https://doi.org/10.53360/2788-7995-2024-3(15)-1

МРНТИ: 81.93.29

А.Р. Ерболулы*, К.Б. Тусупова
Казахский национальный университет имени аль-Фараби,
050040, Республика Казахстан, г. Алматы, пр. аль-Фараби, 71
*e-mail: roma43529@gmail.com

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ЗАВТРА: ВЫВОДЫ ИЗ АНАЛИЗА ВЕДУЩИХ КИБЕРАТАК И ИХ ВЛИЯНИЯ НА ЗАЩИТУ ИНФОРМАЦИИ

Аннотация: *В современном мире, где цифровизация и всеобщая связность играют ключевую роль, вопросы кибербезопасности выходят на передний план в контексте глобальной безопасности. С ростом зависимости от цифровых технологий, киберпространство продолжает эволюционировать, представляя всё новые угрозы и вызовы. Данная статья фокусируется на анализе крупных атак на сетевую инфраструктуру, произошедших в последние годы, исследуя разнообразные типы атак, такие как DDoS, APT, ransomware, Man-in-the-Middle (MitM) и SQL Injection. Основное внимание уделяется выявлению общих паттернов атак и методик защиты, что позволяет лучше понять механизмы и стратегии противодействия киберугрозам. Статья детально рассматривает различные инструменты и методы анализа трафика, применяемые для обнаружения и нейтрализации угроз, анализирует их эффективность в реальных условиях. С помощью включенных гистограмм, диаграмм и таблиц, статья визуализирует данные и тренды, что способствует лучшему пониманию сложности и динамики кибератак. На основе проведенного анализа формулируются рекомендации по улучшению стратегий киберзащиты и разработке новых подходов к обеспечению безопасности в цифровом мире, что является критически важным для защиты ценных информационных активов и поддержания устойчивости киберпространства.*

Ключевые слова: *Кибербезопасность, кибератаки, автоматизация обнаружения угроз, прогнозирование кибератак, защита от вредоносных программ.*

Введение

В последние годы мир стал свидетелем беспрецедентного роста киберугроз, которые оказывают значительное влияние на бизнес, правительства и жизнь обычных людей. Кибератаки становятся всё более изощрёнными и масштабными, что подчёркивает критическую необходимость защиты информационной инфраструктуры [1]. Среди наиболее значимых угроз выделяются DDoS-атаки [2], которые могут парализовать деятельность крупных онлайн-сервисов, APT (Advanced Persistent Threats) – продолжительные целенаправленные атаки [3], часто государственно поддерживаемые, а также атаки с использованием ransomware, которые блокируют доступ к важнейшим данным до выплаты выкупа [4]. Анализ таких инцидентов и методов их обнаружения и предотвращения становится неотъемлемой частью стратегии кибербезопасности. От понимания того, как были организованы атаки и какие инструменты использовались для защиты, зависит не только непосредственное реагирование на инциденты, но и планирование мер профилактики на будущее. В этой статье мы рассмотрим ряд крупнейших атак на сети, проанализируем использованные методы обеспечения сетевой безопасности и оценим эффективность существующих инструментов анализа трафика.

Материалы и методы.

В последние десять лет мир столкнулся с рядом масштабных кибератак, которые значительно повлияли на информационную безопасность государств, компаний и индивидуальных пользователей (рис. 1). С 2020 года мир кибербезопасности столкнулся с

рядом выдающихся атак, каждая из которых выделяется уникальными методами внедрения и разрушительным воздействием. Вот несколько примеров значимых кибератак, произошедших с 2020 года:

1. SolarWinds (2020): Эта кибератака, предположительно осуществленная российской хакерской группой, привлекла внимание мировой общественности из-за своего масштаба и сложности. Вредоносное ПО было внедрено в обновления программного обеспечения Orion Platform компании SolarWinds, что позволило злоумышленникам получить доступ к сетям тысяч организаций, включая федеральные агентства США и крупные корпорации [5].
2. Microsoft Exchange Server Hafnium (2021): В начале 2021 года были обнаружены четыре уязвимости в серверах Microsoft Exchange, которые активно эксплуатировались китайской хакерской группой Hafnium. Эти уязвимости позволили атакующим удаленно устанавливать вредоносное ПО и красть данные с серверов организаций по всему миру [6].
3. Colonial Pipeline (2021): В мае 2021 года группа киберпреступников DarkSide осуществила атаку ransomware на Colonial Pipeline, крупнейшую трубопроводную систему в США. Атака привела к временной остановке всех операций, серьезным перебоям в поставках топлива на Восточном побережье США и выплате выкупа в размере 4,4 миллиона долларов [7].
4. Kaseya VSA (2021): В июле 2021 года REvil, ещё одна известная группа, использующая ransomware, атаковала программное обеспечение для удаленного мониторинга и управления Kaseya VSA. Атака затронула сотни компаний по всему миру, включая множество малых предприятий, которые используют услуги управляемых поставщиков услуг [8].
5. Facebook Data Leak (2021): В апреле 2021 года данные 533 миллионов пользователей Facebook из 106 стран стали доступны онлайн. Утечка включала личную информацию, такую как номера телефонов, даты рождения, и местоположения. Хотя данные были получены в результате уязвимости, которая была устранена ещё в 2019 году, последствия утечки ощущаются до сих пор [9].

