Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
Информатики и радиоэлектроники

УДК 004.056.5

Полещук
Виталий Сергеевич

Защита информационно-коммуникационных систем от информационных атак

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-45 80 01 «Системы, сети и устройства телекоммуникаций»

Научный руководитель
Ширинский Валерий Павлович
канд. техн. наук, доцент

Минск 2020

КРАТКОЕ ВВЕДЕНИЕ

Как известно, информация всегда являлась одним из важнейших ресурсов человечества, что порождало проблему обладания этим ресурсом, его изменения или уничтожения, исходя из государственных, коммерческих, частных и других интересов. Появление и бурное развитие технических средств обработки и передачи информации на основе цифровых технологий, соответственно, породило новые средства нападения или защиты, предназначенные для получения доступа к информации. Как следствие этого, острота проблемы обеспечения информационной безопасности (ИБ) субъектов информационных отношений, защиты их законных интересов при использовании информационных систем и сетей, хранимой, обрабатываемой и передаваемой в них информации постоянно возрастает. Несмотря на интенсивное внедрение новых технологических решений в области информационной безопасности, уровень криминогенности в информационной сфере сетей передачи данных ведущих стран мира постоянно повышается, что приводит к миллиардным финансовым потерям.

По данным координационного центра немедленного реагирования CERT, организованного при университете Карнеги - Меллона, ежегодно наблюдается рост количества регистрируемых информационных атак.

К основным причинам роста количества атак можно отнести следующие факторы:

- с каждым годом увеличивается количество пользователей общедоступных сетей связи, таких, как сеть Интернет. При этом в качестве новых пользователей выступают как отдельные клиентские рабочие станции, так и целые корпоративные сети;

- увеличивается количество уязвимостей, обнаруживаемых в существующем общесистемном и прикладном программном обеспечении;

- возрастает число возможных объектов атаки. Если некоторое время назад в качестве основных объектов несанкционированного воздействия рассматривались исключительно серверы стандартных Web-служб, такие как HTTP, SMTP и FTP, то к настоящему моменту разработаны средства реализации атак на маршрутизаторы, коммутаторы, межсетевые экраны и др.;

- упрощение методов реализации информационных атак. В сети Интернет можно без труда найти простые в использовании программные реализации атак, направленных на активизацию различных уязвимостей.

- увеличение числа внутренних атак со стороны пользователей инфокоммуникационных систем (ИКС). Примерами таких атак является кража

конфиденциальной информации или запуск вредоносного ПО на рабочих станциях пользователей.

Необходимо также отметить, что уровень сложности информационных атак также постоянно растет. Так, в момент своего первого появления в 1980 г. вирусы представляли собой достаточно простые программы, основной задачей которых было нарушение работоспособности системы. В настоящее же время компьютерные вирусы представляют значительно более сложные программы, способные к распространению практически в любой среде передачи данных, а также маскироваться под работу штатного ПО. Кроме этого, современные разновидности компьютерных вирусов в большинстве своем используются для кражи конфиденциальной информации, а также для получения несанкционированного доступа к пользовательским компьютерам. Такая же эволюция присуща и для другим видам угроз безопасности, для реализации которых постоянно создаются новые и более изощренные средства проведения атак.

С учетом вышесказанного можно с уверенностью утверждать, что проблема защиты информационно-коммуникационных систем от информационных атак является одной из наиболее актуальных и значимых в области индустрии интернет-технологий (ИТ-индустрии).

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Работа выполнялась по теме: «Защита информационно-коммуникационных систем от информационных атак».

Проведенная работа по диссертационной тематике соответствует мировым тенденциям в области обеспечения информационной безопасности в сетях связи, а также Приоритетным направлениям фундаментальных и прикладных научных исследований РБ на 2016-2020 гг. в части подраздела «Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантокриптографической системы»

Целью диссертации являлась разработка общей методики выбора и внедрения систем предотвращения атак в ИКС, а также разработка способов обеспечения высокой производительности данных систем .

Для достижения цели были решены следующие задачи:

- проведен обзор литературы и описаны основные угрозы информационно-коммуникационным системам в части информационных атак;
- проанализированы современные стандарты и методики в области анализа защищенности ИКС;

- определены критерии выбора систем обнаружения и предотвращения атак и предложена методика их выбора, обоснованная конкретными примерами;

- разработан комплексный метод повышения производительности систем предотвращения атак путем определения оптимальных значений конфигурационных параметров системного и прикладного ПО, а также выбора наиболее подходящего аппаратного обеспечения.

Научная новизна работы состоит в разработке детальной методики повышения производительности рабочих станций применительно к их использованию в составе систем предотвращения атак. Данная методика может быть практически использована при внедрении таких систем.

Основные положения и результаты магистерской работы докладывались и обсуждались на 55-й научной конференции аспирантов, магистрантов и студентов; XVII Белорусско-российской научно-технической конференции «Технические средства защиты информации».

КРАТКОЕ СОДЕРЖАНИЕ

Во введение рассматривается проблема информационной безопасности на современном этапе технического развития общества, обосновывается актуальность выбранной темы диссертационной работы.

В общей характеристике работы сформирована цель, научная новизна, практическая ценность данной диссертационной работы, а также основные задачи, используемые для достижения поставленной цели.

Первая глава «Основные понятия и определения в области защиты от информационных атак» включает в себя обзор основных понятий в области защиты информации, описание основных видов уязвимостей ИКС и этапов атакующих воздействий.

Во второй главе - «Современные средства и методы защиты от информационных атак» приводятся описания средств и методов защиты от информационных атак, предназначенных для использования на различных участках структуры ИКС.

Третья глава «Системы обнаружения и предотвращения атак» посвящена классификации данных систем, их структуре и архитектуре, а также применяемым в них методам выявления атак.

Четвертая глава «Противодействие выявленным атакам» освещает методы реагирования систем обнаружения и предотвращения атак на попытки злонамеренного воздействия на ИКС.

Пятая глава «Проблемы выбора систем предотвращения информационных атак» охватывает процесс выбора систем предотвращения

атак, включая критерии, определяющие этот выбор, с приведением конкретных примеров и обоснованием принятого решения. Также в подразделе 5.2.6 разработана методика практического увеличения производительности СПА путем выбора оптимальных значений параметров конфигурации аппаратного обеспечения, системного и прикладного ПО системы предотвращения атак, подтвержденная результатами стендовых испытаний.

ЗАКЛЮЧЕНИЕ

В ходе написания диссертации были рассмотрены различные виды уязвимостей и информационных атак в сетях инфокоммуникаций, а также основные методы и средства борьбы с ними . Подробно освящена роль систем предотвращения атак в системе защиты информации, приведена их классификация, структура и принципы работы. Проработан вопрос выбора таких систем, включая основные критерии выбора, с обоснованием решения на основе конкретных примеров; создана методика повышения производительности рабочих станций применительно к их использованию в составе систем предотвращения атак.

В результате проведенной работы можно сделать вывод, что при оптимальной настройке рабочей станции и самой СПА, современные решения с открытым исходным кодом являются весьма эффективными средствами борьбы с информационными атаками, и будут в дальнейшем широко применяться и интенсивно развиваться.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Полещук В.С. Защита информационно-коммуникационных систем от информационных атак / Полещук В.С. // Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 22- 26 апреля 2019 г., БГУИР, Минск

2-А. Полещук В.С., Ширинский В.П., Некрашевич И.Г. Концепция адаптивного управления безопасностью / Полещук В.С., Ширинский В.П., Некрашевич И.Г. // Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 22-26 апреля 2019 г., БГУИР, Минск