УДК 621.396.41

РОЛЬ СЕТЕВОЙ БЕЗОПАСНОСТИ В БОРЬБЕ С КИБЕРПРЕСТУПЛЕНИЯМИ

***Иминов А.А, Исаков А. Ф., Рахмонбердиев Б. Б.*[1],**

Аннотация. В современном цифровом мире киберпреступности уделяется все больше внимания в связи с её растущим влиянием на индивидуальную и корпоративную безопасность. Настоящая статья посвящена анализу роли сетевой безопасности в предотвращении и борьбе с киберпреступлениями. Авторы рассматривают сетевую безопасность не просто как совокупность технических инструментов и протоколов, но и как стратегический элемент, интегрированный в общую систему управления рисками, который требует комплексного подхода, включающего правовые, технические и образовательные аспекты.

Ключевые слова. Киберпреступления, информационная безопасность, борьба с фишингом, DDoS-атаки, сетевая безопасность.

Киберпреступления являются значительной угрозой для отдельных лиц, корпораций и государственных институтов. Прогресс в области цифровых технологий способствует увеличению объема и комплексности кибератак, что, в свою очередь, акцентирует необходимость в разработке и реализации адекватных стратегий сетевой безопасности. Под сетевой безопасностью понимается совокупность мер, направленных на обеспечение защиты сетевой инфраструктуры и данных от несанкционированного доступа, эксплуатации, раскрытия, нарушения целостности, модификации или уничтожения [1].

Основная часть проблем в области безопасности проистекает из действий злоумышленников, стремящихся получить незаконную выгоду или нанести ущерб другим лицам. Разнообразие типологий нарушителей, представленных в таблице 1, наглядно демонстрирует, что обеспечение сетевой безопасности подразумевает гораздо более широкий спектр действий, нежели исключительно исправление программных уязвимостей.

Все эти аспекты (секретность, аутентификация, обеспечение строгого выполнения обязательств и обеспечение целостности) встречаются и в традиционных системах, но с некоторыми существенными отличиями. Секретность и целостность достигаются с помощью заказных писем и хранения документов в несгораемых сейфах.

К основным угрозам кибербезопасности относятся:

К основным угрозам кибербезопасности, с которыми сталкиваются организации и индивидуальные пользователи в современном цифровом мире, относятся:

1. Вирусы и вредоносное программное обеспечение (ПО): Эти программы способны заражать, повреждать данные, управлять устройствами без ведома пользователя и могут быть распространены через электронную почту, веб-сайты, загрузки файлов и USB-накопители.

2. Фишинг: Метод социальной инженерии, целью которого является обман пользователей для получения конфиденциальной информации, такой как пароли и данные банковских карт, путём маскировки под доверенный источник в электронной почте, сообщениях или на веб-сайтах.

3. Атаки типа «отказ в обслуживании» (DDoS): Направлены на перегрузку целевых веб-сайтов, серверов или сетевой инфраструктуры массовым количеством запросов, что приводит к их недоступности для законных пользователей.

4. Программы-вымогатели (ransomware): шифруют данные на зараженном устройстве и требуют выкуп за восстановление доступа к данным. Распространение таких атак усилилось, поражая как индивидуальных пользователей, так и крупные организации.

5. Утечки данных: Несанкционированный доступ к конфиденциальным данным и их распространение или продажа. Утечки могут произойти из-за ошибок в конфигурации системы, уязвимостей безопасности или внутренних угроз.

6. Атаки с использованием нулевого дня (Zero-day exploits): Эксплуатация неизвестных до момента атаки уязвимостей в программном обеспечении или операционной системе, что делает их особенно опасными, поскольку для них ещё не разработаны патчи или обновления безопасности.

7. Инсайдерские угрозы: Действия сотрудников или партнёров, которые имеют доступ к корпоративным системам и могут нанести ущерб, намеренно или по невнимательности.

