Экз. № 2

ОТЗЫВ

официального оппонента доктора технических наук, доцента, заведующего кафедрой «Информационная безопасность автоматизированных систем» Мазина Анатолия Викторовича на диссертационную работу соискателя учёной степени кандидата технических наук Ковалева Максима Сергеевича, выполненную на тему «Оптимизация размещения средств защиты информации в узлах коммутации VPN сети» по специальности 05.12.13 «Системы, сети и устройства телекоммуникаций»

Необходимость осуществления научно-технического прогресса в Российской Федерации связана, прежде всего, с созданием цифровых информационно-телекоммуникационных систем, обеспечивающих эффективное функционирование управленческой, производственно-технологической и социальной сфер общества. Именно на это ориентируют научные организации, коллективы исследователей и предприятия промышленности, Указ Президента РФ от 01.12.2016 г. № 642 «О Стратегии научно-технологического развития Российской Федерации».

В настоящее время информационно-телекоммуникационные системы объединяют все виды трафика в единый цифровой поток, реализуют метод коммутации пакетов, обеспечивают пользователям требуемое качество услуг и являются мультисервисными сетями. Формирование корпоративного коммуникационного кластера в мультисервисной сети реализуется на базе частных выделенных сетей (VPN сетей), что существенно упрощает информационный обмен данными между пользователями с требуемой скоростью и оперативностью.

Одной из важных задач, решаемых VPN-сетью, является задача обеспечения устойчивости функционирования самой сети, а также безопасности циркулирующей в ней информации. При этом объектами угроз в виде различных атак, в основном, являются информационные объекты сети (ИОС), под которыми понимаются маршрутизаторы сети и серверы,

хранящие целевую информацию того или иного характера и размещаемые в узлах VPN-сети. Информационные угрозы в виде атак нарушителя на ИОС VPN-сети реализуются в основном по двум направлениям:

- с целью блокирования тех или иных узлов коммутации путем переполнения их буферной памяти, а также искажением и модификацией маршрутных таблиц;
- с целью копирования, модификации и искажения информации содержащейся в серверах.

Проведенные исследования показали, что достижение требуемого уровня защищенности ИОС в VPN-сетях возможно увеличением числа размещаемых однотипных средств защиты информации (СЗИ) на ИОС. Однако данное направление приводит к существенному удорожанию системы защиты. С другой стороны, возможен подход, базирующийся на оптимальном комплексном использовании различных СЗИ. В связи с этим для разрешения указанного противоречия необходимо создание научно-методического аппарата, определяющего размещение известных различных СЗИ на ИОС VPN-сети для достижения заданного уровня защищенности информации при минимуме их стоимости.

В связи с изложенным, диссертационная работа Ковалева М.С., решающая задачу научного обоснования моделей и методики, обеспечивающих снижение уровня ущерба, наносимого информации в информационных объектах VPN сети нарушителем, за счет оптимального размещения СЗИ при минимуме их стоимости, является актуальной и востребованной практикой реализации частных виртуальных сетей.

Соискателем верно сформулированы цель, объект, предмет и научная задача диссертационных исследований, решение которой потребовало от автора ее декомпозиции на ряд частных подзадач, решение которых позволило в конечном итоге достичь цели диссертационного исследования.

В ходе выполнения диссертации автором получены следующие результаты, обладающие научной новизной и практической значимостью.

Во-первых, это - аналитические и имитационная модели воздействия нарушителя на многоэшелонированную систему защиты информации в информационных объектах сети. Научная новизна разработанных аналитических моделей воздействия нарушителя заключается в том, что они построены на основе математического аппарата конечных марковских цепей, что позволяет, в отличие от известных, учитывать предысторию вскрытия отдельных уровней защиты и динамику их восстановления как по времени, так и по решению администратора сети, что характерно для современных сетевых систем защиты информации. Отличительной особенностью имитационной модели является возможность получения оценок показателей защищенности при минимуме реализаций модели, что позволяет администратору сети оценивать те или иные варианты противодействия атакам в реальном масштабе времени.

Во-вторых, это - автоматизированная методика оптимизации размещения средств защиты информации на информационных объектах сети, позволяющая повысить эффективность функционирования защиты информации без дополнительных существенных финансовых затрат. Научная новизна разработанной методики заключается в том, что оптимизация размещения разнотипных и разнородных средств защиты на ИОС, содержащих большое количество массивов информации различной важности, в отличие от известных подходов, впервые выполнена на основе пошаговой процедуры, реализующей сочетание динамического и вероятностно-игрового методов. Данная методика также реализована в программном виде и позволяет администратору сети находить оптимальные варианты противодействия атакам нарушителя в реальном масштабе времени.

Основные результаты диссертации являются достоверными, что обусловлено:

- корректностью постановки научной задачи исследования и ее декомпозицией на ряд частных задач;

- использованием апробированного аппарата теории защиты

информации, теории конечных марковских цепей, теории оптимизации, теории вероятностей, методов компьютерного моделирования;

- обоснованностью основных предположений, ограничений, допущений и исходных данных для расчетов;

- удовлетворительным совпадением полученных результатов расчета в среде имитационного моделирования с результатами аналитических расчетов и физикой исследуемых процессов реализации угроз и защиты информации.

