ОТЗЫВ

официального оппонента, д.т.н., профессора Ложникова Павла Сергеевича 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»

1. Актуальность работы

Работа Егошина Николая Сергеевича посвящена решению проблем формирования актуальных перечней угроз и политик разграничения доступа, а также исследованию механизмов моделирования и описания процессов передачи информации внутри систем. Эти вопросы являются актуальными, поскольку существующие в настоящий момент времени модели ориентированы на применение прямых экспертных оценок, являющихся в явном виде субъективными.

В работе автор указывает, что одним из важнейших этапов обеспечения безопасности информационных систем является составление перечня угроз информационной безопасности (далее – 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 Егошина Н.С. значится развитие подхода к формированию актуального перечня угроз и политики разграничения доступа за счет применения моделей информационных потоков и угроз безопасности информации. Направленность на решение задачи, имеющей существенное значение в области ИБ, позволяет классифицировать тематику рассматриваемой диссертации как актуальную.

2. Структура и содержание диссертации

Диссертационная работа Егошина Н.С. содержит введение, пять глав, заключение, одно приложение и список источников из 120 наименований. Объем диссертационной работы составляет 113 страниц, включая 31 таблицу и 29 рисунков.

Результаты диссертационного исследования в достаточной мере изложены в основном тексте диссертации и ряде приложений. Автореферат полностью соответствует основному содержанию 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 несколько частей: описаны подходы к описанию информационных систем, формированию политик разграничения доступа, описанию и идентификации угроз, построению моделей угроз информации, а также формированию модели нарушителя. В выводах по главе приводится обобщенный перечень недостатков описанных подходов.

Во второй главе представлено описание авторской модели информационных потоков, которая позволяет описать любую информационную систему с помощью конечного множества элементарных информационных потоков. Приводится пример применения представленной модели.

В третьей главе описана авторская модель угроз безопасности информации. Глава разделена на две части: обоснование полноты модели угроз конфиденциальности информации и обоснование множества угроз целостности и доступности. Приводится сравнение с наиболее полным аналогом.

Четвертая и пятая главы посвящены апробации результатов диссертационного исследования, разработке методики формирования политики разграничения доступа и модели нарушителя.

В заключении приведены основные выводы и результаты диссертационного исследования.

3. Новизна полученных результатов

Результатами диссертации, обладающими признаками научной новизны, являются:

1) мультиграфовая модель элементарных информационных потоков в информационной системе, учитывающая гетерогенность каналов взаимодействия;

2) модель угроз конфиденциальности информации, отличающаяся от аналогов полнотой учета всех типовых угроз элементам системы и каналам передачи информации;

3) модель угроз целостности и доступности информации, отличающаяся от аналогов учетом угроз доступности как подмножество угроз целостности информации, направленных на канал передачи информации.

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 безопасности информации. Сравнение разработанной модели с наиболее полным 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).

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.

5. Достоверность и обоснованность основных результатов и выводов

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.

6. Рекомендации по использованию результатов работы

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

В качестве рекомендации для дальнейшего развития исследований можно предложить расширение авторского подхода за пределы киберпространства на всю информационную систему.

7. Публикации по теме диссертации

Результаты диссертации опубликованы в 10 научных работах, 4 из которых в изданиях из списка ВАК РФ и 2 в изданиях Web of Science и Scopus, результаты представлены на конференциях различного уровня, в том числе всероссийского и международного.

8. Замечания по диссертации

1) В основе разделения модели угроз безопасности информации на две отдельные составляющие лежит утверждение о двух способах взаимодействия с информацией (чтение и непосредственное воздействие), которое не имеет развернутого обоснования;

2) В тексте работы не приводится достаточного обоснования сопоставления видов воздействий (изменение, уничтожение, подмена) на информацию с соответствующими аспектами ИБ – целостностью и доступностью;

3) При описании множества угроз целостности информации графы имеют одинаковый вид независимо от вида воздействия на информацию в вершине, а для угрозы c_7 не указан источник воздействия;

4) По тексту автореферата и диссертации встречаются пунктуационные ошибки и опечатки.

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:

- Теория и методология обеспечения информационной безопасности и защиты информации (п.1).
- Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса (п.3).

10. Оценка диссертации

Диссертация Егошина Н.С. является самостоятельной научно-квалификационной работой, в которой даны научно обоснованные решения по увеличению полноты и объективности составления перечней угроз безопасности информации.

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

Официальный оппонент
Доктор технических наук (05.13.19), профессор,
заведующий кафедрой «Комплексная защита
информации» ФГБОУ ВО «Омский
государственный технический университет»

Ложников Павел Сергеевич

644050, г. Омск, пр-т. Мира, д. 11
Телефон: 8 (3812) 21-77-02
E-mail: lozhnikov@mail.ru