разработанной модели угроз с банком данных угроз ФСТЭК России, а также описывает внедрение результатов работы в процессе работы над автоматизированной системой коммерческого учета энергоресурсов.

В конце каждой главы и в заключении к работе автором сделаны обобщающие выводы, позволяющие составить более полное системное представление о полученных результатах.

Список источников включает 118 позиций, в том числе нормативные правовые акты, методические и научные труды российских и зарубежных ученых, интернет-ресурсы по профилю исследования.

В приложение вынесены акты внедрения диссертационной работы (акт о внедрении в деятельность АО «ПКК Миландр» и акт о внедрении в учебный процесс ФГБОУ ВО «ТУСУР»).

Оформление диссертации и автореферата не вызывает нареканий и соответствует требованиям ГОСТ Р 7.0.11-2011.

Научная новизна полученных результатов

Соискателем получены следующие новые научные результаты:

1. Предложена модель компьютерной сети, основанная на атрибутивных метаграфах, отличающаяся наличием связей между различными уровнями программного обеспечения компьютерных систем.

2. Предложена модель угроз информационной безопасности компьютерных сетей, отличающаяся формированием типов угроз на основе элементарных операций над метаграфами.

3. Разработана новая методика составления перечня угроз информационной безопасности компьютерных сетей, отличающаяся от аналогов использованием матрицы взаимосвязей между элементами.

Теоретическое и практическое значение результатов работы

Теоретическая значимость результатов исследования заключается во вкладе автора в совершенствование научно-методической базы для унификации процессов составления перечней угроз компьютерных сетей в частности и информационных систем в общем. Разработанные автором модели и методика могут использоваться как основа для разработки

автоматизированного средства составления перечней угроз информационных систем.

Практическая значимость полученных результатов не вызывает сомнений и состоит в том, что применение предложенных автором моделей и методики позволяет увеличить количество идентифицируемых угроз при составлении моделей угроз для информационных систем, а также снизить требования к квалификации специалистов, осуществляющих составление перечней угроз безопасности компьютерных сетей за счет формализации процесса.

Значимость результатов диссертационного исследования подтверждена актом внедрения в практическую деятельность АО «ПКК Миландр» в процессе работы над автоматизированной системой коммерческого учета энергоресурсов, а также актом внедрения в учебный процесс ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники».

Обоснованность и достоверность полученных результатов и выводов

Автором адекватно использованы формальные методы дискретной математики (теория множеств и теория графов), системного анализа и теории защиты информации, сделаны корректные выводы на основе полученных данных.

Достоверность результатов подтверждается положительным эффектом от внедрения научных исследований в работу действующего предприятия и сравнением авторского перечня типов угроз с угрозами из банка данных ФСТЭК России.

Пункты научной новизны, положения, выносимые на защиту, и выводы хорошо аргументированы, корректны, подтверждаются внедрением.

Рекомендации по использованию результатов работы

Результаты диссертационной работы Новохрестова А.К. могут быть применены:

– при определении угроз безопасности системы в процессе аудита информационной безопасности или в процессе проектирования (модернизации) системы защиты компьютерных сетей;

– при разработке программного средства для помощи специалисту по защите информации при определении угроз безопасности компьютерных сетей;

– при обучении и повышении квалификации специалистов по защите информации.

Публикации и апробация материалов диссертации

По материалам диссертации Новохрестовым А.К. опубликовано 16 научных работ, в том числе 2 работы в изданиях, рекомендованных ВАК РФ, и 1 работа в материалах конференции, индексируемых в базе данных Scopus. Знакомство с отдельными публикациями соискателя свидетельствует о том, что в них достаточно полно отражены результаты диссертационного исследования.

Замечания к работе

1. Среди выделенных автором недостатков известных моделей угроз приводится отсутствие системности. В пояснении значатся термины «обобщенная угроза» и «частная угроза», однако в существующих нормативных документах они отсутствуют. Хотя из контекста понятно, что имеется ввиду автором, определений в тексте диссертации не приводится.

2. Недостаточно внимания уделено еще одному недостатку, выделяемому автором – присутствию в моделях угроз элементов модели нарушителя. Согласно существующим нормативным документам учет источника угрозы является неотъемлемой частью процесса построения модели угроз.

3. Было бы полезно наличие в тексте работы единого сквозного примера, иллюстрирующего применение разработанных автором моделей и методики.

Общая оценка диссертации

Отмеченные выше замечания хотя и несколько снижают впечатление от диссертации, но не подвергают сомнению основные научные результаты автора, их научную новизну и значимость. Таким образом общая оценка работы остается положительной.

Диссертация Новохрестова А.К. является завершенной научно-квалификационной работой, в которой содержится решение актуальной научно-технической задачи – увеличения полноты перечня угроз информационной безопасности компьютерных сетей. Диссертация соответствует пунктам 3 и 15 паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Содержание работы хорошо структурировано, повествование построено последовательно и логично, графическое оформление – аккуратно. Автореферат соответствует основному содержанию диссертации. Работа

обладает необходимыми признаками научной новизны, теоретической и практической значимостью. Основные результаты диссертации опубликованы в изданиях из перечня ВАК Российской Федерации, представлены в материалах конференций различного уровня.

По актуальности, научной новизне полученных результатов, объему выполненных исследований, практической и теоретической значимости представленная работа соответствует требованиям пункта 9 «Положения о порядке присуждении ученых степеней» ВАК Российской Федерации, утвержденного постановлением Правительства Российской Федерации №842 от 24.09.2013 г., предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор, Новохрестов Алексей Константинович, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Официальный оппонент _____ / Новиков Сергей Николаевич

доктор технических наук (специальность 05.13.19), доцент, заведующий кафедрой безопасности и управления в телекоммуникациях

ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики»
630102, г. Новосибирск, ул. Кирова, д. 86
Телефон: 8-913-923-72-34
E-mail: snovikov@ngs.ru

27 ноября 2018 г.

Подпись Новикова С.Н. заверяю:

Начальник отдела
кадров ОПУ
Конева Г.Н.