Полученные в диссертации результаты имеют существенную теоретическую и практическую ценность, они вносят вклад в теорию и практику построения систем защиты информации в ИОС VPN сети.

Практическая значимость результатов диссертационного исследования заключается в том, что только за счет оптимизации размещения имеющихся средств защиты в распоряжении сетевого администратора уровень ущерба, который может быть нанесен информации, находящейся на исследуемом ИОС, может быть снижен на 17-25%. Результаты исследований представляют практический интерес для научно-исследовательских учреждений и проектных организаций с целью усовершенствования существующих и создания перспективных СЗИ для ИОС VPN сетей. Кроме того, результаты работы могут быть использованы в вузах при изучении учебных дисциплин, соответствующих тематике данной диссертационной работы.

Полученные в диссертации результаты целесообразно использовать заказывающими и научно-исследовательскими организациями РФ (АО НИВЦ АС, МОУ «ИИФ», АО НИИ ССУ, Институт проблем передачи информации РАН) при техническом обосновании перспектив развития комплекса средств и систем защиты информации в сетях и системах передачи информации различного профиля и формировании ТЗ на создание таких средств и систем, а также организациями промышленности (АО «Концерн «Созвездие»», АО «ЦНИИ ЭИСУ», АО «Лаборатория Касперского», АО «ВНИИА») при решении сложных научно-технических задач защиты информации, возникающих при разработке подобных VPN сетей.

Обобщая замечания по диссертационной работе и автореферату, их можно свести к следующим:

1. В аналитических моделях воздействия нарушителя на многоэшелонированную систему защиты информации ключевым параметром является вероятность преодоления отдельного рубежа защиты с одной попытки. В материалах диссертации и автореферата не указано, каким образом находятся данные величины по каждому рубежу.

2. Из материалов диссертации и автореферата не ясно, насколько адаптивной является автоматизированная методика оптимизации размещения средств защиты информации на информационных объектах сети к пополняемой номенклатуре средств защиты информации.

В целом, однако, отмеченные недостатки не носят принципиального характера и не наносят существенного ущерба значимости результатам диссертационной работы, выполненной на высоком научном уровне. Отличительными особенностями работы являются логическая последовательность поставленных задач и направленность их на решение важной практической технической задачи – обеспечение требуемого уровня защищенности информации в ИОС VPN сети при минимуме стоимости комплекса его СЗИ.

Диссертация написана хорошим литературным языком и аккуратно оформлена. Основные выводы и положения диссертации достаточно широко опубликованы в научных изданиях и докладывались на представительных научно-технических конференциях, где получили одобрение научной общественности, признающей авторитет автора в разработке вопросов, положенных в основу диссертационной работы. Требование ВАК о наличии двух и более публикаций в изданиях из Перечня ВАК выполнено.

Исследования по тематике представленной диссертации целесообразно продолжить в направлении учета более детальной градации СЗИ по их профилю.

Содержание автореферата соответствует основным положениям диссертации и позволяет сформировать обоснованное представление по всей

работе в целом, а содержание диссертации соответствует паспорту специальности 05.12.13 «Системы, сети и устройства телекоммуникаций».

Выводы:

1. Представленная диссертация является законченной научно-квалификационной работой, содержащей решение научной задачи обоснования моделей и методики, обеспечивающих снижение уровня ущерба, наносимого информации в информационных объектах VPN сети нарушителем, за счет оптимального размещения СЗИ при минимуме их стоимости.

2. По актуальности тематики, глубине проведённых исследований и значимости полученных результатов диссертационная работа полностью удовлетворяет требованиям п.п. 9,10,11,13,14 «Положения о присуждении учёных степеней», а её автор, Ковалев Максим Сергеевич, заслуживает присуждения учёной степени кандидата технических наук по специальности 05.12.13 «Системы, сети и устройства телекоммуникаций».

Официальный оппонент:
заведующий кафедрой «Информационная безопасность автоматизированных систем» Калужского филиала Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана» (национальный исследовательский университет), доктор технических наук, доцент А.В. Мазин.

Анатолий Викторович Мазин
Калужский филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени Н.Э. Баумана» (национальный технический исследовательский университет)
Юридический адрес: 248000, г. Калуга, ул. Баженова, д. 2.

Телефон организации: (4842) 74-40-32,

Факс: (4842) 56-30-45

E-mail организации: mail@bmstu-kaluga.ru

Официальный сайт организации: http://bmstu-kaluga.ru Телефон официального оппонента: 8910915 58 25

E-mail официального оппонента: MazinAV@Yandex.ru

Официальный оппонент
доктор технических наук, доцент
«12» сентября 2017 года А.В. Мазин

Подпись подписи
заверяю
Зам. нач. УК Мердина Т.М.

Управление кадров