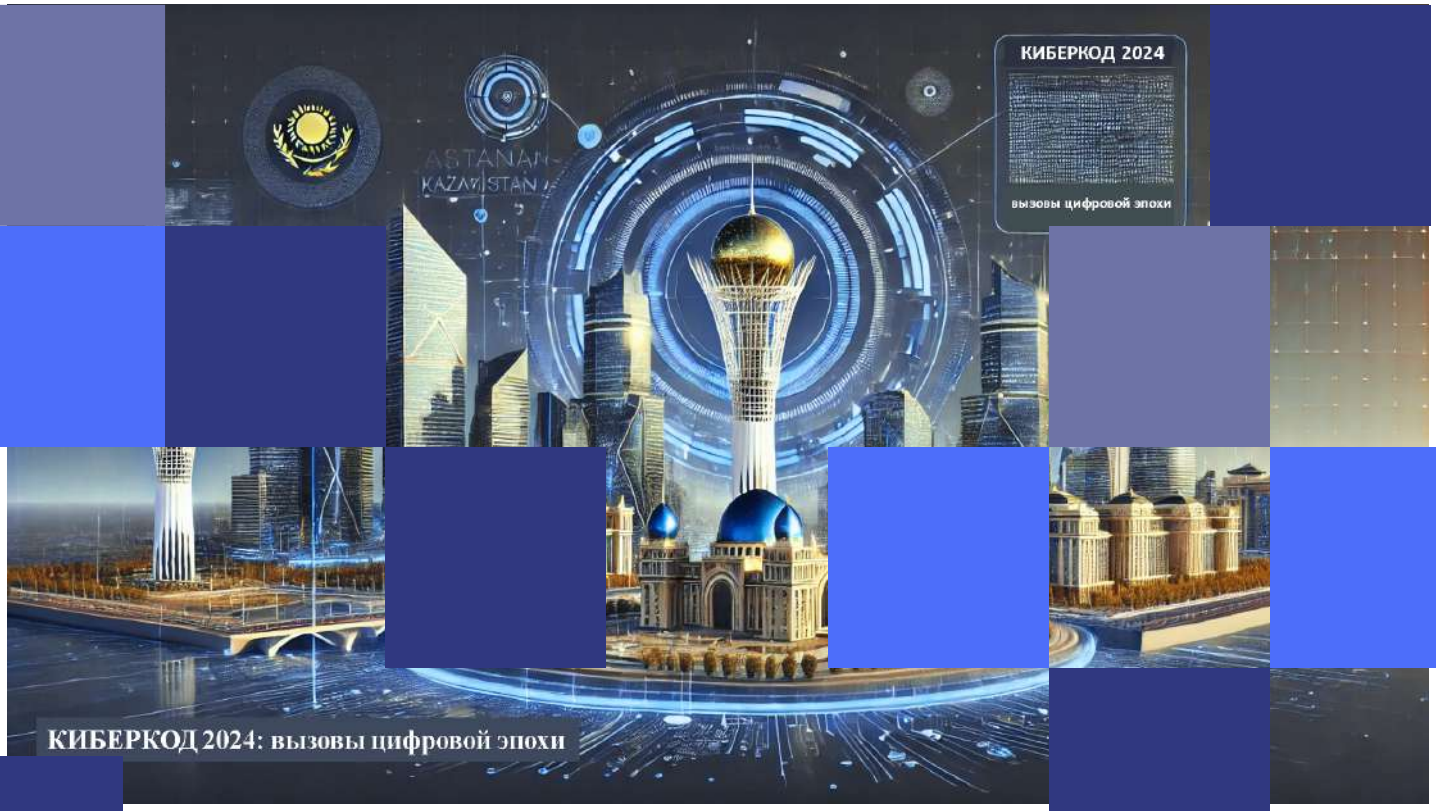
АО «Государственная техническая служба»

КИБЕРКОД 2024:
вызовы цифровой эпохи

Кибербезопасность — это стратегическая необходимость, определяющая устойчивость и успех организаций в цифровом мире.