Эти случаи еще раз подчеркивают критическую важность регулярного обновления и укрепления систем киберзащиты, а также подтверждают необходимость всестороннего подхода к обеспечению безопасности цифровой инфраструктуры.

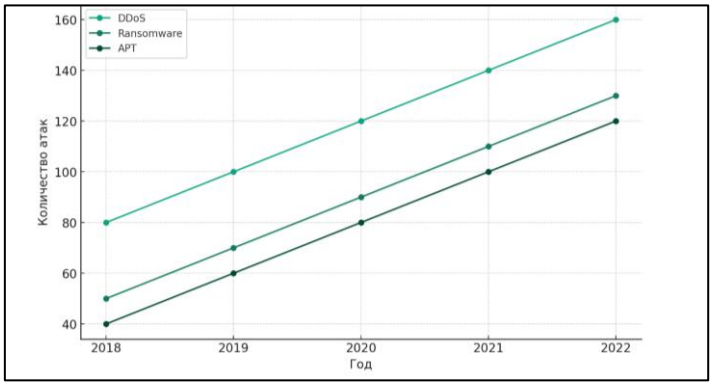

Рисунок 1 – Линейный график прирост атак с 2018 по 2022 годы

На рисунке 1 представленом линейном графике иллюстрируется временная динамика атак трёх типов – DDoS, Ransomware и APT – за период с 2018 по 2022 годы. Как видно, количество атак каждого типа растёт со временем, что подчеркивает увеличение активности и сложности киберугроз. Этот график помогает анализировать тенденции развития угроз и оценивать эффективность внедрённых мер безопасности со временем [10].

Кибератака представляет собой попытку несанкционированного проникновения, нарушения или использования компьютерных систем, инфраструктуры, сетей или личных данных [11]. С ростом числа подключенных устройств и объемов цифровых данных, кибератаки становятся всё более сложными и разнообразными, что увеличивает риски для как частных лиц, так и для организаций. Кибербезопасность, в свою очередь, включает в себя стратегии, технологии и процессы, разработанные для защиты сетей, устройств, программ и данных от атак или несанкционированного доступа. Эффективная кибербезопасность требует комплексного подхода, включающего физическую безопасность, программное обеспечение, а также обучение сотрудников основам безопасного поведения в сети.

Обеспечение кибербезопасности остаётся критически важным аспектом для всех организаций, учитывая разнообразие и постоянное развитие кибератак. Вот обзор основных типов кибератак, с которыми сталкиваются современные организации:

DDoS (Distributed Denial of Service) атаки продолжают оставаться одной из самых популярных и разрушительных форм кибератак . Эти атаки осуществляются путём захвата и использования огромного числа интернет-подключённых устройств для отправки колоссального количества трафика к целевым серверам, что приводит к их перегрузке и невозможности обрабатывать законные запросы (табл. 1) [12].

Таблица 1 – DDoS атаки и методы обнаружения и защиты

DDoS атаки	**Примеры крупных DDoS атак**				
	Атака на Dyn (2016): Эта масштабная DDoS атака использовала ботнет Mirai, состоящий из миллионов зараженных IoT устройств, для нападения на DNS провайдера Dyn. Это привело к значительным сбоям в работе крупнейших веб-сайтов, таких как Twitter, Spotify и Netflix [13].	Атака на GitHub (2018): GitHub столкнулся с самой масштабной DDoS атакой в своей истории, пиковый трафик которой достигал 1.35 Тбит/с. Атака была осуществлена с использованием метода усиления через Memcached сервера, что увеличило объем атакующего трафика [14].	Атака на Amazon Web Services (2020): В феврале 2020 года AWS отразила DDoS атаку с трафиком в 2.3 Тбит/с, что стало одной из самых мощных атак в истории. Атака была направлена на сверхувеличение трафика с помощью отражения и усиления через сторонние сервера [15].		
	Методы обнаружения и защиты				
	Мониторинг трафика	Сетевые снифферы и IDS	Митигация на основе границ сети	Облачные защитные услуги	Распределенная защита

Эти методы и инструменты являются ключевыми в современной стратегии защиты от DDoS атак, помогая организациям защищать свои сети и сервисы от возрастающей угрозы кибератак.

APT (Advanced Persistent Threat) обозначает продвинутые устойчивые угрозы, которые представляют собой целенаправленные атаки, часто спонсируемые государствами и направленные на длительное и скрытое проникновение в информационные системы высокозначимых целей, таких как правительственные учреждения, военные объекты и крупные корпорации. Эти атаки характеризуются высокой сложностью и тщательным планированием (табл. 2) [16].

Таблица 2 – Кейс-стади по крупным APT атакам

APT атаки	**Примеры крупных APT атак**		
	Stuxnet. Хотя это и более ранняя атака, Stuxnet является одной из наиболее известных APT из-за своей специфики и масштаба. Этот вирус был направлен против иранской ядерной программы и специально разработан для атаки на ПЛК Siemens, управляющие центрифугами для обогащения урана [17].	Атаки группы APT28/Fancy Bear. APT28, связываемая с российским правительством, использовала методы фишинга для получения доступа к сетям, что привело к значительным политическим последствиям и публичному разоблачению важных документов [18].	SolarWinds (2020): Эта кампания, как упоминалось, связана с российскими хакерскими группами и включала внедрение вредоносного кода в обновления программного обеспечения SolarWinds, что позволило атакующим необнаруженно проникнуть в сети тысяч организаций [5].
	Методы обнаружения и защиты		
	Сетевой мониторинг	Анализ поведения	Ответ на инциденты

Эффективное использование IDS и IPS в сочетании с комплексной стратегией безопасности помогает защитить организации от продвинутых угроз, таких как APT, обеспечивая глубокий уровень наблюдения и контроля за сетевой активностью.

