ОТЗЫВ

официального оппонента, к.т.н., доцента Ложникова Павла Сергеевича 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»

1 Актуальность работы

Диссертационная работа направлена на решение научно-технической задачи повышения эффективности обеспечения информационной безопасности (ИБ) в системах и сетях телекоммуникаций за счет построения новых моделей угроз ИБ на основе атрибутивных метаграфов.

Складывающаяся в Российской Федерации организационно-правовая конъюнктура, а также все возрастающее влияние глобальной информационной инфраструктуры, являющейся благоприятной средой для осуществления разного рода угроз ИБ, подталкивает руководство организаций и предприятий более внимательно относится к вопросам противодействия сетевым атакам и защите информации. При этом, согласно исследованиям, количество успешно реализованных атак на компьютерные сети организаций не только не уменьшается, но и растет. В работе автор указывает, что одним из важнейших этапов обеспечения безопасности информационных систем является составление перечня угроз ИБ, с чем нельзя не согласиться. Результат применения существующих подходов, описанных в нормативных документах и научных работах, во многом зависит от квалификации и субъективного мнения специалиста.

В качестве цели работы Новохрестова А.К. значится повышение объективности составления перечня угроз ИБ и поиск подхода к составлению максимально полного перечня угроз ИБ. Направленность на решение задачи, имеющей существенное значение в области ИБ, позволяет классифицировать тематику рассматриваемой диссертации как актуальную.

2 Структура и содержание диссертации

Диссертационная работа Новохрестова А.К. содержит введение, три главы, заключение, одно приложение и список источников из 118

наименований. Объем диссертационной работы составляет 114 страниц, включая 14 таблиц и 14 рисунков.

Оформление и структура диссертации соответствует ГОСТ Р 7.0.11-2011. Содержание автореферата соответствует основным идеям, результатам, выводам и положениям диссертации.

Во введении автор обосновывает актуальность темы диссертации, обозначает цель и задачи исследования, приводит научную новизну, практическую и теоретическую значимость полученных результатов, положения, выносимые на защиту.

В первой главе кратко описаны существующие аналоги. Обзор разделен на две части – подходы к построению моделей компьютерных сетей и подходы к составлению перечней угроз. В выводах по главе приводится обобщенный перечень недостатков описанных подходов.

Во второй главе представлено описание авторских моделей: модели компьютерной сети, построенной с помощью математического аппарата атрибутивных метаграфов; модели угроз ИБ компьютерных сетей, основанной на элементарных операциях над метаграфами. Также описывается методика составления перечня угроз, элементами которой являются упомянутые модели.

В третьей главе описано сравнение и внедрение. В сравнении автор показывает преимущество разработанной им модели угроз над банком данных угроз ФСТЭК России. Основным критерием сравнение является полнота перечней угроз. Внедрение осуществлялось в процессе разработки автоматизированной системы коммерческого учета энергоресурсов.

В заключении приведены основные выводы и результаты диссертационного исследования.

3 Новизна полученных результатов

Результатами диссертации, обладающими признаками научной новизны, являются:

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

2) Модель угроз ИБ компьютерных сетей, отличающаяся формированием типов угроз на основе элементарных операций над метаграфами.

3) Методика составления перечня угроз ИБ компьютерных сетей, отличающаяся от аналогов использованием матрицы взаимосвязей между элементами.

4 Практическая и теоретическая ценность и внедрение результатов

Практическая значимость полученных автором результатов заключается в увеличении количества обнаруживаемых угроз ИБ и снижении влияния субъективного мнения специалиста при составлении моделей угроз компьютерных сетей. Значимость результатов работы подтверждена актом внедрения в деятельность АО «ПКК Миландр»: внедрение методики позволило при применении к разрабатываемой системе коммерческого учета энергоресурсов обнаружить на 18% больше угроз, чем ранее было обнаружено экспертами.

Теоретическая значимость результатов диссертационного исследования заключается в результативном использовании математического аппарата теории графов для моделирования угроз ИБ компьютерных сетей, что послужило основой для создания методики составления перечня угроз ИБ компьютерных сетей. Теоретические результаты используются в учебном процессе Томского государственного университета систем управления и радиоэлектроники, что подтверждается актом внедрения.

5 Достоверность и обоснованность основных результатов и выводов

Достоверность результатов и выводов подтверждается положительным эффектом от внедрения результатов исследований в работу действующего предприятия, корректным использованием методов теории защиты информации, теории графов, теории множеств и системного анализа.

6 Рекомендации по использованию результатов работы

Результаты диссертационного исследования рекомендуются к применению на практике специалистами по защите информации при построении моделей угроз компьютерных сетей.

В качестве рекомендации для дальнейшего развития исследований можно предложить расширение авторского подхода на угрозы безопасности информации, а не только угрозы безопасности системы.

7 Публикации по теме диссертации

Результаты диссертации опубликованы в 16 научных работах, 2 из которых в изданиях из списка ВАК РФ, представлены на конференциях различного уровня, в том числе всероссийского и международного.

8 Замечания по диссертации

1) Увеличение полноты перечня угроз ИБ, которое обозначено автором в заключении, подтверждается сравнением с банком данных угроз ФСТЭК России. Однако, в работе не раскрывается понятие полноты перечня угроз ИБ, и отсутствуют какие-либо выводы о полноте авторской модели угроз.

2) В тексте диссертации нет примера (или примеров) описания компьютерной сети с помощью авторской модели. В третьей главе автор приводит модель АСКУЭ, отмечая при этом, что рассматривает не 3 выделенных уровня программного обеспечения компьютерной сети, а только 2 – программный и аппаратный. Таким образом, пример, который бы демонстрировал применение разработанной автором модели, отсутствует.

3) Ограничение на применение моделей только к программному обеспечению, обозначенное автором, выглядит не обоснованным. По факту в работе описано применение моделей к АСКУЭ на программном и аппаратном уровне.

4) В рамках авторской модели угроз не рассматриваются способы реализации и источники угроз, что требует дополнительных пояснений. Согласно ГОСТ Р 53114-2008 угроза характеризуется наличием объекта угрозы, источника угрозы и проявления угрозы.

5) В тексте диссертации встречаются опечатки. Так на странице 71 пропущено слово «работе»: «… в настоящей рассмотрен подход…»; на странице 89 в конце одного из предложений отсутствует точка; и т.д.

Приведенные замечания не снижают общей положительной оценки диссертационной работы и не ставят под сомнение значимость полученных результатов.

9 Соответствие темы диссертации заявленной научной специальности

Тема и положения, выносимые на защиту, соответствуют паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по следующим пунктам:

п.3. «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса»:

п.15. «Модели и методы управления информационной безопасностью».

10 Оценка диссертации

Диссертация Новохрестова А.К. является самостоятельной научно-квалификационной работой, в которой даны научно обоснованные решения по увеличению полноты и объективности составления перечней угроз ИБ компьютерных сетей.

Диссертация отвечает требованиям пункта 9 «Положения о порядке присуждении ученых степеней» ВАК РФ по актуальности, научной новизне, значимости, опубликованности и апробированности, а её автор, Новохрестов Алексей Константинович, достоин присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (технические науки).

Официальный оппонент,
кандидат технических наук (05.13.01), доцент, заведующий кафедрой «Комплексная защита информации» Ложников Павел Сергеевич

ФГБОУ ВО «Омский государственный технический университет»
644050, г. Омск, пр-т. Мира, д. 11
Телефон: 8 (3812) 62-87-07
E-mail: lozhnikov@mail.ru