Вместе мы сможем сделать шаг навстречу более защищённому будущему.



Кибердайджест:

Содержание

В 2024 году кибербезопасность остаётся критически важной сферой, которая влияет на стабильность бизнеса, государственных структур и общества в целом

Введение: глобальный контекст и ключевые тренды

Мир продолжает стремительно переходить в цифровой формат, делая технологии неотъемлемой частью нашей жизни. Вместе с этим растут и угрозы информационной безопасности, где атаки становятся всё более сложными, а последствия всё более масштабными. В 2024 году кибербезопасность остаётся критически важной сферой, которая влияет на стабильность бизнеса, государственных структур и общества в целом.

Для обеспечения кибербезопасности требуется значительное финансирование, поскольку современные цифровые технологии требуют надежной защиты от кибератак и угроз. Инвестиции необходимы для создания мощных систем мониторинга и предотвращения угроз, обеспечения безопасности государственных информационных систем, защиты данных и разработки инновационных решений. Финансовые ресурсы также важны для подготовки высококвалифицированных специалистов, проведения регулярных технических тренировок, а также для поддержки международного сотрудничества в области кибербезопасности. Без должного уровня финансирования невозможно обеспечить надежную защиту национальной инфраструктуры и цифровой экономики.

Так, согласно новому прогнозу компании Gartner, продолжающееся усиление угроз, развитие облачных технологий и нехватка кадров в 2025 году заставит руководителей служб информационной безопасности повысить расходы конечных пользователей на информационную безопасность на 15%.

Искусственный интеллект, интернет вещей, автоматизированные системы управления и облачные технологии открывают новые возможности, но одновременно создают уникальные риски. Киберпреступники используют эти технологии для утечек данных, манипуляций и взломов, оставляя перед организациями и правительствами сложные задачи по защите.

Особую актуальность приобретает человеческий фактор: недостаточная осведомлённость сотрудников об информационной безопасности часто становится слабым звеном.

Программы по кибергигиене, обучение и повышение культуры информационной безопасности – залог устойчивости перед угрозами

2024

В этом дайджесте мы собрали ключевые события,тенденции и уроки в области информационной безопасности за прошедший год.

Мы расскажем о значимых инцидентах, обсудим изменения в законодательстве РК, новые технические решения и лучшие практики противодействия угрозам информационной безопасности.

КИБЕРКОД 2024:

вызовы цифровой эпохи

- Зачимые инциденты
- Изменения в законодательстве РК
- Новые технические решения
- Лучшие практики противодействия угрозам ИБ

Кибербезопасность больше не просто техническая дисциплина.

Это стратегическая необходимость, определяющая устойчивость и успех организаций в цифровом мире.

Вместе мы сможем сделать шаг навстречу более защищённому будущему

2. **Крупные инциденты в Казахстане:** обзор внутренних угроз и ответных мер

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ: ФАЙЛЫ С ЛИЧНОЙ ИНФОРМАЦИЕЙ НА КАЗАХСТАНСКИХ ИНТЕРНЕТ-РЕСУРСАХ

В 2024 году выявлялись файлы, содержащие персональные данные на казахстанских интернет-ресурсах, которые могли быть использованы для фишинга и социальной инженерии, включая взлом социальных сетей. Утечки данных, такие как фишинг, кибершпионаж и использование информации в преступных целях, имеют долгосрочные последствия.

Подводя итоги о крупных инцидентах в Казахстане в 2024 году, можно отметить, что киберпреступность в стране достигла нового уровня. Регистрация множества утечек данных и кибератак на государственные и частные учреждения, включая инциденты с фишингом и кибершпионажем, стала тревожным сигналом.

АО «ГТС» зафиксировано более 41 тысячи инцидентов в области информационной безопасности, в том числе с вирусами, сетевыми червями и троянами

Обострение угроз связано с применением IoT и ИИ в кибератаках, что требует постоянного совершенствования защиты и улучшения осведомленности пользователей по вопросам кибергигиены.