Ransomware (вымогательское ПО) – это тип вредоносного программного обеспечения, которое блокирует доступ к системам или данным жертвы и требует выплаты выкупа за их восстановление. Эти атаки могут серьезно повлиять на операционную деятельность, финансовое состояние и репутацию организаций (табл. 3). В последние годы ransomware стал основной угрозой для крупных организаций во всем мире [4].

Таблица 3 – Примеры крупных Ransomware атак

Ransomware	**Примеры крупных Ransomware атак**				
	Colonial Pipeline (2021): Одна из самых крупныхтрубопроводных компаний США была вынуждена временно прекратить работу из-за атаки ransomware, что привело к серьезным перебоям в поставках топлива на Восточном побережье США. Компания выплатила выкуп в размере 4.4 миллиона долларов, чтобы восстановить доступ к своим системам [7].	JBS S.A. (2021): Крупнейший в мире производитель мяса, компания JBS S.A., стала жертвой атаки ransomware, которая привела к остановке производства в США и Австралии. Компания выплатила выкуп в размере 11 миллионов долларов для предотвращения утечки данных и восстановления операционной деятельности.	Kaseya VSA (2021): Через программное обеспечение для удаленного управления Kaseya VSA была проведена атака, затрагивающая сотни конечных пользователей, включая множество малых и средних предприятий. REvil, группа стоящая за атакой, потребовала $70 миллионов за дешифратор [8].		
	Методы обнаружения и защиты				
	Образование и обучение сотрудников	Резервное копирование данных	Использование передовых антивирусных решений и EDR	Патч-менеджмент	Инцидентный ответ и план восстановления

Применение этих методов позволяет не только обнаруживать и предотвращать атаки ransomware, но и эффективно реагировать на них, сокращая возможный ущерб и обеспечивая защиту критически важной информации.

Результаты и обсуждение

Методы анализа трафика и обеспечения безопасности сети включают широкий спектр технологий и практик, которые помогают организациям защитить свои сетевые активы от внешних и внутренних угроз (рис. 2) [19]. Они позволяют не только обнаруживать и реагировать на атаки, но и предотвращать их.

Рисунок 2 – Распределение различных методов анализа трафика и обеспечения безопасности

Сетевые снифферы (или анализаторы трафика) – это инструменты, предназначенные для перехвата и анализа сетевого трафика. Они позволяют администраторам сетей и специалистам по безопасности видеть, что происходит в сети в режиме реального времени или из архивированных данных [14]. Эти инструменты могут быть использованы для

мониторинга, диагностики сетевых проблем, анализа производительности сети, а также для обнаружения и расследования подозрительной или вредоносной активности.

Примеры использования сетевых снифферов:

- Обнаружение вторжений и аномалий: Снифферы могут обнаруживать необычные изменения в трафике, такие как резкие увеличения активности, необычные запросы или трафик, исходящий из неожиданных источников. Это может указывать на наличие вредоносных программ, атак на сеть или другие угрозы.
- Отладка сетевых проблем: Снифферы позволяют анализировать трафик и определять проблемы, такие как потери пакетов, задержки или проблемы с протоколами. Это помогает в устранении проблем с производительностью и доступностью сетевых ресурсов.
- Проверка политик безопасности: С помощью снифферов можно проверять, соответствует ли сетевой трафик установленным политикам безопасности. Например, можно проверить, не передаются ли через сеть незашифрованные пароли или другие чувствительные данные.
- Регуляторное соблюдение: В некоторых отраслях действуют строгие требования к мониторингу и архивации сетевого трафика. Снифферы могут помочь организациям соблюдать эти требования, предоставляя необходимые данные и отчеты.

Возможности сетевых снифферов:

- Глубокий анализ пакетов: Современные снифферы могут проводить глубокий анализ пакетов, изучая детали на уровне отдельных битов и байтов. Это позволяет точно определить содержание и происхождение трафика.
- Фильтрация и сортировка: Снифферы обычно предоставляют широкие возможности для фильтрации и сортировки трафика по различным параметрам, таким как IP-адреса, порты, протоколы и т.д. Это помогает быстро находить интересующую информацию в больших объемах данных.
- Интеграция с другими инструментами: Многие снифферы можно интегрировать с другими инструментами безопасности, такими как системы предотвращения вторжений (IPS), системы управления и анализа событий безопасности (SIEM) и инструменты автоматизации, что улучшает общую эффективность системы безопасности.
- Визуализация: Современные решения предоставляют возможности визуализации трафика, которые помогают визуально анализировать паттерны и тенденции, делая анализ более наглядным и понятным.

Сетевые снифферы являются мощным инструментом в арсенале специалиста по кибербезопасности, обеспечивая важные данные и аналитику для поддержания безопасности и стабильности сетевых сред [20].

