УТВЕРЖДАЮ
Ректор ФГБОУ ВО «Уфимский государственный авиационный технический университет»
_____ Н.К. Криони
«5» 12 2018 г.

ОТЗЫВ

ведущей организации на диссертацию Новохрестова Алексея Константиновича на тему «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

1. Актуальность темы диссертации

Определение перечня актуальных угроз является неотъемлемым этапом процесса обеспечения безопасности информационных систем. Причем до определения актуальности необходимо составить перечень угроз, включающий все существующие угрозы безопасности рассматриваемой системы, т.е. осуществить идентификацию угроз. При этом существенное влияние на перечень угроз оказывает квалификация и субъективное мнение специалистов, выполняющих их идентификацию.

В данном контексте видится актуальной разработка методики составления перечня угроз информационной безопасности информационных систем, при использовании которой влияние профессионального уровня и субъективного мнения эксперта будет минимизировано.

Указанное обуславливает актуальность темы диссертационного исследования Новохрестова А.К. В качестве цели исследования автором обозначено повышение объективности составления перечня угроз информационной безопасности компьютерных сетей.

2. Структура и объем диссертации

Объем диссертационной работы составляет 114 страниц машинописного текста, в том числе 14 таблиц, 14 рисунков и список литературы, состоящий из 108 наименований. Диссертация содержит введение, три главы, заключение, список источников и одно приложение.

Во введении обоснована актуальность темы диссертационного исследования, сформулированы цель и задачи, объект и предмет исследования, отражены его научная новизна, практическая и теоретическая значимость, приведены положения, выносимые на защиту, и информация об апробации и внедрении результатов работы.

Первая глава посвящена исследованию современного состояния предметной области. Рассматриваются подходы к построению моделей компьютерных сетей, применяемые при идентификации угроз и оценке защищенности, а также подходы к описанию, идентификации угроз и построению моделей угроз для информационных систем и, в частности, компьютерных сетей. Выделяются недостатки существующих решений, требующие устранения. В качестве ключевого недостатка приводится отсутствие разделения угроз на угрозы системе и информации.

Во второй главе автором с учетом выделенных в первой главе недостатков предлагается модель компьютерной сети и модель угроз информационной безопасности компьютерной сети в совокупности с подходом к классификации угроз, основанные на атрибутивных метаграфах. Также описывается методика определения перечня угроз, использующая разработанные модели.

В третьей главе изложено сравнение с аналогом и внедрение результатов работы, описанных во второй главе. Сравнение разработанной модели угроз производится с наиболее полным аналогом, существующим на данный момент и применяемым на практике – банком данных угроз ФСТЭК России. Внедрение методики составления перечня угроз и моделей осуществлялось при разработке автоматизированной системы коммерческого учета энергоресурсов.

В заключении приведены основные результаты и выводы по проделанной работе.

Стиль изложения работы соответствует требованиям к научным работам. Ссылки на библиографические источники и литературу, включая собственные публикации автора, оформлены в соответствии с требованиями.

3. Научная новизна исследования и полученных результатов

Полученные результаты диссертационного исследования являются новыми и могут быть классифицированы как изложение научно-обоснованных решений, внедрение которых внесет вклад в науку и обеспечение безопасности Российской Федерации, в частности в практику составления перечней угроз компьютерных сетей и информационных систем в общем.

Наиболее важные результаты диссертационной работы, обладающие признаками научной новизны:

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.

4. Обоснованность и достоверность полученных результатов

Цель диссертационного исследования и вытекающие из нее задачи изложены корректно, являются практически значимыми и реализуемыми. Решения задач исследования доведены до практических приложений. По приведенному списку литературы можно судить о полноте изучения соискателем рассматриваемых вопросов.

Достоверность полученных в работе результатов обеспечивается строгостью применения методов теории множеств, системного анализа, теории защиты информации и теории графов и подтверждается положительным эффектом, полученным в результате внедрения в практическую деятельность действующего предприятия, о чем свидетельствует соответствующий акт о внедрении.

5. Значимость результатов диссертации для соответствующей отрасли науки

Результаты диссертационной работы Новохрестова А.К. используются в учебном процессе и научно-исследовательской деятельности студентов Томского государственного университета систем управления и радиоэлектроники. Конкретно значимость полученных результатов заключается в следующем:

1. Применительно к разработке модели угроз информационной безопасности компьютерной сети результативно использован математический аппарат теории графов для моделирования компьютерных сетей.

2. Изучена связь между типами угроз и базовыми операциями над метаграфами.