Ключевыми инцидентами стали две крупные утечки данных:

- В феврале 2024 года на площадке GitHub был опубликован слив данных китайской компании, где содержались персональные данные казахстанцев.
- В марте 2024 года была выявлена утечка данных микрофинансовой организации zaimer.kz, затронувшая данные более двух миллионов казахстанцев.

Также было расследовано несколько инцидентов, имевших резонанс:

- В одной из организаций Казахстана были обнаружены вредоносные программы, связанные с кампаниями кибершпионажа, спонсируемыми другими государствами. Вредоносные файлы использовались для компрометации учетных записей сотрудников и установления удаленного доступа.
- В марте 2024 года была зафиксирована массовая фишинговая рассылка с целью заражения сотрудников государственных органов RAT-программой SugarGh0st, которая позволяла злоумышленникам управлять файлами, собирать данные, а также записывать использование клавиш и делать снимки экрана.
- На одном из квазигосударственных объектов Казахстана было зафиксировано заражение вирусом-шифровальщиком, в результате которого злоумышленники потребовали выплату в биткойнах. Проблемы возникли из-за отсутствия антивирусной защиты, многократного нарушения законодательства РК в сфере ИБ и несанкционированного доступа к интернет-ресурсам.

- В мае 2024 года АО «ГТС» была исследована атака на подведомственную организацию государственного органа РК, где были выявлены многочисленные нарушения ИБ, включая отсутствие защиты, устаревшее оборудование и отсутствие своевременного патч-менеджмента. Также были зафиксированы следы злоумышленников, использующих инструмент Mimikatz для кражи учетных данных.

МАСШТАБ ИСПОЛЬЗОВАНИЯ ПРОТОКОЛА SSL ВЕРСИИ 2.0 ОПЕРАТОРОМ СВЯЗИ И РИСКИ ДЛЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В эпоху цифровизации безопасность телекоммуникационных сетей играет критическую роль для национальной безопасности. Информационные потоки между государственными структурами, коммерческими организациями и гражданами являются основой функционирования общества и экономики. Любые уязвимости в этих сетях могут привести к серьезным последствиям, включая утечку конфиденциальной информации, сбои в критической инфраструктуре и угрозы суверенитету государства.

Протоколы шифрования SSL/TLS являются важнейшими инструментами для обеспечения безопасности передачи данных в интернете. Они позволяют установить защищенные соединения между клиентами и серверами, обеспечивая конфиденциальность и целостность данных. Однако с течением времени некоторые версии этих протоколов устаревают и становятся уязвимыми для современных методов кибератак.

SSLv2 *(Secure Sockets Layer version 2)*, выпущенный в 1995 году, признан небезопасным из-за известных уязвимостей, таких как отсутствие поддержки современных алгоритмов шифрования и подверженность атакам типа «Man-in-the-Middle». Это делает его использование крайне ненадежным в условиях современной угрозы.

В 2023 году исследование показало, что Казахстан имеет наибольшее количество веб-серверов, поддерживающих устаревший протокол SSL версии 2.0. Этот протокол, официально признанный устаревшим в 2011 году, всё ещё используется на более чем 460 000 устройствах по всему миру, значительная часть которых расположена в Казахстане.

Анализ выявил, что большинство уязвимых устройств в Казахстане принадлежит одному из операторов связи в стране, который использует устройства, произведенные китайской компанией и работающие с устаревшим веб-сервером GoAhead. Для анализа использования протокола SSLv2 в инфраструктуре телекоммуникационных операторов страны использовались данные поисковой системы shodan.io.

Основной оператор, на устройствах которого были обнаружены уязвимости, является крупнейший телекоммуникационный оператор в Казахстане, который обслуживает значительную часть интернет-инфраструктуры. Другие операторы имеют значительно меньшую долю.

