УТВЕРЖДАЮ
Научный руководитель
АО «Концерн «Созвездие»
доктор технических наук,
член-корреспондент РАН
В.И. Борисов
«09» 2017 г.

ОТЗЫВ

на автореферат диссертации Ковалева Максима Сергеевича, выполненной на тему «Оптимизация размещения средств защиты информации в узлах коммутации VPN сети», представленной на соискание ученой степени кандидата технических наук по специальности 05.12.13 «Системы, сети и устройства телекоммуникаций»

В настоящее время информационные технологии пронизывают все сферы деятельности общества: хозяйственную, политическую, социальную, образовательную и другие, что обеспечивает государству и обществу существенное движение вперед. С другой стороны, информационные технологии подвержены различным деструктивным воздействиям, что в потенциале несет в себе огромный ущерб государству и обществу в указанных сферах, в том числе и материальный.

Информационные технологии, как правило, требуют информационного обмена его участников в рамках некоторой коммуникационной среды. В настоящее время в качестве такой среды выступают мультисервисные сети, базирующиеся на технологии коммутации пакетов и обеспечивающие пользователям весьма разнообразный набор услуг. Корпоративные профильные секторы в мультисервисной сети реализуются в виде частных выделенных сетей (VPN -- сетей). Однако VPN – сети также являются объектами атак нарушителей, имеющих целью либо профильную информацию на серверах сети, либо деградацию самой сети, например, через воздействия на её маршрутизаторы или другие информационные объекты сети (ИОС).

Защита информации на ИОС в узлах VPN – сети реализуется путем размещения комплекса средств защиты информации (СЗИ). Исходя из изложенного, диссертационная работа Ковалева М.С., решающая задачу научного обоснования совокупности 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.

В ходе выполнения работы автором были получены научные результаты, обладающие научной новизной и практической ценностью:

1. 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.

2. 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.

Практическая ценность результатов работы определяется их реализацией в НИР и ОКР промышленности, а также в учебном процессе ВУЗа, что подтверждается соответствующими актами о внедрении.

Полнота публикаций и апробаций материалов диссертационной работы подтверждают достоверность полученных научных результатов, которые опубликованы в 31 труде, из них 5 статей в журналах из Перечня ВАК.

Автореферат написан строгим научным языком и достаточно полно отражает сущность проведенных исследований. Материал изложен логично, результаты взаимосвязаны. Формулировка научной задачи, постановка частных подзадач исследования, их решение и выводы аргументированы.

По автореферату диссертации Ковалева М.С. можно выявить следующие недостатки работы:

1. Из материалов автореферата неясно, насколько применимы разработанные модели воздействия нарушителя и методика размещения СЗИ наряду с VPN - сетями

к сетям связи другого типа, например, радиосетям.

2. Из материалов автореферата неясно, на какой стадии жизненного цикла VPN - сети применимы разработанные модели и методика.

В целом по автореферату можно сделать вывод о том, что диссертационная работа Ковалева М.С. является законченной научно-квалификационной работой, содержащей решение научной задачи по оптимизации размещения средств защиты информации в узлах коммутации VPN - сети, что имеет важное значение для телекоммуникационной инфраструктуры РФ.

Диссертация отвечает 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».

Отзыв составили:

Научный референт АО «Концерн «Созвездие»
Доктор технических наук, профессор

Николаев Валерий Иванович

Научный консультант
Кандидат технических наук

Буслов Сергей Дмитриевич