УТВЕРЖДАЮ
И.о. первого проректора НИЯУ «МИФИ»
_____ О.В. Нагорнов
«12» 12 2021 г.

ОТЗЫВ

ведущей организации – федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ» на диссертацию Егошина Николая Сергеевича на тему «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

1. Актуальность темы диссертации

Определение перечня актуальных угроз безопасности информации (УБИ) является неотъемлемым этапом процесса обеспечения безопасности информационных систем (ИС). Причем до определения актуальности необходимо составить перечень УБИ, включающий все существующие УБИ для рассматриваемой ИС, т.е. осуществить идентификацию УБИ. При этом существенное влияние на перечень УБИ оказывает квалификация и субъективное мнение специалистов, выполняющих их идентификацию. В данном контексте видится актуальной разработка новой модели УБИ и методики формирования политики разграничения доступа, при использовании которых влияние профессионального уровня и субъективного мнения эксперта будет минимизировано. Это обуславливает актуальность темы диссертационного исследования Егошина Н.С., в качестве цели которого автором обозначено развитие подхода к формированию актуального перечня УБИ и политики разграничения доступа за счет применения моделей информационных потоков и УБИ.

2. Структура и объем диссертации

Объем основной части диссертационной работы (с введения по заключение) составляет 90 страниц машинописного текста, в том числе 31 таблица, 29 рисунков. Список литературы состоит из 120 наименований. Диссертация содержит введение, пять глав, 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, применяемые при описании ИС, подходы к построению моделей УБИ, формированию модели нарушителя информационной безопасности (ИБ) и методик формирования политики разграничения доступа.

Во второй главе автором с учетом выделенных в первой главе недостатков предлагается модель информационных потоков, которая позволяет описать любую ИС с помощью конечного множества элементарных информационных потоков.

В третьей главе представлена модель УБИ и приведено ее сравнение с наиболее полным перечнем УБИ, существующим на данный момент и применяемым на практике – банком данных ФСТЭК России. Представлены результаты внедрения указанной модели.

В четвертой главе автором описывается разрабатываемая модель нарушителя ИБ, описываются его параметры и связь с предложенной ранее моделью УБИ.

В пятой главе описывается разработанная автором методика формирования политики разграничения доступа, представлены результаты ее апробации.

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 УБИ.

Наиболее важные результаты диссертационной работы, обладающие признаками научной новизны:

1) предложена мультиграфовая модель элементарных информационных потоков в ИС, 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.

4. Обоснованность и достоверность полученных результатов

Цель диссертационного исследования и поставленные для ее достижения 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 Егошина Н.С. используются в учебном процессе и научно-исследовательской деятельности студентов Томского государственного университета систем управления и радиоэлектроники. Конкретно значимость полученных результатов заключается в следующем:

1. Сравнение разработанной модели УБИ с перечнем угроз из базы УБИ ФСТЭК России позволило выделить ещё 13 типовых угроз. Разработанная модель УБИ была внедрена в деятельность ООО «НПФ «ИСБ». Применение модели УБИ, позволило получить полный перечень типовых УБИ, обрабатываемой в ИСПДн. Полученный список был учтен при определении перечня актуальных УБИ, что показало необходимость внедрения в систему дополнительных мер обеспечения ИБ. Результатом внедрения работы в деятельность ООО «НПФ «ИСБ» стал перечень из 43 УБИ в ИСПДн, что на 14 % больше, чем количество угроз, выявленных экспертами ранее.

2. Представлены методические рекомендации по формированию политики разграничения доступа к информации в ИС.

3. Разработанная методика формирования политики разграничения доступа, использующая модель элементарных информационных потоков, позволила разграничить доступ к каналам передачи данных как к самостоятельным структурным единицам системы. 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).

6. Рекомендации по использованию результатов диссертационной работы

Предприятиям и организациям, занимающимся анализом защищенности, построением и сопровождением систем защиты информации в ИС – использовать предложенные автором модели и методику для определения перечней угроз безопасности обрабатываемой информации.

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 «Управление информационной безопасностью», «Разработка и эксплуатация защищенных автоматизированных систем» и «Основы информационной безопасности».

В качестве возможного продолжения и развития исследований, выполненных в диссертации, рекомендуется расширение предложенного автором подхода за пределы киберпространства, а также программная реализация методики формирования политики разграничения доступа.