IDS (Intrusion Detection System) и *IPS* (Intrusion Prevention System) являются ключевыми компонентами в инфраструктуре сетевой безопасности. IDS предназначены для обнаружения и предупреждения о потенциальных атаках, в то время как IPS не только обнаруживает угрозы, но и активно вмешивается, чтобы предотвратить выполнение вредоносных действий. Обе системы играют важную роль в защите сетей от широкого спектра угроз, от DDoS-атак до сложных APT.

Примеры реализации IDS/IPS:

- Cisco IPS 4200 Series: Эти устройства используются во многих крупных организациях для защиты корпоративных сетей. Cisco IPS обеспечивает предотвращение вторжений в реальном времени, используя глубокий анализ пакетов и сигнатурный подход к обнаружению угроз. Эффективность таких систем подтверждается их способностью быстро адаптироваться к новым угрозам с помощью регулярно обновляемых сигнатур.
- Snort: Это одна из наиболее популярных систем обнаружения вторжений с открытым исходным кодом. Snort можно настроить как IDS или IPS и использовать для анализа трафика в реальном времени и обнаружения подозрительной активности по сигнатурам и аномальным поведениям. Благодаря своей гибкости и широкой базе пользователей, Snort обладает большой базой данных сигнатур и широким сообществом, которое постоянно разрабатывает новые правила и обновления.
- Palo Alto Networks Next-Generation Firewalls: Эти современные брандмауэры включают в себя функционал IPS и предлагают интегрированную защиту от множества угроз. Они способны анализировать содержимое трафика, чтобы обнаруживать и предотвращать атаки

на приложения, эксплойты, вирусы и спайвэр. Palo Alto Firewalls также используют машинное обучение для повышения точности и эффективности в обнаружении угроз.

Эффективность систем IDS/IPS зависит от ряда факторов, включая:

- Актуальность сигнатур: Системы должны регулярно обновляться, чтобы отражать новейшие угрозы и эксплойты. Задержки в обновлениях могут оставить сеть уязвимой для недавно разработанных атак.
- Настройка и тонкая настройка: Эффективность IDS/IPS значительно увеличивается с правильной настройкой и тонкой настройкой правил, что позволяет минимизировать ложные срабатывания и упустить реальные угрозы.
- Интеграция с другими системами безопасности: IDS/IPS, интегрированные с другими системами безопасности, такими как SIEM и EDR, могут обеспечить более комплексную защиту, позволяя лучше анализировать и реагировать на угрозы.

В целом, IDS и IPS являются жизненно важными элементами в обеспечении защиты сетей, предоставляя слой безопасности, который помогает предотвращать, обнаруживать и реагировать на разнообразные угрозы в режиме реального времени [21].

Системы управления сетевой безопасности представляют собой комплексные платформы, включающие в себя различные инструменты и методы для обеспечения безопасности сетевых операций. Эти системы позволяют централизованно управлять безопасностью, обеспечивать соблюдение нормативных требований и защищать сеть от внутренних и внешних угроз. Они обычно включают функции обнаружения и предотвращения вторжений, управления уязвимостями, мониторинга трафика и реагирования на инциденты.

Обзор ключевых инструментов и методов в системах управления сетевой безопасности:

- Firewall Management: Управление брандмауэрами включает настройку и поддержку правил фильтрации трафика, которые контролируют входящие и исходящие соединения через сетевые точки доступа. Современные брандмауэры также могут выполнять глубокий анализ пакетов и распознавание приложений для более тонкой настройки правил безопасности.
- Intrusion Detection and Prevention Systems (IDS/IPS): Эти системы являются неотъемлемой частью сетевого мониторинга, обеспечивая обнаружение аномальных активностей и автоматическое прекращение вредоносных операций. IDS/IPS могут быть интегрированы с другими системами безопасности для усиления реакции на угрозы.
- Data Loss Prevention (DLP): Системы DLP предотвращают потерю или утечку конфиденциальной информации. Они контролируют данные, пересекающие границы сети, и могут блокировать передачу чувствительной информации на основе политик безопасности.
- Security Information and Event Management (SIEM): SIEM объединяет и анализирует логи и данные с различных источников безопасности в реальном времени для обнаружения аномалий, управления инцидентами и создания отчетов. SIEM позволяет видеть большую картину сетевой безопасности, облегчая принятие своевременных мер.

Эффективность систем управления сетевой безопасности.

Эффективность систем управления сетевой безопасности во многом зависит от их способности интегрироваться с существующей инфраструктурой, адаптивности к новым угрозам и легкости управления. Интеграция различных инструментов безопасности в единую систему позволяет более эффективно контролировать безопасность, быстро реагировать на инциденты и поддерживать высокий уровень защиты персональных данных и корпоративных ресурсов. Системы должны постоянно обновляться и модернизироваться для соответствия текущим угрозам и обеспечения соответствия нормативным требованиям [22].

Анализ распределения кибератак по странам показывает, что не только традиционно технологически развитые страны, такие как США, Китай и Германия, подвергаются атакам, но и страны с бурно развивающимися цифровыми инфраструктурами, такие как Казахстан, становятся мишенями для киберпреступников (рис. 4). В последние годы Казахстан испытал увеличение числа кибератак, что подчеркивает необходимость усиления мер безопасности на национальном уровне. Это распределение подсказывает, что киберугрозы являются глобальной проблемой, требующей координированных усилий международного сообщества для разработки эффективных стратегий защиты и реагирования.

