Отзыв научного руководителя
на диссертационную работу Егошина Николая Сергеевича
«Модели угроз нарушения безопасности информационных потоков в киберпространстве»,
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 безопасности информации существенно влияет на итоговый результат.

Предложенная автором модель угроз позволяет составить максимально полный перечень типовых угроз безопасности информации с минимальным влиянием профессионального уровня и субъективного мнения эксперта.

Научная новизна. В работе получены следующие новые результаты.

1. Предложена мультиграфовая модель элементарных информационных потоков в информационной системе, учитывающая гетерогенность каналов взаимодействия.
2. Разработана модель угроз конфиденциальности информации, отличающаяся от аналогов полнотой учета всех типовых угроз элементам системы и каналам передачи информации.
3. Предложена модель угроз целостности и доступности информации, отличающаяся от аналогов учетом угроз доступности как подмножество угроз целостности информации, направленных на канал передачи информации.

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

Достоверность и обоснованность предлагаемых научных положений, результатов и выводов работы подкрепляется разносторонним изучением современного состояния предметной области, системным обоснованием предложенных моделей, не противоречащих известным положениям других авторов, апробацией полученных результатов в научных публикациях и

докладах на международных и российских научных и научно-практических конференциях, а также практикой внедрения результатов исследования.

Теоретическая ценность работы состоит в развитии теории и методологии обеспечения информационной безопасности в части создания новых моделей угроз информации, нарушителя, описания информационных потоков в системе и методики формирования политики разграничения доступа с применением математического аппарата теории графов для моделирования процессов взаимодействия в системе.

Практическая ценность работы состоит в следующем:

1. Модель нарушителя позволила расширить количество учитываемых типов нарушителя за счет комбинирования его характеристик;
2. Методика формирования политики разграничения доступа, основанная на модели информационных потоков, позволила разграничить доступ к каналам передачи информации как к самостоятельным структурным элементам системы.

Внедрение результатов.

Результаты диссертационной работы внедрены в деятельность УЦ Сибири, «НПФ «ИСБ», а также в учебный процесс Томского государственного университета систем управления и радиоэлектроники.

Полнота опубликования результатов работы. По материалам исследования опубликовано 11 работ, в том числе 4 работы в изданиях, рекомендованных ВАК РФ, и 2 в изданиях WoS и Scopus.

Содержание работы

В *первой главе* рассматриваются подходы к описанию информационных систем, непосредственно подходы к описанию и идентификации угроз и построению моделей угроз безопасности информации, а также подходов к формированию политики разграничения доступа и построению модели нарушителя.

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

Вторая глава посвящена разработке модели информационных потоков.

Результатами работы, представленной в настоящей главе, является модель информационных потоков в информационной системе. Описываются преимущества разработанной автором модели.

В *третьей главе* представлен процесс разработки модели типовых угроз безопасности информации и сравнение модели с перечнем угроз из банка данных угроз ФСТЭК России. Результатом внедрения работы в деятельность ООО «НПФ «ИСБ» стал перечень из 43 угроз безопасности информации в

ИСПДн, что на 14 % больше, чем количество угроз, выявленных экспертами ранее.

Четвертая глава посвящена процессу разработки модели нарушителя информационной безопасности, представлен перечень недостатков аналогов. Разработанная модель нарушителя, позволяет проследить причинно-следственные связи между элементами модели и цепочками предполагаемых последствий. Основываясь на этом, а также на описании состояния окружающей среды, рубежей защиты и всех зон, окружающих конфиденциальную информацию, были описаны и ранжированы возможные виды предполагаемых нарушителей. Как следствие, модель позволяет построить полное и универсальное по отношению к различным системам описание вероятного нарушителя информационной безопасности

В *пятой главе* описана методика формирования политики разграничения доступа к информации. Предложенная методика была внедрена в деятельность ООО «УЦ Сибири», результатом внедрения стало уменьшение времени, необходимого для формирования политики разграничения доступа на 19 % (в частном случае с 16 до 13 часов).

Установлено, что предложенная автором модель угроз позволяет специалистам по защите информации учесть больше типов угроз информационной безопасности системы, чем использование банка данных угроз ФСТЭК России.

Во время обучения в аспирантуре Николай Сергеевич 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 «Модели угроз нарушения безопасности информационных потоков в киберпространстве» удовлетворяет требованиям «Положения о порядке присуждения ученых степеней» ВАК РФ, предъявляемым к кандидатским диссертациям, а её автор – Егошин Николай Сергеевич заслуживает присуждения ему ученой степени кандидата технических наук по

специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Научный руководитель
Заведующий кафедрой КИБЭВС,
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