7. Публикации, апробация и внедрение результатов работы

Научные и практические результаты диссертационной работы докладывались и обсуждались на семинарах и 5 конференциях различного уровня, в том числе всероссийского и международного. Материалы исследования отражены в 10 научных публикациях, в том числе 4 работах в изданиях, рекомендованных ВАК Российской Федерации и в 2 изданиях из перечня WoS и Scopus.

Результаты диссертационной работы внедрены в деятельность «Удостоверяющего Центра Сибири» и НПФ «Информационные системы безопасности», а также в учебный процесс Томского Государственного Университета Систем Управления и Радиоэлектроники.

8. Замечания по диссертации

1. Замечания терминологического характера. Во-первых, автор использует термины «безопасность информации» и «информационная безопасность», не определив, одно это и тоже или нет. Во-вторых, в работе присутствуют понятия «информационная система», «компьютерная система», «киберпространство», которые автор периодически подменяет друг другом; такая подмена не корректна, поскольку эти понятия не тождественны между собой.
2. Замечания по названию разделов диссертации. Разделы 1.2 и 3 и аналогичные названы некорректно – лучше «...угроз безопасности информации». Это же касается и названия раздела 1.3. Разделы «Выводы по главе» должны быть дополнены номером главы, чтобы не было разделов с одинаковым названием.
3. В разделе 1.2.2 и 1.2.3 без четкого обоснования предлагается не рассматривать важных характеристики угроз (потери и ущерб), которые на самом деле очень важны для расчетов рисков ИБ, являющихся определяющими при установлении актуальности УБИ – если риск недопустим, то угроза актуальна и наоборот – если риск допустим, то угроза неактуальна.
4. При анализе существующих моделей угроз не рассмотрен методический документ ФСТЭК России «Методика оценки угроз безопасности информации» 2021 г.
5. В соответствующем разделе отдельно как часто применяемая не рассмотрена ролевая модель доступа.
6. В описании модели нарушителя ИБ говорится: «Для удобства ... введена условная бальная система», однако сами параметры нарушителя имеют собственные значения, которые никак не соотносятся с бальной системой; не представлено соотношение баллов с уровнем нарушителя.
7. В работе упоминается, что модель нарушителя ИБ позволила расширить количество учитываемых типов нарушителя, но не указывается количественная характеристика увеличения (на сколько типов нарушителя данная модель позволяет определить больше, чем аналоги). Кстати, по всему тексту диссертации было бы лучше использовать «модель нарушителя ИБ», а не просто «модель нарушителя».
8. Определено четыре множества каналов взаимодействия, при этом не поясняя чем отличается взаимодействие в виртуальной и электромагнитной среде; также не указано чем отличается удаленное взаимодействие от обычного (локального?).
9. В тексте диссертации и автореферата встречаются пунктуационные ошибки и явные опечатки, которые при этом не мешают общему пониманию работы.

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 Егошина Н.С. 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 ИБ как методы и модели идентификации и классификации УБИ объектов различного вида и класса, а также модели и методы управления ИБ.

Таким образом, диссертационная работа оформлена в соответствии с ГОСТ Р 7.0.11-2011 и удовлетворяет требованиям «Положения о присуждении ученых степеней» ВАК Российской Федерации от 24 сентября 2013 г. № 842 (ред. от 11.09.2021), а её автор – Егошин Николай Сергеевич– заслуживает присуждения ей ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв ведущей организации на диссертацию Егошина Н.С. рассмотрен и одобрен на заседании кафедры «Информационная безопасность банковских систем» НИЯУ МИФИ (протокол № 4 от 08.12.2021).

Отзыв подготовил:
Доцент Отделения интеллектуальных кибернетических систем офиса образовательных программ Института интеллектуальных кибернетических систем НИЯУ МИФИ, и.о.зав.каф. «Информационная безопасность банковских систем», доцент, кандидат технических наук,
115409, г. Москва, Каширское шоссе, д. 31, ауд. Т-202
Тел. +7 (495) 7885699*9644, электронная почта: aitolstoj@mephi.ru

Толстой Александр Иванович

«9» декабря 2021 г.

Подпись заверяю
Зам. директора по персоналу НИЯУ МИФИ
Л.В. Васильченко

Сведения об организации:
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ), 1115409, г. Москва, Каширское шосее, д. 31, info@mephi.ru, +7 495 788-5699