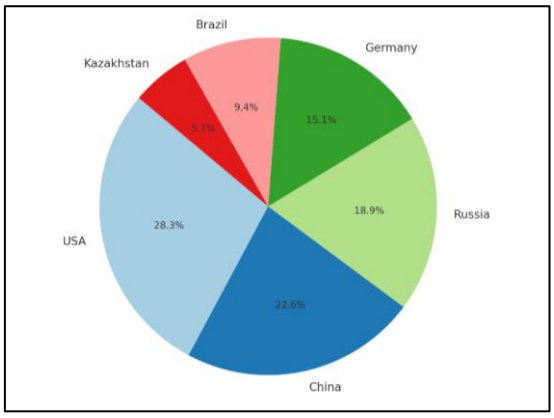

Рисунок 4 – Диаграмма распределение атак по странам

На представленной круговой диаграмме показано распределение кибератак по странам. США возглавляют список с наибольшим количеством инцидентов, за ними следуют Китай, Россия, Германия, Бразилия и Казахстан. Эта диаграмма помогает визуализировать, какие страны наиболее подвержены кибератакам, что может указывать на географические "горячие точки" кибератиности и потребность в укреплении мер безопасности в этих регионах. Это помогает лучше понимать географический спектр киберугроз и определять регионы, нуждающиеся в усиленной киберзащите [23].

Экономический ущерб от кибератак может быть значительным и оказывать длительное воздействие на пострадавшие организации и экономики в целом. Атаки типа ransomware, например, могут привести к потере критически важных данных и длительным перебоям в работе, что в свою очередь приводит к значительным финансовым потерям и ущербу для репутации компаний. Кроме прямых потерь, таких как выплата выкупов или восстановление систем, компании также сталкиваются с косвенными издержками, включая штрафы за нарушение нормативных требований, судебные иски и утрату доверия клиентов. В глобальном масштабе, затраты на борьбу с киберпреступностью и меры предосторожности продолжают расти, что подчеркивает критическую необходимость инвестиций в эффективные системы кибербезопасности для предотвращения и смягчения последствий таких атак.

На диаграмме (рис. 5) представлен экономический ущерб от атак типов DDoS, Ransomware и APT в различных секторах, таких как финансы, здравоохранение, технологии, производство и образование. Эти данные помогают оценить финансовые последствия кибератак и определить приоритеты в защите критически важных секторов экономики. Как видно, финансовый сектор и здравоохранение понесли наибольший ущерб от атак типа Ransomware, что подчеркивает необходимость особенно тщательной защиты этих сфер. В то время как атаки типа APT также значительно затрагивают технологический сектор, подчеркивая их целенаправленный и разрушительный характер [24].

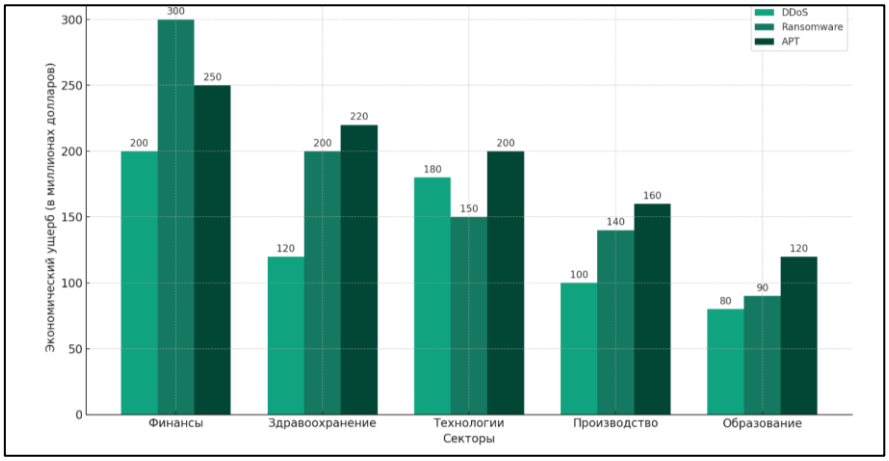

Рисунок 5 – Экономический ущерб от атак

Экономический ущерб от кибератак продолжает расти, поскольку всё больше бизнес-процессов переходит в цифровое пространство. Затраты на восстановление после атак включают не только непосредственное восстановление данных и систем, но и потери от простоев, когда ключевые бизнес-операции оказываются парализованными. Компании сталкиваются с дополнительными расходами на юридические услуги и консультации по управлению кризисными ситуациями, а также могут нести значительные издержки в связи с необходимостью уведомления клиентов о нарушениях безопасности и защиты их от возможного мошенничества. Долгосрочные последствия включают ущерб для бренда и потерю доверия со стороны клиентов, что может серьезно снизить рыночную стоимость компании. По этим причинам предприятиям крайне важно инвестировать в профилактические меры и стратегии быстрого реагирования на инциденты кибербезопасности.

Исходя из визуализированных данных и представленных графиков о крупнейших кибератаках, можно сделать несколько ключевых выводов относительно текущих трендов в сфере кибербезопасности и общей динамики угроз. Эти выводы помогают понять, какие аспекты требуют особого внимания со стороны организаций и государственных структур.