Были обнаружены уязвимости SSL/TLS, включая DROWN CVE-2016-0800 и другие уязвимости, такие как CCS *(CVE-2014-0224),* CRIME *(CVE-2012-4929),* POODLE *(CVE-2014-3566),* SWEET32 *(CVE-2016-2183)*, FREAK *(CVE-2015-0204)* и другие.

Эти уязвимости связаны с использованием слабых шифров и отсутствием поддержки современных протоколов TLS 1.2 и 1.3, а также отсутствием Forward Secrecy. Также была обнаружена проблема с использованием самоподписанного сертификата с несовпадающим доменным именем и устаревшим алгоритмом подписи MD5, что снижает уровень безопасности.

ИНЦИДЕНТ В ОДНОЙ ИЗ КОМПАНИЙ: КОМПРОМЕТАЦИЯ СЕТИ И УТРАТА ДАННЫХ

В январе 2024 года в одной компании столкнулись с серьёзным инцидентом информационной безопасности, продемонстрировавшим уязвимость организации перед внутренними угрозами и недостаточность соблюдения стандартов безопасности.

Ход атаки: в начале января 2024 года злоумышленник с одного IP-адреса получил доступ к рабочей станции через доменную учётную запись системного администратора. Критической уязвимостью стал единый пароль для доступа ко всем устройствам сети, что позволило злоумышленнику:

- авторизоваться на всех рабочих станциях;
- провести шифрование данных;
- удалить лог-файлы, затруднив анализ инцидента.

Атака развивалась стремительно. . В ночь января произошло повторное проникновение, в результате которого все данные были зашифрованы.

Ключевые ошибки:

- Не были выполнены рекомендации по отключению хоста WIN от сети, что привело к утрате ценных данных для анализа;
- Использование одного пароля для всех устройств сети значительно облегчило работу злоумышленника.

Реакция и последствия: сотрудники НКЦИБ провели выездную проверку и анализ скомпрометированных хостов с предоставлением рекомендаций по устранению. Однако к моменту реагирования часть данных была уже утрачена. Были утрачены лог-файлы с критически важного хоста, что серьёзно затруднило полное восстановление картины инцидента. Для выявления возможного внутреннего участия в инциденте Службе безопасности компании было предложено провести служебное расследование в отношении системного администратора, чья учётная запись использовалась для атаки.

Этот случай подчёркивает важность строгого соблюдения рекомендаций по реагированию на инциденты информационной безопасности, а также необходимости:

- использования уникальных паролей для каждой системы;
- ограничения прав доступа по принципу минимальной достаточности;
- оперативного отключения скомпрометированных устройств от сети.

Инцидент в данной компании стал наглядным примером, как внутренние ошибки и несоблюдение базовых правил безопасности могут существенно усугубить последствия кибератаки.

Этот кейс подчёркивает важность внедрения комплексных мер по защите и укреплению информационной безопасности в организациях.

DDOS-АТАКА НА КАЗАХСТАНСКИЙ ИНТЕРНЕТ-РЕСУРС: ЭВОЛЮЦИЯ УГРОЗ И АДАПТИВНАЯ ЗАЩИТА

В январе 2024 года Казахстанский интернет-ресурс стал жертвой серии высокоинтенсивных DDoS-атак, которые показали, насколько быстро злоумышленники могут адаптироваться к установленным защитным мерам. Изначально атаки происходили на уровнях L3 *(сетевой)* и L4 *(транспортный)* и были нацелены на перегрузку серверных ресурсов за счёт огромного числа запросов, что делает сайт недоступным. Интернет-ресурс был защищён с помощью AntiDDoS от АО «ГТС», успешно блокировавшего угрозы этих уровней.

Далее злоумышленники перешли к атакам на уровне L7 *(уровень приложений)* - более сложному типу DDoS, который затрудняет работу самого веб-приложения. В январе 2024 года атака на L7 началась в 14:51 и за час вывела интернет-ресурс из строя, направив более 120 тысяч запросов с более чем 6 тысяч IP-адресов, из которых около 2000 принадлежали Казахстану.