8. Социальная инженерия остается одним из самых распространенных методов атак на организации (50%) и частных лиц (91%). Основными путями атак с использованием социальной инженерии являются электронная почта (86 %) для организаций и веб-ресурсы и сервисы (59 %) для частных лиц (см. диаграмму 1).

9. Расширенные постоянные угрозы (APT): Долгосрочные целенаправленные кампании, в ходе которых атакующий получает несанкционированный доступ к сети и остаётся незамеченным в течение длительного времени.

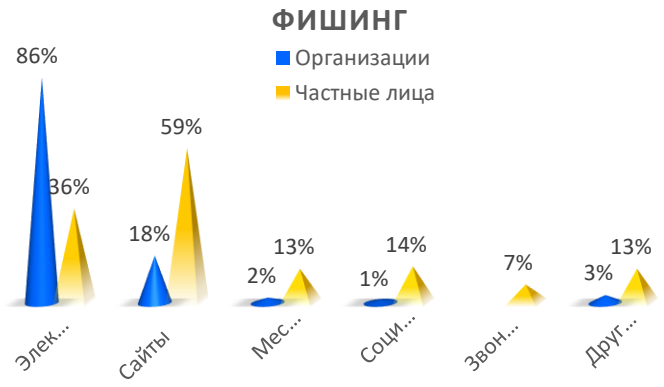

Диаграмма 1. Распределение фишинга
по категориям [2]

Сетевая безопасность является ключевой компонентой защиты информационных систем и данных в цифровую эпоху. Она включает в себя множество технологий, протоколов и практик, разработанных для защиты сетевой инфраструктуры и данных, передаваемых через компьютерные сети, от различных угроз и атак. Основная цель сетевой безопасности — предотвращение несанкционированного доступа, злоупотреблений, модификации, уничтожения или перехвата данных [3]. Основные элементы сетевой безопасности:

1. Межсетевой экран (Firewall): работает как барьер между защищенной внутренней сетью и внешним миром, контролируя входящий и исходящий трафик на основе заранее установленных правил безопасности.

2. Антивирусное и антималварное ПО: Предназначено для обнаружения, предотвращения и устранения вредоносного ПО, включая вирусы, черви, троянские кони и шпионское ПО.

3. Системы обнаружения и предотвращения вторжений (IDS/IPS): анализируют трафик в сети для выявления подозрительных действий или атак и могут автоматически предпринимать действия для их блокирования или смягчения последствий.

4. Шифрование данных: используется для защиты конфиденциальности данных при их передаче по сети или при хранении, преобразуя информацию в зашифрованный вид, который можно прочитать только с помощью соответствующего ключа.

5. Многофакторная аутентификация: требует от пользователя предоставления двух или более факторов аутентификации для доступа к ресурсам сети, увеличивая таким образом уровень защиты от неавторизованного доступа.

Эти данные, будучи продуктом информационных технологий, представляют собой неконнектные сведения о различных объектах, действуя в качестве дискретных элементов в цифровой среде[4]. В последние годы наблюдался значительный рост числа кибератак, что отражает увеличивающуюся активность киберпреступников и расширение их методов. Основные тенденции включали:

Рост фишинговых атак: Фишинг оставался одним из наиболее распространённых методов кибератак, при этом злоумышленники стали использовать более изощрённые методы социальной инженерии для обмана пользователей и получения конфиденциальной информации.

Увеличение числа атак с использованием программ-вымогателей (ransomware): Эти атаки продолжили набирать обороты, целясь как в крупные организации, так и в малый и средний бизнес. Злоумышленники шифровали данные жертв и требовали выкуп за их восстановление.

Рост числа DDoS-атак: Атаки типа «отказ в обслуживании» становились всё более масштабными и сложными, нацеленными на нарушение работы веб-сайтов и онлайн-сервисов.

Увеличение инцидентов, связанных с утечками данных: Несмотря на усилия по укреплению защиты данных, утечки конфиденциальной информации продолжали происходить, затрагивая миллионы пользователей.

