ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертацию 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 диссертации

Несмотря на то, что в настоящее время специалистами коммерческих и государственных учреждений, а также учеными, занимающимися вопросами обеспечения информационной безопасности, уделяется большое внимание противодействию атакам на информацию, которая обрабатывается в информационных системах, количество успешных атак продолжает увеличиваться. Во многом это обусловлено тем, что при обеспечении безопасности компьютерных сетей специалисты по защите информации руководствуются только личным опытом. Специалисту приходится опираться на множество различных подходов к классификации и идентификации угроз, которые часто противоречат друг другу.

Работа Егошина Н.С. посвящена решению проблемы составления максимально полного перечня угроз безопасности информации и снижению влияния личного опыта специалиста, осуществляющего идентификацию угроз, что несомненно имеет существенное значение для решения задач информационной безопасности. Таким образом, тема диссертации Егошина Н.С. является актуальной.

Структура и содержание диссертации

Диссертационная работа Егошина Н.С. состоит из введения, пяти глав, заключения, списка источников и 1 приложения. Общий объем диссертационной работы: 113 страниц, в том числе 31 таблица и 29 рисунков.

Во введении автором обоснована актуальность темы исследования, поставлены цель и задачи, приведены научная новизна, практическая и теоретическая значимость полученных результатов, а также положения, выносимые на защиту.

В первой главе приведен обор современного состояния предметной области. Приведены недостатки существующих подходов, на устранение которых направлено диссертационное исследование.

Вторая глава посвящена описанию разработанной Егошиным Н.С. модели информационных потоков, предназначенной для математического описания информационной системы.

В третьей главе представлена предложенная автором модель угроз безопасности информации, обосновывается полнота модели, приводятся результаты внедрения и сравнение с аналогом – Банк данных угроз безопасности информации ФСТЭК.

В четвертой и пятой главах представлены модель нарушителя, методика формирования политики разграничения доступа к информации в информационной системе и результаты ее внедрения.

В конце каждой главы и в заключении автором сделаны обобщающие выводы, позволяющие составить представление о полученных результатах.

Список источников включает 120 позиций, в том числе нормативные правовые акты, методические и научные труды российских и зарубежных ученых, интернет-ресурсы по профилю исследования.

В приложение вынесены акты внедрения диссертационной работы (акт о внедрении в деятельность ООО «НПФ «ИСБ», акт о внедрении в деятельность ООО «УЦ Сибири» и акт о внедрении в учебный процесс ФГБОУ ВО «ТУСУР»).

Оформление диссертации и автореферата не вызывает нареканий и соответствует требованиям ГОСТ Р 7.0.11-2011.

Научная новизна полученных результатов

Соискателем получены следующие новые научные 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.

Теоретическое и практическое значение результатов работы

Теоретическая значимость 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. Теоретические

результаты используются в учебном процессе Томского государственного университета систем управления и радиоэлектроники, что подтверждается актом внедрения.

Практическая значимость полученных автором результатов заключается в увеличении количества обнаруживаемых угроз ИБ и снижении влияния субъективного мнения специалиста при составлении моделей угроз безопасности информации. Сравнение разработанной модели с наиболее полной аналогом позволило выделить ещё 13 типовых угроз. Разработанная модель угроз была внедрена в деятельность ООО «НПФ «ИСБ». Применение модели угроз, позволило получить полный перечень типовых угроз безопасности информации, обрабатываемой в ИСПДн. Полученный список был учтен при определении перечня актуальных угроз, что показало необходимость внедрения в систему дополнительных механизмов защиты. 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.

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).

Обоснованность и достоверность полученных результатов и выводов

Автором адекватно использованы формальные методы дискретной математики (теория множеств и теория графов), системного анализа и теории защиты информации, сделаны корректные выводы на основе полученных данных. Достоверность результатов подтверждается положительным эффектом от внедрения научных исследований в работу действующего предприятия и сравнением авторского перечня типов угроз с угрозами из банка данных ФСТЭК России.

Пункты научной новизны, положения, выносимые на защиту, и выводы хорошо аргументированы, корректны, подтверждаются внедрением.

Рекомендации по использованию результатов работы

Результаты диссертационной работы Егошина Н.С. могут быть применены:

– при определении угроз безопасности системы в процессе аудита информационной безопасности или в процессе проектирования (модернизации) системы защиты информационных систем;

– при разработке программного средства для помощи специалисту по защите информации при определении угроз безопасности информации;

– при обучении и повышении квалификации специалистов по защите информации.

Публикации и апробация материалов диссертации

По материалам диссертации Егошиным Н.С.опубликовано 10научных работ, в том числе 4 работы в изданиях, рекомендованных ВАК РФ, и 2 работы в изданиях, индексируемых в базах данных Scopus и WoS. Знакомство с отдельными публикациями соискателя свидетельствует о достаточно полном отражении результатов диссертационного исследования.

Замечания к работе

1. При построении модели угроз конфиденциальности информации недостаточно подробно расписан случай компрометации всей системы целиком (угроза k_4); резкий переход от формулировки «компрометация системы целиком» к «контроль канала передачи данных»;
2. В обеих моделях рассматриваются примеры для каждой из типовых угроз, однако в некоторых случаях пример имеет некорректную формулировку и звучит как атака, а не угроза;
3. В работе говорится о применении нотации информационных потоков, которая основана на нотации теории графов; судя по тексту работы, упомянутая нотация – это математический аппарат, описывающий предложенную автором модель информационных потоков, однако отдельное ее описание отсутствует, корректнее было бы просто использовать теорию графов без ввода дополнительного определения;
4. Было бы нагляднее, если бы в качестве примера при демонстрации применения методики формирования политики разграничения доступа применился бы тот же пример, что и при демонстрации модели информационных потоков и модели угроз.

Общая оценка диссертации

Отмеченные выше замечания хотя и несколько снижают впечатление от диссертации, но не подвергают сомнению основные научные результаты автора, их научную новизну и значимость. Таким образом общая оценка работы остается положительной.

Диссертация Егошина Н.С. является завершенной научно-квалификационной работой, в которой содержится решение актуальной научно-технической задачи – развитие подхода к формированию актуального перечня угроз и политики разграничения доступа. Диссертация соответствует пунктам 1 и 3 паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Содержание работы хорошо структурировано, повествование построено последовательно и логично, графическое оформление – аккуратно. Автореферат соответствует основному содержанию диссертации. Работа обладает необходимыми признаками научной новизны, теоретической и практической значимостью. Основные результаты диссертации опубликованы в изданиях из перечня ВАК Российской Федерации, представлены в материалах конференций различного уровня.

По актуальности, научной новизне полученных результатов, объему выполненных исследований, практической и теоретической значимости представленная работа соответствует требованиям пункта 9 «Положения о порядке присуждении ученых степеней» ВАК Российской Федерации, утвержденного постановлением Правительства Российской Федерации №842 от 24.09.2013 г., предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор, Егошин Николай Сергеевич, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Официальный оппонент ____________ / Золотарев Вячеслав Владимирович

кандидат технических наук (специальность 05.13.01), доцент, заведующий кафедрой безопасности информационных технологий

ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева»

660037, Сибирский федеральный округ, Красноярский край, г. Красноярск, проспект им. газеты Красноярский рабочий, 31
Телефон: +7 (391) 222-76-39
E-mail: zolotorev@sibsau.ru

Подпись Золотарева В.В.
удостоверяю
Ведущий специалист по персоналу
Я.Кади / Я.В. Кадырская
«10» 12 2021 г.

УПРАВЛЕНИЕ КАДРОВ