3. Представлены методические рекомендации по формированию перечня угроз, направленных на нарушение конфиденциальности и целостности информационной системы.

4. Разработана и внедрена методика составления перечня угроз информационной безопасности, использующая разработанные модели компьютерной сети и угроз. Внедрение методики позволило при применении к разрабатываемой системе коммерческого учета энергоресурсов обнаружить на 18% больше угроз, чем ранее было обнаружено экспертами.

6. Рекомендации по использованию результатов диссертационной работы

Предприятиям и организациям, занимающимся анализом защищенности, построением и сопровождением систем защиты компьютерных сетей – использовать предложенные автором модели и методику для определения перечней угроз безопасности защищаемых систем.

Высшим учебным заведениям, осуществляющим подготовку кадров по защите информации – использовать результаты настоящей работы в учебном процессе при чтении курсов лекций и проведении лабораторных и практических работ по дисциплинам «Моделирование автоматизированных информационных систем», «Безопасность сетей ЭВМ» и «Управление информационной безопасностью».

В качестве возможного продолжения и развития исследований, выполненных в диссертации, рекомендуется расширение предложенного автором подхода и создание обобщенной модели угроз системе и информации, а также программная реализация методики для создания программного инструмента построения моделей угроз.

7. Публикации, апробация и внедрение результатов работы

Научные и практические результаты диссертационной работы докладывались и обсуждались на семинарах и 13 конференциях различного уровня, в том числе всероссийского и международного. Материалы исследования отражены в 16 научных публикациях, в том числе 2 работах в изданиях, рекомендованных ВАК Российской Федерации.

Результаты диссертационной работы внедрены в деятельность АО «ПКК Миландр» в процессе реализации комплексного проекта по созданию высокотехнологичного производства интеллектуальных приборов энергоучета, разработанных и изготовленных на базе отечественных микроэлектронных компонентов, и гетерогенной автоматизированной системы мониторинга потребляемых энергоресурсов на их основе. Также результаты работы внедрены в учебный процесс Томского государственного университета систем управления и радиоэлектроники.

8. Замечания по диссертации

1. Обзор моделей информационной системы, приведенный в диссертации, неполный. Отсутствует информация – для решения каких задач эти модели использовались. В работе отсутствуют обзоры моделей зарубежных авторов.

2. Автор предлагает модель компьютерной сети, основанной на метаграфах, однако, не указаны возможные размеры этого графа для реальной компьютерной сети. Отсутствует оценка трудоемкости операций на этом графе.

3. Представленная методика составления перечня угроз информационной безопасности компьютерных сетей не алгоритмизирована. Из диссертации не ясно как ей пользоваться для произвольных информационных систем и насколько это трудоемко.

4. В диссертации не указано, какими средствами защиты информации надо устранять выявленные угрозы. Если для их устранения потребуется добавить в систему новые программные компоненты, то это может привести к возникновению новых угроз.

Данные замечания не снижают общей положительной оценки диссертации и значимости полученных научно-практических результатов.

9. Заключение о соответствии диссертации критериям, установленным Положением о порядке присуждения ученых степеней

Диссертация Новохрестова А.К. является законченной научно-квалификационной работой, в которой на основании выполненных автором исследований решена научно-техническая задача, имеющая важное хозяйственное значение. Полученные результаты вносят определенный вклад в развитие таких областей информационной безопасности, как методы и модели идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса, а также модели и методы управления информационной безопасностью.

Диссертация отвечает требованиям п.9 «Положения о присуждении ученых степеней» ВАК Российской Федерации, предъявляемых к диссертациям на соискание ученой степени кандидата технических наук, а ее автор, Новохрестов Алексей Константинович, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв ведущей организации на диссертацию Новохрестова А.К. рассмотрен и одобрен на заседании кафедры вычислительной техники и

защиты информации Уфимского государственного авиационного технического университета (протокол № 7 от «22» ноября 2018 г.)

Отзыв подготовлен заведующим кафедрой вычислительной техники и защиты информации Уфимского государственного авиационного технического университета доктором физико-математических наук, профессором Картаком Вадимом Михайловичем.

Специальность д.ф.-м.н., профессора Картака В.М.:

05.13.01 – Системный анализ, управление и обработка информации (в промышленности).

Заведующий кафедрой
вычислительной техники
и защиты информации
ФГБОУ ВО «Уфимский государственный
авиационный технический
университет»,
д.ф.-м.н., профессор Картак Вадим Михайлович

« 5 » декабря 2018 г.

450008, г. Уфа, ул. К.Маркса, 12, корп. 5
Тел.: (347)273-06-72
E-mail: vtizi@ugatu.su