О Т З Ы В

официального оппонента доктора технических наук, профессора
Куприянова Александра Ильича
о диссертационной работе «Оптимизация размещения средств
защиты информации в узлах коммутации VPN сети»
представленную Максимом Сергеевичем Ковалевым
на соискание ученой степени кандидата технических наук
по специальности
05.12.13 «Системы, сети и устройства телекоммуникаций»

1. Актуальность темы диссертации.

XXI век начался под знаком бурного, опережающего развития информационных технологий и информационных систем. Эта особенность порождает необходимость совершенствования технологий создания, хранения, передачи и обработки больших объемов информации, как в сетях общего пользования, так и в корпоративных сетях. Широко развивающиеся в последнее время облачные технологии и так называемый «интернет вещей» требуют для обеспечения своего функционирования определенной информационно-телекоммуникационной инфраструктуры, базирующейся на высокоскоростных сетях передачи данных. При этом, как правило, такими сетями передачи данных служат виртуальные частные сети (VPN). Ключевыми информационными объектами сети (ИОС) рассматриваемой информационно-телекоммуникационной инфраструктуры являются хранилища информации и центры обработки данных, а также маршрутизаторы и коммутаторы пакетов VPN-сети. Развитие и совершенствование технической базы информационных систем сопровождается острыми конфликтами в информационном пространстве. Именно ИОС являются объектами информационных угроз целями информационных атак противников в информационных конфликтах. Атак, реализация которых влечет за собой существенные финансовые и материальные потери. Поэтому проблема обеспечения целостности и конфиденциальности информационных массивов ИОС является **актуальной** для поставщиков информационных услуг.

Вопросам защиты информации (ЗИ) уделяется значительное внимание в трудах отечественных и зарубежных ученых. К настоящему времени подготовлена методическая база, созданы различные программные и аппаратные средства ЗИ (СЗИ) на ИОС. Проводимые в этой области исследования однозначно позволяют добиться требуемого уровня защиты при тривиальном наращивании количества СЗИ на ИОС. Однако данный подход не учитывает экономические затраты на защиту информации. С дру-

гой стороны, учет важности различных ИОС с точки зрения экономических рисков в условиях ограниченности бюджета на защиту информации требует разработки методического аппарата оптимального размещения СЗИ по критерию минимальной достаточности. Поэтому диссертационная работа Ковалева М.С., посвященная научному обоснованию 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 организациями – поставщиками IT-услуг.

2. Основные результаты, полученные соискателем и представленные к защите.

1. Аналитические и имитационная модели воздействия нарушителя на многоэшелонированную систему защиты информации в информационных объектах сети.
2. Методика оптимизации размещения средств защиты информации на информационных объектах сети, позволяющая повысить эффективность функционирования защиты информации без дополнительных существенных затрат ресурсов.

3. Научная новизна, обоснованность и достоверность результатов.

Результаты диссертационного исследования обладают **научной новизной.**

Во-первых, разработанные аналитические модели воздействия противника в информационном конфликте построены на основе математического аппарата конечных марковских цепей, что позволяет, в отличие от известных подходов, 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.

Во-вторых, оптимизация размещения разнотипных и разнородных средств защиты на информационных объектах сети, содержащих большие массивы информации различной важности, в отличие от известных подходов, впервые выполнена на основе пошаговой процедуры, реализующей сочетание динамического и вероятностно-игрового методов;

Достоверность результатов подтверждается совпадением основных получаемых результатов с результатами ручного счета известными апробированными математическими методами, корректностью и логической обоснованностью постановки частных подзадач исследования и принятых допущений. Ценно, что все разработанные модели и методика доведены до программной реализации и могут быть непосредственно

использованы для модернизации существующих и разработки перспективных сетевых СЗИ.