По последним данным за 2021-2023 международной организации Positive Technoliogies количество кибератак с вредоносном кодом «шировальщик» снизилось на 13% (см. диаграмму 2).

Диаграмма 2. Количество атак вымогателей (по кварталам)[5]

Система обеспечения безопасности должна обладать функционалом для верификации аутентичности сообщений, таких как «Оплатите счета до пятницы», определяя, исходят ли они действительно от налоговых органов, или же представляют собой мошенническую имитацию. Дополнительно, задачи систем безопасности включают в себя противодействие атакам, связанным с

перехватом и повторной отправкой сообщений, а также с попытками лиц отрицать факт отправления ими данных сообщений.

Системы обнаружения и предотвращения вторжений (IDPS) в сетевом исполнении обычно встраиваются непосредственно в сетевую архитектуру и выполняют анализ сетевых пакетов с целью выявления атак[6].

Эти системы способны перехватывать все пакеты данных в определённом сегменте сети, включая те, что передаются через коммутационные узлы. IDPS восстанавливает и анализирует потоки трафика, выявляя шаблоны, указывающие на вредоносную активность, и оснащены функционалом для логирования активности и генерации уведомлений или предупреждений о подозрительных событиях. Ключевые преимущества сетевых IDPS включают в себя:

1. Анализ пакетов: Сетевые IDPS проводят детальный анализ пакетов, проверяя заголовки IP-пакетов на наличие вредоносных элементов. Это обеспечивает возможность выявления распространённых типов атак, в том числе атак типа «отказ в обслуживании» (DoS). Например, в случае DoS-атаки совпадение адресов источника и назначения, а также портов источника и назначения с адресами целевого устройства может привести к попытке устройства установить соединение само с собой, что замедляет его работу или даже выводит из строя. Дополнительно, IDPS могут анализировать конкретные команды, содержащиеся в полезной нагрузке IP-пакетов.

2. Обнаружение и реагирование в реальном времени: Сетевые IDPS обладают способностью к обнаружению атак в момент их осуществления и обеспечивают возможность немедленного реагирования. К примеру, при запуске TCP-атаки на основе DoS, IDPS может прервать атаку, инициируя сброс TCP-соединения.

3. Удаление вредоносного содержимого: Сетевые IDPS могут не только обнаруживать подозрительные элементы в трафике, но и удалять или заменять их. Например, при обнаружении электронного письма с заражённым вложением, система может удалить вредоносный файл, заменив его на «чистую» копию сообщения.

4. Фиксация доказательств для судебного преследования: Сетевые IDPS способны отслеживать трафик в режиме реального времени, что позволяет фиксировать атаки без возможности их последующего удаления злоумышленниками. Зафиксированные данные атак могут содержать не только техническую информацию, но и данные, способные идентифицировать личность нападающего, что может быть использовано в качестве доказательств в судебном разбирательстве.

Сетевая безопасность играет ключевую роль в защите от

киберпреступлений. Она обеспечивает комплексный подход к защите информационных систем и данных, что включает в себя использование современных технологий, обучение персонала и разработку эффективной политики безопасности. В условиях постоянно развивающихся угроз кибербезопасности, важно не только применять существующие методы защиты, но и постоянно разрабатывать новые подходы и решения для обеспечения безопасности в цифровом мире.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

[1]А. Аббаси, Дж. Ветцельс, В. Бокслэг, Э. Замбон и С. Эталле, «О системах обнаружения сетевых вторжений на основе эмуляции», в исследовании атак, вторжений и защит: 17-й международный симпозиум, RAID 2014, Гетеборг, Швеция, 17-19 сентября 2014 года. Материалы, А. Ставру, Х. Бос и Г. Портокалидис, ред. Cham: Springer International Publishing, 2014, стр. 384-404

[2]Т. Ф. Лант, «Автоматизированный анализ контрольного журнала и обнаружение вторжений: обзор», Материалы 11-й Национальной конференции по компьютерной безопасности, 1988, том 353: Балтимор, Мэриленд

