Отзыв научного руководителя
на диссертационную работу 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 исследования обоснована тем, что неотъемлемым этапом процесса обеспечения безопасности является определение перечня актуальных угроз, для чего необходимо составить как можно более обширный перечень угроз, т.е. осуществить их полную идентификацию.

Профессиональный уровень, а также субъективное мнение эксперта при использовании существующих подходов к построению перечней угроз информационных систем существенно влияет на итоговый результат.

Предложенная автором методика совместно с разработанной в её рамках моделью позволяет составить максимально полный перечень угроз информационной безопасности компьютерных сетей с минимальным влиянием профессионального уровня и субъективного мнения эксперта.

Научная новизна. В работе получены следующие новые 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.

Методы исследования. Для решения поставленных задач в диссертационной работе использовались методы математического моделирования, системного анализа, теории графов и теории защиты информации.

Достоверность результатов работы подтверждается их внутренней непротиворечивостью и положительным эффектом от внедрения научных исследований в работу действующего предприятия, о чем свидетельствует соответствующий Акт о внедрении. Использовано сравнение авторского перечня типов угроз с угрозами из банка данных ФСТЭК России.

Теоретическая ценность работы заключается в том, что:

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.

Практическая ценность работы состоит в следующем:

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

2. 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.

Внедрение результатов.

Результаты диссертационной работы внедрены в деятельность АО «ПКК Миландр» в процессе работы над автоматизированной системой коммерческого учета энергоресурсов, а также в учебный процесс Томского государственного университета систем управления и радиоэлектроники.

Полнота опубликования результатов работы. Результаты работы обсуждались на ряде всероссийских и международных конференций и семинаров и отражены в 16 публикациях, в том числе 2 публикации в рецензируемых журналах из перечная ВАК.

Содержание работы

В *первой главе* рассматриваются подходы к построению моделей компьютерных сетей, применяемые при идентификации угроз и оценке защищенности, а также непосредственно подходы к описанию и идентификации угроз и построению моделей угроз компьютерных сетей и информационных систем.

В результате установлено, что существующие модели имеют различные недостатки, например, отсутствие математической формализации и описания угроз непосредственно информационной системе.

Вторая глава посвящена разработке методики составления перечня угроз, отличающаяся от аналогов использованием матрицы взаимосвязей между элементами. Также описываются используемые в методике модель компьютерной сети и подход к классификации угроз.

Результатами работы, представленной в настоящей главе, являются методика определения перечня угроз, а также модели компьютерной сети и угроз безопасности компьютерной сети. Описываются преимущества

разработанной автором методики, представлен перечень недостатков аналогичных моделей, которые были устранены.

В *третьей главе* представлено сравнение разработанной автором модели с перечнем угроз из банка данных угроз ФСТЭК России, а также в качестве апробации разработанной методики и моделей рассмотрена модель угроз АСКУЭ.

Установлено, что предложенный автором подход к построению моделей угроз позволяет специалистам по защите информации учесть при построении системы защиты информации больше типов угроз информационной безопасности системы, чем использование банка данных угроз ФСТЭК России.

В ходе внедрения результатов работы в деятельность АО «ПКК Миландр» при разработке автоматизированной системы коммерческого учета энергоресурсов был составлен перечень из 70 угроз целостности системы. Угрозы рассматривались на программном и аппаратном уровнях для трех основных типов элементов системы. Полученный с использованием авторской методики и моделей перечень оказался на 18% больше составленного экспертами заказчика ранее (59 угроз целостности системы). Это позволило учесть при проектировании системы защиты необходимость дополнительных механизмов защиты. Также использование авторской модели информационной системы позволило учесть при построении структуры АСКУЭ характеристики элементов и взаимосвязи между ними.

Во время обучения в аспирантуре Алексей Константинович совмещал научную деятельность с педагогической. Он является младшим научным сотрудником лаборатории безопасных биомедицинских технологий центра технологий безопасности кафедры комплексной информационной безопасности электронно-вычислительных систем факультета безопасности ТУСУРа. При выполнении диссертации он проявил инициативность, самостоятельность, ответственность, нацеленность на практическую значимость и полезность проводимых исследований.

Диссертационная работа представляет собой законченную научно-квалификационную работу, выполненную на актуальную тему. Научная новизна полученных результатов, их обоснованность и достоверность, а также теоретическая и практическая значимость позволяет считать, что диссертация «Модель угроз информационной безопасности программного обеспечения компьютерных сетей на основе атрибутивных метаграфов» удовлетворяет требованиям «Положения о порядке присуждения ученых степеней» ВАК РФ, предъявляемым к кандидатским диссертациям, а её автор – Новохрестов Алексей Константинович заслуживает присуждения ему ученой степени

кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Научный руководитель
Ректор ТУСУР,
д.т.н., профессор

А. А. Шелупанов

634050. Томск, пр. Ленина, 40
Тел.: 8 (3822) 51-05-30
E-mail: saa@tusur.ru

Подпись А.А. Шелупанов заверяю
Ученый секретарь ученого Совета ТУСУР / Е. В. Прокопчук