

УТВЕРЖДАЮ  
ВрИО начальника Военной академии связи  
полковник  
«28» июля 2017 г.  
С. Ишимов



**О Т З Ы В**  
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»

Развитие мирового сообщества наглядно демонстрирует, что в последнее время критически важным государственным ресурсом, оказывающим все большее влияние на национальную безопасность, становится информация, циркулирующая в автоматизированных системах управления и сетях, а также информация об их составе и структуре.

Внедрение новых технологий в автоматизированные системы управления и сети не только в значительной мере способствовало повышению эффективности их функционирования, но и открыло дополнительные возможности для реализации противником компьютерных атак (КА). Принято считать, что эффективное воздействие компьютерных атак должно обеспечить возможность навязать противостоящей стороне ложное видение обстановки, принудить ее действовать в невыгодных для нее условиях. Это

достигается в основном благодаря проведению комплекса мероприятий, позволяющих, с одной стороны, нарушить процесс принятия решений, а с другой - обрабатывать информацию по циклу принятия решений в своей системе управления эффективнее и быстрее, чем это может сделать противоборствующая сторона.

В таких условиях локально вычислительные сети должны при приемлемых экономических затратах обеспечивать решение задач защищенного функционирования, однако уже в настоящее время, становится очевидным обострение противоречия между разнообразием средств защиты информации, представленных на рынке, и устаревшими подходами их оптимального размещения в информационных объектах сети для обеспечения заданного уровня защищенности информации при минимуме их стоимости. Таким образом, на наш взгляд актуальность темы и задачи представленного исследования не вызывает сомнений.

Автором изучены и критически проанализированы известные достижения и теоретические положения других авторов по вопросам обеспечения защиты информации в сетях телекоммуникаций.

В качестве результатов исследования, выносимых автором на защиту, в автореферате представлены:

аналитические и имитационные модели воздействия нарушителя на многоэшелонированную систему защиты информации в информационных объектах сети (ИОС).

автоматизированная методика оптимизации размещения средств защиты информации на информационных объектах сети, позволяющая повысить эффективность функционирования защиты информации без дополнительных существенных финансовых затрат.

Новизна первого научного результата состоит в том, что разработанные аналитические модели воздействия нарушителя 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.

Новизна второго научного результата состоит в том, что оптимизация размещения разнотипных и разнородных средств защиты на информационных объектах сети, содержащих большое количество массивов информации различной важности, в отличие от известных подходов, впервые выполнена на основе пошаговой процедуры, реализующей сочетание динамического и вероятностно-игрового метода.

Практическая значимость работы заключается в том, что разработанные модели и методика позволяют снизить на 17-25% ущерб, который может быть нанесен информации, только за счет оптимизации размещения имеющихся средств защиты. Также результаты исследования представляют практический интерес при обосновании мероприятий по защите информационных объектов сети, разработке перспективных средств связи и средств защиты, применяемых в информационных объектах сети, а также в учебном процессе вузов в части касающейся обеспечения защищенного функционирования информационных объектов сети в условиях компьютерных атак.

Представленные в автореферате результаты опубликованы в 29 научных трудах, 5 из которых в изданиях, рецензируемых ВАК и приравненных к ним, в 1 отчете об ОКР, получен один патент на полезную модель.

Работа выполнена на высоком научном уровне, однако, имеет определенные недостатки.

1. Не предложена модель воздействия на элементы ИОС и не доказана опасность атаки типа «Несанкционированный доступ к информации», единственно учтенной в работе.

2. Отсутствует анализ зависимости целевой функции от варьируемых параметров оптимизации, поэтому не обнаружен их противоречивый характер. Учитывая это, вывод о том, что чем дороже система защиты информации, тем выше его эффективность противоречит практике, по этой причине и вероятностный ущерб снижен в 2 раза (стр. 14).

3. Отсутствуют научно-технические предложения по построению защищенной ИОС. Не рассмотрена возможность реализации аппаратно-программных средств защиты на технологическом уровне.

4. Отсутствует научно-методическое обеспечение, позволяющее оценить эффективность каждого средства защиты от воздействия различных атак.

5. Отсутствует приложение А, ссылка на которое приведена на странице 2 автореферата.

Указанные замечания по нашему мнению не снижают общей ценности диссертационной работы и не влияют на главные теоретические и практические результаты диссертации. Судя по автореферату, диссертационная работа является законченным научным трудом. Автор показал умение самостоятельно вести исследования в определенном научном направлении с доведением их до законченных технических решений. Результаты работы по нашему мнению в достаточной степени опубликованы, апробированы и реализованы. Автореферат написан грамотно и логически связно, оформлен в соответствии с требованиями.

Вывод: Диссертационная работа соответствует специальности 05.12.13 «Системы, сети и устройства телекоммуникаций» и отвечает критериям «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 г. № 842, а ее автор КОВАЛЕВ МАКСИМ СЕРГЕЕВИЧ заслуживает присуждения ему ученой степени кандидата технических наук.

Отзыв обсужден и одобрен на заседании 32 кафедры (безопасности инфокоммуникационных систем специального назначения) «21» июля 2017 года, протокол № 26.

Начальник 32 кафедры  
Военной академии связи  
(194064, Санкт-Петербург, Тихорецкий проспект, д. 3  
247-98-32, vas@mil.ru)

кандидат технических наук, доцент  
полковник

  
Чернов Дмитрий Владимирович

Преподаватель 32 кафедры  
Военной академии связи  
(194064, Санкт-Петербург, Тихорецкий проспект, д. 3  
247-98-32, vas@mil.ru)

кандидат технических наук  
подполковник

  
Лаута Олег Сергеевич