[3]Колиас С., Камбуракис Г., Ставру А., Грицалис С. (2016) Обнаружение вторжений в сетях 802.11: эмпирическая оценка угроз и общедоступный набор данных. IEEE Communications Surveys & Tutorials 18(1):184-208

[5]Закон Республики Узбекистан, от 15.04.2022 г. № ЗРУ-764 «О кибербезопасности»//URL: https://lex.uz/ru/docs/5960609

[6]Gulomov Sherzod Rajaboevich, Mirzaeva Malika Bakhadirovna, Iminov Abdurasul Abdulatipovich. Port-Knocking Method for Enhancing Network Security. 2022 International Conference on Information Science and Communications Technologies (ICISCT) | 978-1-6654-7229-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICISCT55600.2022.10146918

I Siddikov, H Khujamatov, D Khasanov, [7]E Reypnazarov, A Iminov. Analyze Wireless Sensor Network Structures for Intellectual Monitoring Systemhttps://ieeexplore.ieee.org/abstract/document/10146824

[8]I Siddikov, H Khujamatov, D Khasanov, E Reypnazarov, A Iminov Data Transfer Methods and Algorithms in Wireless Sensor Networks for IoT-based Remote Monitoring System of Hybrid Energy Supply Sources. https://ieeexplore.ieee.org/abstract/document/10146865

[9]Iminov A.A. Implementation of International Legislation in the Field of Information and Cyber Security in the Republic of Uzbekistan. https://ijcm.academicjournal.io/index.php/ijcm/article/view/501

[10]А.А.Иминов и др. Основы информационной безопасности. Учебник. –Т. Академия МВД РУз.-2021г. С.128.

Иминов Абдурасул Абдулатипович,
начальник кафедры Информационных технологии Академия МВД
Эл.почта: iminovabdurasul1970@gmail.com

Исаков Аброр Фахриддинович, заместитель начальника кафедры Информационных технологии Академия МВД

Рахмонбердиев Бобирхон Баходир ўғли, слушатель факультета подготовки иностранных специалистов Московского университета МВД России имени В.Я. Кикотя рядовой МВД республики Узбекистан
Эл. почта: bob.raxmanberdiev@bk.ru

Iminov A.A., Isakov A.F., Rakhmonberdiev B.B.

The Role of Network Security in Combating Cybercrime

Abstract: In the modern digital world, cybercrime is receiving increasing attention due to its growing impact on individual and corporate security. This article is dedicated to analyzing the role of network security in preventing and combating cybercrime. The authors consider network security not merely as an aggregate of technical tools and protocols, but as a strategic element integrated into the overall risk management system, requiring a comprehensive approach that includes legal, technical, and educational aspects.

Keywords: Cybercrime, information security, anti-phishing, DDoS attacks, network security.

Иминов А.А., Исаков А. Ф., Рахмонбердиев Б. Б.

Тармоқ хавфсизлигининг кибержиноятларга қарши курашишдаги роли

Аннотация. Замонавий рақамли дунёда кибержиноятларга борган сари кўпроқ эътибор қаратилмоқда, чунки уларнинг шахсий ва корпоратив хавфсизликка таъсири ортиб бормоқда. Ушбу мақола тармоқ хавфсизлигининг кибержиноятларни олдини олиш ва уларга қарши курашишдаги ролини таҳлил қилишга бағишланган. Муаллифлар тармоқ хавфсизлигини фақатгина техник воситалар ва протоколлар мажмуи сифатида эмас, балки умумий хавфларни бошқариш тизимига интеграция қилинган стратегик элемент сифатида қарайдилар, бу эса ҳуқуқий, техник ва таълимий жиҳатларни ўз ичига олган комплекс ёндашувни талаб қилади.

Калит сўзлар. Кибержиноятлар, ахборот хавфсизлиги, фишингга қарши кураш, DDoS-ҳужумлар, тармоқ хавфсизлиги.

Иминов Абдурасул Абдулатипович
Тел.: +998 (99) 832-35-01