Овсянников Р.Я. Современные методы защиты от сетевых атак: анализ эффективных стратегий и инструментов // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 4(54) с. 142–146

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК: АНАЛИЗ ЭФФЕКТИВНЫХ СТРАТЕГИЙ И ИНСТРУМЕНТОВ

Овсянников Р.Я.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: rovsyannikov23@gmail.com

В современном мире количество сетевых атак стремительно растет, что требует эффективных методов защиты для предотвращения угроз и минимизации ущерба. В статье рассматриваются основные виды атак на сетевую инфраструктуру, приложения и пользователей, а также анализируются современные методы защиты, включая фильтрацию трафика, системы обнаружения вторжений, шифрование данных, сегментацию сетей и управление уязвимостями. Особое внимание уделено вопросам мониторинга безопасности и правового регулирования. Рассмотрены перспективы развития кибербезопасности, а также даны рекомендации по повышению защищенности сетевых систем.

Ключевые слова: Кибербезопасность, сетевые атаки, защита данных, шифрование, мониторинг безопасности, управление уязвимостями, правовое регулирование.

MODERN METHODS OF PROTECTION AGAINST NETWORK ATTACKS: ANALYSIS OF EFFECTIVE STRATEGIES AND TOOLS

Ovsyannikov R.Ya.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: rovsyannikov23@gmail.com

In the modern world, the number of network attacks is rapidly increasing, requiring effective protection methods to prevent threats and minimize damage. This article examines the main types of attacks on network infrastructure, applications, and users, as well as analyzes modern protection methods, including traffic filtering, intrusion detection systems, data encryption, network segmentation, and vulnerability management. Special attention is paid to security monitoring and legal regulations. The prospects for cybersecurity development are considered, and recommendations are provided for enhancing network security.

Keywords: Cybersecurity, network attacks, data protection, encryption, security monitoring, vulnerability management, legal regulation.

Введение

В условиях стремительного развития цифровых технологий и роста количества подключенных устройств проблема сетевой безопасности приобретает особую актуальность. Современные кибератаки становятся все более сложными и изощренными, что требует от организаций и частных пользователей применения эффективных мер защиты для предотвращения несанкционированного доступа, утечки данных и разрушительных последствий. Согласно статистике, число инцидентов, связанных с нарушением

кибербезопасности, ежегодно увеличивается, а финансовый и репутационный ущерб от атак продолжает расти.

Сетевые атаки представляют собой широкий спектр угроз, направленных на компрометацию сетевой инфраструктуры, нарушение работы сервисов, хищение конфиденциальных данных и манипуляцию информационными потоками. Вредоносные действия злоумышленников могут включать DDoS-атаки, перехват данных, использование уязвимостей программного обеспечения, фишинг, внедрение вредоносного кода и атаки на сетевые протоколы. В связи с этим разработка и внедрение современных механизмов защиты становится необходимым условием для обеспечения безопасного функционирования цифровых систем.

Цель данной статьи — проанализировать основные виды сетевых атак, рассмотреть традиционные и современные методы защиты, а также оценить перспективные направления развития кибербезопасности. В работе рассматриваются как технические, так и организационные меры, направленные на повышение устойчивости сетевой инфраструктуры к угрозам. Особое внимание уделяется мониторингу сетевого трафика, управлению уязвимостями, сегментации сетей, использованию криптографических методов защиты и внедрению стандартов безопасности.

Таким образом, защита от сетевых атак требует комплексного подхода, включающего превентивные меры, своевременное выявление угроз и эффективные механизмы реагирования. В статье представлена подробная классификация атак, анализируются наиболее распространенные методы противодействия им, а также рассматриваются правовые аспекты регулирования кибербезопасности.

Основные виды сетевых атак

Современные киберугрозы охватывают широкий спектр атак, направленных на нарушение работы сетевой инфраструктуры, компрометацию данных и манипуляцию информацией. Эти атаки можно условно разделить на несколько категорий: атаки на уровень сетевой инфраструктуры, атаки на уровень приложений и атаки, нацеленные на конечных пользователей.