После анализа логов и выявления характера атаки системному администратору были даны рекомендации подключить защиту Cloudflare и установить CAPTCHA для противодействия автоматизированным запросам. Этот инцидент стал примером того, как киберпреступники используют разноуровневые подходы для достижения своих целей. Он также подчёркивает важность адаптивных мер защиты, таких как комбинирование AntiDDoS решений и инструментов фильтрации на уровне приложений.

Для противостояния современным угрозам информационной безопасности организациям необходимо использовать многослойный подход к защите, оперативно реагируя на эволюцию атакующих стратегий.

В ФЕВРАЛЕ 2024 ГОДА В МЕССЕНДЖЕРЕ БЫЛО ОПУБЛИКОВАНО ОБЪЯВЛЕНИЕ О ПРОДАЖЕ ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ МИНИСТЕРСТВА «РЕГИСТР ПРИКРЕПЛЕННОГО НАСЕЛЕНИЯ»

В феврале 2024 года в мессенджере был опубликован анонс о продаже доступа к информационной системе одного из министерств. Доступ к системе имеет только персонал, и для входа используется двухфакторная аутентификация, логин и пароль, а также электронная цифровая подпись *(ЭЦП)*. Было установлено, что неизвестное лицо предлагает данный доступ, предоставляя учетные данные, такие как логин, пароль и ЭЦП работников. Инцидент был передан в правоохранительные органы для дальнейшего расследования.

КОМПРОМЕТАЦИЯ УЧЕТНЫХ ЗАПИСЕЙ WHATSAPP: АНАЛИЗ И ДЕАНОНИМИЗАЦИЯ

В середине февраля 2024 года АО «ГТС» была обнаружена массовая вредоносная рассылка по мессенджеру WhatsApp гражданам Республики Казахстан, содержащая в себе ссылку на страницу с голосованием, с одного IP-адреса.

Мошенники отправляли пользователям сообщение с вредоносной ссылкой на страницу с голосованием, после чего перенаправляли на форму ввода номера телефона. Как только пользователь вводил номер телефона, мошенники в автоматическом режиме запрашивали код подтверждения для авторизации на официальном ресурсе https://web.whatsapp.com. Пользователи на своем мобильном устройстве получали уведомление о подтверждении привязки устройства, после нажатия пользователями кнопки «**Confirm**», мошенники получали доступ к аккаунту Whatsapp.

В ходе анализа была выявлена страница «**SCAM**», которая состояла из панели управления и API-сервиса. Фаззинг API-сервиса выявил директорию **/docs** с описанием методов сервиса. В одном из методов была выявлена критическая уязвимость типа **RCE**, позволяющая внедрять произвольный Python-код **(Python Code Injection)**, уязвимости был подвержен метод **/api/download_logs/**. Эксплуатация этой уязвимости позволила получить привилегированный доступ root на сервере. Анализ исходного кода и базы данных выявил список администраторов и данные о скомпрометированных учетных записях. В общей сложности содержалось 18 480 записей, из которых 15 897 уникальных номеров принадлежали гражданам Казахстана. Был выявлен IP-адрес сервера мошенника, а также 16 доменов, которые использовались для фишинговых атак.

Ответные действия:

- Используя полученные в ходе анализа исходного кода API-сервиса идентификаторы пользователей мессенджера Telegram, удалось установить личности некоторых владельцев или разработчиков панели «SCAM».

Выводы и рекомендации:

- Заблокировать IP-адрес сервера мошенника и все связанные домены, использовавшиеся для фишинговых атак.
- Ограничивать и следить за сессиями на других связанных устройствах.

Фишинговые атаки по-прежнему остаются актуальной и опасной угрозой, поскольку злоумышленники совершенствуют методы, делая поддельные сообщения и веб-сайты все более правдоподобными.

Поэтому необходимо обратить внимание на повышение осведомленности граждан в информационной безопасности для предотвращения компрометации учетных записей.

