Федеральное государственное автономное научное учреждение
"Научно-исследовательский институт
"Специализированные вычислительные устройства защиты и автоматика"

344003, г. Ростов-на-Дону, ул. Города Волос, 6 | Тел. (863) 201-28-17, факс (863) 201-28-13, e-mail: info@niisva.org

УТВЕРЖДАЮ
Директор
ФГАНУ НИИ "Спецвузавтоматика"
_____ Р.А. Хади
"20" 12 2021 г.

ОТЗЫВ

на автореферат диссертации Егошина Н.С. «Модели угроз безопасности информационных потоков в киберпространстве», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Несмотря на существование и широкое использование нескольких подходов к построению моделей угроз безопасности информации при ее обработке и хранении в информационной системе (ИС), зачастую модели угроз, создаваемые с ориентацией на их практическое использование, зачастую не обладают полнотой и достаточной обоснованностью. Иногда это приводит к возникновению угроз безопасности, потенциально предотвратимых на этапе проектирования ИС. В связи с этим, диссертационное исследование Егошина Н.С., направленное на разработку подхода к построению моделей угроз безопасности информации, ориентированного на полноту, является актуальным.

В ходе проведения диссертационного исследования соискателем разработана модель информационных потоков в системе, модель угроз безопасности информации, модель нарушителя, а также методика формирования политики разграничения доступа к информационным ресурсам. Теоретическая значимость результатов 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 терминологии теории графов для

моделирования процессов взаимодействия в системе. Практическая значимость результатов исследования заключается в предложенной модели нарушителя, которая позволила расширить количество учитываемых типов нарушителя за счет комбинирования его характеристик, а также в методике формирования политики разграничения доступа, которая позволила разграничить доступ к каналам передачи информации как к самостоятельным структурным элементам системы.

Полученные результаты обладают научной новизной и практической обоснованностью. Результаты работы отражены в 10 публикациях, из них 4 публикации в рецензируемых журналах из перечня ВАК. Полученные результаты внедрены и используются в практической деятельности.

К работе имеется несколько замечаний.

1. Автор довольно небрежен в обращении с математической терминологией. Так, например, конструкция, изображенная в автореферате на рис. 10, названа «ненаправленным мультипликативным графом». Это представляется ошибкой. Мультипликативным называют граф, для которого из гомоморфности ему тензорного произведения двух графов следует гомоморфность ему же одного из этих графов. Если автор имел в виду это свойство графа, о котором идет речь в главе 2, то оно нуждается в доказательстве, а также в пояснении нуждается важность этого свойства для обсуждения. Представляется, однако, что тут произошла ошибка в терминологии, и речь идет о мультиграфе.

2. Предлагаемый автором подход к построению модели угроз ориентирован на полноту учета возможных угроз для конкретной информационной системы. Между тем, пример, приводимый в главе 2 (рис. 11 в автореферате) характеризуется как раз недостаточной полнотой учета структуры и особенностей функционирования ИС: проигнорированы, как минимум, процессы аутентификации клиентов сервиса для доступа к его функциональности (крайне важные в прикладных случаях; их корректное описание добавило бы к схеме несколько существенных элементов), а также особенности сетевой инфраструктуры, используемой при передаче информации (узлы сети Интернет, через которые маршрутизируется трафик, элементы беспроводной сети и т.п.), и потому фактически оказывающейся частью ИС на время конкретного эпизода её использования. Между тем, в прикладных ситуациях именно такого рода детали зачастую оказываются основой для нарушения защищенности ИС. Понятна интенция автора сделать иллюстрацию по возможности структурно простой, но в таком случае, возможно, следовало бы рассмотреть другие примеры, обладающие простотой структуры в действительности.

3. Во всем тексте автореферата подразумевается автономность системы мандатного управления правами доступа от ИС, модель угроз которой рассматривается. Представляется, что этот момент требует пояснения, а обоснованность такого ограничения – дополнительных аргументов.

4. Хотелось бы получить комментарий относительно типов угроз g2c2 и g3c1 из списка на стр. 15 автореферата. Без дополнительного пояснения создается впечатление, что ситуации, формально описываемые в этих пунктах, хотя и являются косвенными свидетельствами проблем в ИС, не являются непосредственно эпизодами нарушения информационной безопасности.

Перечисленные недостатки кажутся признаками того, что диссертация, вероятно, не достаточно детально рассматривалась профессиональным и научным сообществом в процессе работы автора над ней.

Тем не менее, работа соответствует паспорту специальности, полученные результаты представляют ценность, и требования ВАК о порядке присуждения учетных степеней формально выполнены. Считаю, что автор работы, Егошин Н.С., заслуживает присуждения ему учетной степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Старший научный сотрудник
лаборатории телекоммуникационных технологий
ФГАНУ НИИ "Спецвузавтоматика",
кандидат технических наук В.В. Мкртичян