Одной из наиболее распространенных угроз являются атаки на уровень сетевой инфраструктуры, в том числе DDoS-атаки, направленные на перегрузку серверов и отказ в обслуживании пользователей. Такие атаки, как UDP Flood, SYN Flood и HTTP Flood, используют массовые запросы для истощения ресурсов сети. Вредоносный трафик создается с помощью ботнетов, объединяющих тысячи зараженных устройств. Еще одной серьезной угрозой является компрометация сетевых протоколов, например, атаки на маршрутизаторы и коммутаторы, такие как BGP Hijacking и ARP Spoofing. Они позволяют злоумышленникам перенаправлять трафик, подменять данные и перехватывать конфиденциальную информацию.

На уровне приложений особую опасность представляют инъекционные атаки, такие как SQL-инъекции и межсайтовый скриптинг (XSS). SQL-инъекции используются для внедрения вредоносных команд в базы данных, что позволяет хакерам извлекать, модифицировать или удалять критически важную информацию. Атаки XSS, в свою очередь, направлены на внедрение вредоносных скриптов в веб-страницы, что может привести к краже данных пользователей или выполнению несанкционированных действий от их имени. Другим видом

атак являются атаки на веб-сессии, например, перехват cookies или угон сессий (Session Hijacking), что позволяет злоумышленникам получить доступ к аккаунтам пользователей.

Не менее опасны атаки, нацеленные на пользователей, которые чаще всего связаны с методами социальной инженерии. Фишинговые атаки представляют собой попытки обманным путем получить учетные данные пользователей через поддельные веб-сайты, электронные письма или сообщения. Вредоносные ссылки, замаскированные под легитимные ресурсы, могут приводить к загрузке вредоносного программного обеспечения или передаче персональных данных злоумышленникам. Еще одной распространенной угрозой является манипуляция с DNS (DNS Spoofing, Cache Poisoning), позволяющая перенаправлять пользователей на поддельные сайты для кражи их данных.

Таким образом, разнообразие сетевых атак требует комплексного подхода к защите, включающего мониторинг сетевого трафика, своевременное выявление угроз и использование надежных механизмов защиты данных. В следующих разделах рассматриваются эффективные методы противодействия данным атакам [1].

Классические методы защиты от сетевых атак

В современных условиях обеспечение кибербезопасности требует применения комплексных методов защиты, направленных на предотвращение атак, обнаружение угроз и быстрое реагирование на инциденты. Эффективная защита включает несколько ключевых направлений: фильтрацию трафика, аутентификацию и шифрование, мониторинг безопасности, управление уязвимостями, сегментацию сети и использование специализированных защитных систем [2].

Одним из фундаментальных методов защиты является фильтрация сетевого трафика, которая позволяет выявлять и блокировать вредоносную активность. Для этого применяются межсетевые экраны (firewalls), которые контролируют входящий и исходящий трафик на основе заранее заданных правил. Помимо традиционных файрволов, используются системы глубокого анализа пакетов (DPI), позволяющие анализировать содержимое трафика и блокировать подозрительные соединения. Специализированные решения, такие как системы предотвращения вторжений (IPS) и обнаружения вторжений (IDS), помогают выявлять аномалии и блокировать попытки компрометации сети.

Не менее важной мерой является аутентификация и шифрование данных, которые защищают информацию от несанкционированного доступа. Для этого применяются многофакторная аутентификация (MFA), криптографические протоколы (TLS, IPsec) и механизмы безопасного хранения паролей. Шифрование данных при передаче предотвращает их перехват злоумышленниками, а цифровые сертификаты гарантируют подлинность участников обмена данными [3].

Мониторинг безопасности и анализ аномалий играют ключевую роль в своевременном обнаружении атак. Современные системы безопасности используют поведенческий анализ и технологии машинного обучения для выявления подозрительной активности. Логирование событий и анализ сетевого трафика позволяют отслеживать попытки вторжений, а также обеспечивать оперативное реагирование на инциденты. Особую роль в мониторинге играют Security Information and Event Management (SIEM) системы, которые централизованно собирают и анализируют данные о безопасности из различных источников.

Еще одним важным аспектом является управление уязвимостями, включающее регулярные обновления программного обеспечения, патчинг критических уязвимостей и контроль конфигураций сетевых устройств. Использование автоматизированных сканеров уязвимостей позволяет выявлять слабые места в инфраструктуре и устранять их до того, как они будут использованы злоумышленниками.

Сегментация сети и контроль доступа помогают минимизировать риски распространения атак внутри инфраструктуры. Разделение сети на логические сегменты с ограничением доступа между ними снижает вероятность компрометации всей системы при атаке на один из узлов. Использование принципа минимально необходимого доступа (Least Privilege) и ролевой модели управления доступом (RBAC) предотвращает несанкционированное использование ресурсов.