4. Практическая значимость результатов диссертационного исследования заключается в том, что только за счет оптимизации размещения имеющихся средств защиты (без дополнительных финансовых затрат) уровень ущерба, который может быть нанесен информационным ресурсам в исследуемом ИОС, может быть снижен на 17 … 25%. Также практическая ценность научных результатов подтверждается актами об их внедрении в ОКР промышленности и в учебном процессе ВУЗа.

Результаты исследований представляют практический интерес для научно-исследовательских учреждений и проектных организаций с целью усовершенствования существующих и создания перспективных адаптивных систем защиты информации. 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 телекоммуникационного профиля РФ (АО «КНИИ ТМУ», МОУ «ИИФ», АО «НИИ ССУ») при техническом обосновании размещения существующих средств защиты информации в узлах коммутации VPN сети общего и специального назначения, а также организациями промышленности (АО «Концерн «Созвездие»», АО «ЦНИИ ЭИСУ», АО «Ростелеком», АО «Воентелеком» и др.) при комплексном оснащении создаваемых центров коммутации и обработки данных СЗИ различного профиля.

5. Анализ содержания диссертации

Диссертационная работа по содержанию соответствует паспорту специальности 05.12.13 «Системы, сети и устройства телекоммуникаций». Основные результаты диссертационной работы соответствуют области исследования п.10 паспорта указанной специальности (исследование и разработка новых методов защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций).

Содержание автореферата соответствует основным положениям работы и позволяет вынести обоснованное представление о диссертации в целом.

Основные результаты диссертации достаточно широко и полно опубликованы в научной печати и апробированы на представительных международных и всероссийских

научно-технических конференциях. Требования ВАК о наличии публикаций в изданиях, список которых утвержден ВАК, выполнено.

6. Замечания по диссертации

1. В автореферате не уделено внимания альтернативным вариантам постановки задачи оптимизации размещения СЗИ на ИОС, имеющим место в первом разделе диссертации.

2. В диссертации не приводятся аналитические модели оценки коэффициента относительной важности, хранимой на ИОС информации. Таким образом, не ясно, из каких соображений формируются исходные данные для определения частных ущербов, наносимых злоумышленниками.

Досадный перечень недостатков, не украшающих работу и затрудняющих восприятие материала, можно и продолжить, и расширить. И нельзя утверждать, что недостатки не снижают качества рецензируемой работы. Но следует также отметить и то, что эти недостатки не отрицают справедливости выводов и не порочат положений, вынесенных автором на защиту. Поэтому работу в целом можно оценить положительно.

Дальнейшие исследования целесообразно продолжить в области комплексного применения СЗИ объектов сети и телекоммуникационной среды передачи данных.

7. Оценка работы в целом.

1. Диссертационная работа по форме и содержанию, актуальности, полноте поставленных и решенных задач, совокупности новых научных результатов отвечает требованиям п.п. 9, 10, 11, 13, 14 «Положения о присуждении ученых степеней», предъявляемым ВАК к кандидатским диссертациям, является научно-квалификационной работой, в которой содержится решение научной задачи 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, имеющей важное значение для телекоммуникационной инфраструктуры РФ.

2. Автор диссертационной работы, Ковалев Максим Сергеевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 «Системы, сети и устройства телекоммуникаций».

Официальный оппонент
доктор технических наук, профессор
Московского авиационного института
(национального исследовательского университета) А.И. Куприянов

01 сентября 2017 г.

Подпись профессора Александра Ильича Куприянова удостоверяю

Начальник отдела кадров
Московского авиационного института
(национального исследовательского университета) О.В. Носова

01 сентября 2017 г.

Московский авиационный институт (национальный исследовательский университет)
МАИ
Юридический адрес: 125993 Москва, Волоколамское шоссе, д. 4, А-80, ГСП-3.
Телефон организации: +7 (499) 158-43-33
Email МАИ: mai@mai.ru
Официальный сайт МАИ: http://www.mai.ru
Телефон официального оппонента: 8 910 469 09 55
Email официального оппонента: aik125167@mail.ru