1. Увеличение числа и сложности кибератак: Линейный график временной динамики атак показывает постоянный рост количества атак типов DDoS, Ransomware и APT. Это свидетельствует о том, что киберпреступники становятся более изощренными и их методы более разнообразными.
2. Распределение уязвимостей по секторам: Тепловая карта уязвимостей выявила наиболее часто эксплуатируемые уязвимости в различных секторах. Например, финансовый сектор особенно уязвим для атак типа Credential Stuffing и SQL Injection, что подчеркивает необходимость усиления защиты данных в этой отрасли.
3. Секторальные финансовые потери: Столбчатая диаграмма потерь показала, что финансовый ущерб от кибератак наиболее значителен в секторах финансов и здравоохранения. Это указывает на высокую стоимость восстановления и потерь данных для этих секторов, а также потенциальное воздействие на общественное благосостояние.
4. Географические «горячие точки»: Диаграмма распределения атак по странам показывает, что некоторые страны, включая США и Китай, испытывают значительно большее число атак. Это может быть связано с большей цифровизацией их экономик и более высоким уровнем технологического развития.

Заключение

Анализ данных о крупнейших кибератаках последних лет явно демонстрирует рост и эволюцию угроз в киберпространстве. В свете этих выводов, рекомендуется, чтобы организации и государственные институты уделили повышенное внимание разработке и реализации комплексных стратегий кибербезопасности. Это включает в себя усиление защиты критически важных инфраструктур, особенно в финансовом и здравоохранительном секторах, где последствия атак оказывают наибольшее влияние.

Следует акцентировать внимание на обучении персонала методам распознавания и предотвращения киберугроз, поскольку человеческий фактор остается одним из слабых звеньев в цепи кибербезопасности. Также важно улучшать международное сотрудничество в обмене информацией о киберугрозах и методах их нейтрализации, что поможет оперативно реагировать на новые угрозы и минимизировать их последствия.

Разработка и внедрение продвинутых технологических решений, таких как искусственный интеллект и машинное обучение для обнаружения и блокирования атак, также должны стать приоритетом. Эти технологии могут значительно повысить эффективность систем обнаружения и предотвращения вторжений, предоставляя более глубокий анализ и быстрое реагирование на инциденты кибербезопасности.

Список литературы

1. Entanglement: cybercrime connections of a public forum population / Masarah Paquet-Clouston et al // Journal of Cybersecurity. – 2022. – Vol. 8, Issue 1. https://doi.org/10.1093/cybsec/tyac010.
2. Ali T.E. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review / T.E. Ali, Y.-W. Chong, S. Manickam // Appl. Sci. – 2023. – № 13(5). – P. 3183. https://doi.org/10.3390/app13053183.

3. Quintero-Bonilla S. A New Proposal on the Advanced Persistent Threat: A Survey // S. Quintero-Bonilla, A. Martín del Rey // Appl. Sci. – 2020. – № 10(11). – P. 3874. https://doi.org/10.3390/app10113874.
4. Alraizza A. Ransomware Detection Using Machine Learning: A Survey / A. Alraizza, A. Algarni // Big Data Cogn. Comput. – 2023. – № 7(3). – P. 143. https://doi.org/10.3390/bdcc7030143.
5. Coco A. Illegal: The SolarWinds Hack under International Law / A. Coco, T. Dias // European Journal of International Law. – 2022. – Vol. 33, Issue 4. – P. 1275-1286. https://doi.org/10.1093/ejil/chac063.
6. O'Neill P.H. How China's attack on Microsoft escalated into a «reckless» hacking spree. .Security experts warn Hafnium attacks are «highly reckless» and «dangerous» / P.H. O'Neill // MIT Technology Review. – 2021. https://www.technologyreview.com/2021/03/10/1020596/how-chinas-attack-on-microsoft-escalated-into-a-reckless-hacking-spree/.
7. Parfomak P.W. Colonial Pipeline: The DarkSide Strikes. Colonial Pipeline: The DarkSide Strikes (congress.gov) / P.W. Parfomak, C. Jaikaran // Congressional Research Service. – 2021. https://crsreports.congress.gov/product/pdf/IN/IN11667.
8. Brash R.Colonial Pipeline Attack: Lessons Learned for Ransomware Protection / R. Brash // Verve Industrial. – 2021. https://verveindustrial.medium.com/colonial-pipeline-attack-lessons-learned-for-ransomware-protection-156bdd6961fa.
9. Jee Ch. What you need to know about the Facebook data leak. Everything you need to know about the Facebook data leak / Ch. Jee // MIT Technology Review. – 2021. https://www.technologyreview.com/2021/04/07/1021892/facebook-data-leak/.
10. Next-generation cyber attack prediction for IoT systems: leveraging multi-class SVM and optimized CHAID decision tree / U.K. Lilhore et al // Journal of Cloud Computing. – 2023. – Vol. 12. – P. 137. https://doi.org/10.1186/s13677-023-00517-4.
11. Almansoori A. Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. / A. Almansoori, M. Al-Emran, Kh. Shaalan // Appl. Sci. – 2023. – № 13(9). – P. 5700. https://doi.org/10.3390/app13095700.
12. Adedeji K.B. DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges / K.B. Adedeji, A.M. Abu-Mahfouz, A.M. Kurien // J. Sens. Actuator Netw. – 2023. – № 12(4). – P. 51. https://doi.org/10.3390/jsan12040051.
13. Wang C. The 2016 Dyn Attack and its Lessons for IoT Security. The 2016 Dyn Attack and its Lessons for IoT Security / C. Wang // MS&E 238 Blog (stanford.edu). – 2018. https://mse238blog.stanford.edu/2018/07/clairemw/the-2016-dyn-attack-and-its-lessons-for-iot-security/.
14. Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning / Francisco Sales de Lima Filho et al // Hindawi Security and Communication Networks. – 2019. https://doi.org/10.1155/2019/1574749.
15. Porter J. Amazon says it mitigated the largest DDoS attack ever recorded. Amazon says it mitigated the largest DDoS attack ever recorded / J. Porter // The Verge. – 2020. https://www.theverge.com/2020/6/18/21295337/amazon-aws-biggest-ddos-attack-ever-2-3-tbps-shield-github-netscout-arbor.
16. Zou Q. An Approach for Detection of Advanced Persistent Threat Attacks / Q/ Zou et al // Computer. – 2020. – Vol. 53, Issue 12. https://doi.org/10.1109/MC.2020.3021548.
17. Kushner D. The Real Story Of Stuxnet.The Real Story of Stuxnet / D. Kushner // IEEE Spectrum. – 2013. https://spectrum.ieee.org/the-real-story-of-stuxnet.
18. Tennessee A. Everything you need to know about the apt, fancy bear. TIR-20220718 Everything You Need to Know About the APT / A. Tennessee // Fancy Bear (avertium.com). – 2022. https://otx.alienvault.com/pulse/63c500b4b4bc0829561a50cb.
19. An autoML network traffic analyzer for cyber threat detection / A. Papanikolaou et al // Regular Contribution. – 2023. – Vol. 22. – P. 1511-1530. https://doi.org/10.1007/s10207-023-00703-0.
20. Anomaly Detection in Activities of Daily Living with Linear Drift / Ó. Belmonte-Fernández et al // Cogn Comput. – 2020. – № 12. – P. 1233-1251. https://doi.org/10.1007/s12559-020-09740-6.
21. Survey of intrusion detection systems: techniques, datasets and challenges / A. Khraisat et al // Cybersecurity. – 2019. – Vol. 2, № 20. https://doi.org/10.1186/s42400-019-0038-7.