Дополнительно, для защиты от DDoS-атак применяются специализированные анти-DDoS решения, которые анализируют трафик и автоматически фильтруют вредоносные запросы. Такие технологии используют эвристические алгоритмы и искусственный интеллект для адаптивного реагирования на угрозы.

Таким образом, защита от сетевых атак требует комплексного подхода, включающего технические, организационные и административные меры. Современные методы безопасности направлены не только на предотвращение атак, но и на их быстрое выявление и устранение последствий, что позволяет минимизировать ущерб и обеспечивать надежную работу сетевой инфраструктуры [4].

Итоги и перспективы развития кибербезопасности

Сетевые атаки продолжают эволюционировать, становясь все более сложными и изощренными, что требует постоянного совершенствования методов защиты. В результате анализа современных угроз можно сделать вывод о необходимости комплексного подхода к обеспечению кибербезопасности, включающего фильтрацию трафика, многоуровневую аутентификацию, шифрование данных, мониторинг активности и эффективное управление уязвимостями [5].

Одним из ключевых трендов в развитии защиты от сетевых атак является интеграция технологий искусственного интеллекта и машинного обучения в системы кибербезопасности. Современные алгоритмы позволяют в реальном времени анализировать большие объемы данных, выявлять аномалии и предсказывать потенциальные атаки на основе поведения пользователей и сетевого трафика. Автоматизированные системы реагирования помогают оперативно блокировать угрозы, снижая нагрузку на специалистов по безопасности.

Еще одним перспективным направлением является развитие концепции Zero Trust, которая предполагает полный контроль и верификацию всех пользователей и устройств перед предоставлением доступа к ресурсам. Этот подход минимизирует риски атак за счет строгого разграничения прав доступа и постоянного мониторинга активности в сети.

Кроме того, значительную роль играет развитие международного сотрудничества в сфере кибербезопасности. Разработка единых стандартов защиты, обмен информацией об угрозах и координация действий между государственными и частными организациями позволяют быстрее реагировать на новые угрозы и обеспечивать высокий уровень защиты критической инфраструктуры.

Необходимость постоянного обучения и повышения осведомленности пользователей также остается важным фактором в обеспечении безопасности. Большая часть атак, таких как фишинг и социальная инженерия, становится возможной из-за человеческого фактора. Развитие программ киберграмотности и внедрение строгих политик безопасности на предприятиях помогут снизить риск успешных атак.

Таким образом, перспективы развития кибербезопасности связаны с внедрением новых технологий, усилением контроля доступа, развитием международного сотрудничества и повышением уровня осведомленности пользователей. В условиях быстро меняющейся цифровой среды обеспечение надежной защиты данных и сетевой инфраструктуры остается приоритетной задачей, требующей комплексного подхода и постоянного совершенствования методов защиты.

Список литературы

1. Алехин Р. В. и др. Анализ защищенности облачной инфраструктуры openstack при эмуляции атаки вида ddos на узлах инфраструктуры //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 52-55.
2. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2015. – С. 193-197.
3. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
4. Ковалев И. А., Косов Н. А. Состязательные атаки в нейронных сетях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 490-492.
5. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.

References

1. Alekhin R. V. et al. Analysis of the security of the openstack cloud infrastructure during the emulation of a ddos attack on infrastructure nodes //Actual Problems of Infocommunications in Science and Education (APINO 2023). – 2023. – pp. 52-55.
2. Andrianov V. I., Romanov G. G., Shterenberg S. I. Expert Systems in the Field of Information Security //Actual Problems of Infocommunications in Science and Education. – 2015. – pp. 193-197.
3. Volkogonov V. N., Gelfand A. M., Derevyanko V. S. Relevance of Automated Control Systems //Actual Problems of Infocommunications in Science and Education (APINO 2019). – 2019. – pp. 262-266.
4. Kovalev I. A., Kosov N. A. Adversarial Attacks in Neural Networks //Actual Problems of Infocommunications in Science and Education (APINO 2021). – 2021. – pp. 490-492.
5. Orlov G. A., Krasov A. V., Gelfand A. M. Application of Big Data in the Analysis of Large Data in Computer Networks //Knowledge-Intensive Technologies in Earth Space Research. – 2020. – Vol. 12. – No. 4. – pp. 76-84.