22. Taherdoost H. Understanding Cybersecurity Frameworks and Information Security Standards – A Review and Comprehensive Overview / Hamed Taherdoost. (2022). // Electronics. – 2022. – № 11(14). – P. 2181. https://doi.org/10.3390/electronics11142181.
23. Bocharova M. How Digitalisation Became a Cyber Security Threat in Kazakhstan / M. Bocharova // A PROJECT OF THE INSTITUTE FOR WAR & PEACE REPORTING. – 2022. https://cabar.asia/en/how-digitalisation-became-a-cyber-security-threat-in-kazakhstan.
24. Anomaly Detection in Activities of Daily Living with Linear Drift / Ó. Belmonte-Fernández et al // Cogn Comput. 2020. – Vol. 12. – P. 1233-1251. https://doi.org/10.1007/s12559-020-09740-6.

Ә.Р. Ерболұлы*, К.Б. Түсіпова
әл-Фараби атындағы Қазақ Ұлттық университеті,
050040, Қазақстан Республикасы, Алматы қ, аль-Фараби даңғылы, 71
*e-mail: roma43529@gmail.com

ЕРТЕҢГІ КҮНДІ ҚАУІПСІЗ ЕТУ: ЖЕТЕКШІ КИБЕРШАБУЫЛДАРДЫ ТАЛДАУДАН АЛЫНҒАН НӘТИЖЕЛЕР ЖӘНЕ ОЛАРДЫҢ АҚПАРАТТЫ ҚОРҒАУҒА ӘСЕРІ

Цифрландыру мен жалпыға ортақ байланыс шешуші рөл атқаратын қазіргі әлемде киберқауіпсіздік мәселелері жаһандық қауіпсіздік контекстінде алдыңғы қатарға шығады. Цифрлық тәуелділіктің артуымен киберкеңістік дамып, жаңа қауіптер мен қиындықтарды ұсынады. Бұл мақала DDoS, APT, ransomware, man-in-the-middle (MitM) және SQL Injection сияқты шабуылдардың әртүрлі түрлерін зерттей отырып, соңғы жылдары болған ірі желілік инфрақұрылымдық шабуылдарды талдауға бағытталған. Киберқауіптерге қарсы тұрудың механизмдері мен стратегияларын жақсы түсінуге мүмкіндік беретін шабуылдардың жалпы үлгілері мен қорғаныс әдістерін анықтауға баса назар аударылады. Мақалада қауіптерді анықтау және бейтараптандыру үшін қолданылатын трафикті талдаудың әртүрлі құралдары мен әдістері егжей-тегжейлі қарастырылады, олардың нақты әлемдегі тиімділігін талдайды. Қосылған гистограммалар, диаграммалар мен кестелер арқылы мақала кибершабуылдардың күрделілігі мен динамикасын жақсырақ түсінуге ықпал ететін деректер мен трендерді визуализациялайды. Жүргізілген талдау негізінде киберқауіпсіздік стратегияларын жақсарту және цифрлық әлемде қауіпсіздікті қамтамасыз етудің жаңа тәсілдерін әзірлеу бойынша ұсыныстар тұжырымдалады, бұл құнды ақпараттық активтерді қорғау және киберкеңістіктің тұрақтылығын сақтау үшін маңызды болып табылады.

Түйін сөздер: *Киберқауіпсіздік, кибершабуылдар, қауіпті анықтауды автоматтандыру, кибершабуылдарды болжау.*

A.R. Yerbolulу*, T.K. Tusipova
Al-Farabi Kazakh National University, Republic of Kazakhstan, Almaty
050040, Republic of Kazakhstan, Almaty, 71 Al-Farabi Avenue
*e-mail: roma43529@gmail.com

ENSURING A SAFE TOMORROW: CONCLUSIONS FROM THE ANALYSIS OF THE LEADING CYBER ATTACKS AND THEIR IMPACT ON INFORMATION SECURITY

In today's world, where digitalization and universal connectivity play a key role, cybersecurity issues are coming to the fore in the context of global security. With increasing dependence on digital technologies, cyberspace continues to evolve, presenting new threats and challenges. This article focuses on the analysis of major attacks on network infrastructure that have occurred in recent years, exploring various types of attacks such as DDoS, APT, ransomware, Man-in-the-Middle (MitM) and SQL Injection. The main focus is on identifying common attack patterns and protection techniques, which allows for a better understanding of the mechanisms and strategies for countering cyber threats. The article examines in detail the various tools and methods of traffic analysis used to detect and neutralize threats, analyzes their effectiveness in real conditions. Using the included histograms, charts and tables, the article visualizes data and trends, which contributes to a better understanding of the complexity and dynamics of cyber attacks. Based on the analysis, recommendations are formulated to improve cyber defense strategies and develop new approaches to ensuring security in the digital world, which is critically important for protecting valuable information assets and maintaining the stability of cyberspace.

Key words: *Cybersecurity, cyber attacks, threat detection automation, cyber attack forecasting*

Сведения об авторах

Алишер Рахматулла Ерболулы – магистрант 2 курса по специальности «Система Информационной Безопасности»; Казахский национальный университет имени аль-Фараби, Республика Казахстан; e-mail: roma43529@gmail.com.

Камшат Бакытжановна Тусупова – ДокторPhD кафедры «Информационные системы»; старший преподаватель; Казахский национальный университет имени аль-Фараби, Республика Казахстан.

Авторлар туралы мәліметтер

Әлішер Рахматулла Ерболұлы – «Ақпараттық қауіпсіздік жүйелері» мамандығының 2 курс магистранты; әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан Республикасы; e-mail: roma43529@gmail.com.

Камшат Бақытжановна Түсіпова – «Ақпараттық жүйелер» кафедрасының PhD доктары; аға оқытушы; әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан Республикасы.

Authorlar turaly malimetter

Alisher Rakhmatulla Erboluly – «Information security systems» profession 2nd year master's students; Al-Farabi Kazakh National University, Republic of Kazakhstan; e-mail: roma43529@gmail.com

2Kamshat Bakytzhanovna Tusipova– «Information system» of the Department of PhD Doctors; Senior Lecturer; Al-Farabi Kazakh National University, Republic of Kazakhstan.

Поступила в редакцию 30.04.2024
Поступила после доработки 07.09.2024
Принята к публикации 09.09.2024

https://doi.org/10.53360/2788-7995-2024-3(15)-2

МРНТИ: 50.41.01

Э.Н. Бопанова[1*], И.Б. Карымсакова[1], Ю.В. Крак[2]
[1]Университет имени Шакарима города Семей,
071412, Республика Казахстан, г. Семей, ул. Глинки, 20 А
[2]Киевский национальный университет имени Шевченко,
01033, Украина, г. Киев, ул. Володимирська, 60
* email: emiliya2000@mail.ru

АНАЛИЗ И СИСТЕМАТИЗАЦИЯ МЕТОДОВ РАЗРАБОТКИ ПРОГРАММНЫХ ИНТЕРФЕЙСОВ

Аннотация: *Целью данного исследования является анализ и систематизация методов разработки программных интерфейсов (ПИ), а также определение оптимальных подходов и технологий для создания интуитивно понятных и удобных ПИ. В современном мире программные интерфейсы играют ключевую роль в обеспечении взаимодействия пользователя с программными продуктами, поэтому важность их качественного проектирования сложно переоценить. В рамках работы рассматриваются различные методики проектирования ПИ, включая классические и современные подходы, такие как пользовательско-ориентированный дизайн (UCD), прототипирование, тестирование на удобство использования и адаптивный дизайн. Также изучаются принципы взаимодействия с пользователем, включая когнитивные аспекты и модели восприятия информации, что позволяет создать более эффективные и удобные в использовании интерфейсы.*

Особое внимание уделяется современным технологиям и инструментам, таким как фреймворки и библиотеки для разработки интерфейсов, методы автоматизации и использования искусственного интеллекта в процессе проектирования ПИ. Исследование включает анализ успешных примеров реализации ПИ в различных отраслях, а также обзор новейших тенденций в области интерфейсного дизайна. Результаты исследования направлены на формирование рекомендаций по выбору оптимальных методов и технологий разработки ПИ в зависимости от специфики проекта и требований конечных пользователей.

Основные выводы исследования могут быть полезны разработчикам программного обеспечения, специалистам по пользовательскому опыту и дизайнерам интерфейсов для повышения качества взаимодействия пользователей с программными продуктами. Работа также может служить основой для дальнейших исследований в области разработки и оптимизации пользовательских интерфейсов, способствуя развитию данной области знаний и практики.