КИБЕРАТАКА НА КАЗАХСТАНСКОГО ТЕЛЕКОММУНИКАЦИОННОГО ОПЕРАТОРА КАЗАХСТАНА: СЛЕДЫ APT-ГРУППИРОВОК В ИНФРАСТРУКТУРЕ

С марта 2024 года инфраструктура одного из телекоммуникационных операторов Казахстана оказалась под угрозой, связанной с деятельностью APT-группировок. С 10 по 16 марта сотрудники АО «ГТС» провели выездное расследование. Основной целью было определение степени проникновения и идентификация APT-группировок, действующих в инфраструктуре телекоммуникационного оператора.

Анализ логов антивирусного ПО «Лаборатории Касперского» и межсетевых экранов Check Point выявил:

- Многочисленные факты компрометации хостов;
- Обращения на заражённые C2-серверы, что указывает на управление инфраструктурой извне;
- Наличие backdoor, оставленных злоумышленниками для обеспечения постоянного доступа.

Основные выводы:

- Установлено, что APT-группировка имела полный контроль над инфраструктурой телекоммуникационного оператора, включая доступ к критически важным системам.
- Компрометация телекоммуникационной инфраструктуры влияет на безопасность связи, данные пользователей и доступность услуг.

Для минимизации ущерба и нейтрализации угрозы предложены следующие шаги:

- Проведение тотальной проверки всех хостов и сетевых устройств на наличие вредоносных компонентов.
- Устранение обнаруженных backdoor и изменение ключей доступа.
- Усиление мониторинга трафика с использованием средств анализа поведения и раннего обнаружения атак.

Инцидент подчеркнул важность создания многоуровневой системы защиты телекоммуникационной инфраструктуры.

Особое внимание должно быть уделено:

- Обучению персонала выявлению и реагированию на подозрительные действия.
- Внедрению современных решений для предотвращения сложных атак, таких как поведенческий анализ и системы реагирования на инциденты *(SOAR)*.
- Организации регулярных аудитов безопасности.

Данный инцидент стал одним из самых тревожных за год, подчеркивая угрозы национального масштаба, связанные с APT-группировками. Он требует от государства и бизнеса пересмотра подходов к защите критически важной инфраструктуры, чтобы предотвратить подобные сценарии в будущем.

УТЕЧКА ДАННЫХ ZAIMER.KZ: КОМПРОМЕТАЦИЯ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ДВУХ МИЛЛИОНОВ ГРАЖДАН РК

В марте 2024 года произошла одна из крупнейших утечек персональных данных в Казахстане. В открытом доступе в мессенджере Telegram появились дампы баз данных микрофинансовой организации ТОО МФО «Робокэш.кз» *(Zaimer.kz)*. Данная утечка произошла на платформе Robo.finance.

В целом обнаружено более 36 млн. данных клиентов микрофинансовых организаций *(РФ – 23,6 млн. (zaimer.ru – 16.8 млн., adengi.ru – 6.8 млн.)*; Филиппины – 5 млн. *(digido.ph);* Вьетнам – 2 млн. *(vietloan.vn))*. Эти данные содержали конфиденциальную информацию почти двух миллионов казахстанцев, включая персональные сведения. 5 марта злоумышленники опубликовали массивы, затронувшие данные 1 947 022 граждан РК. Информация включала личные данные клиентов Zaimer.kz, что делает инцидент критически значимым в условиях возрастающих рисков финансового мошенничества.

После выявления утечки АО «Национальные информационные технологии» были направлены PUSH-уведомления через мобильное приложение eGov Mobile и SMS через единый контакт-центр «1414». Уведомления получили 1 945 271 человек, что позволило минимизировать возможный ущерб. Однако 1 695 граждан РК, отсутствующих в базе мобильных граждан, остались без уведомлений.

Уроки инцидента:

- Данный случай подчёркивает необходимость строгого соблюдения стандартов информационной безопасности, особенно в финансовом секторе, где утечка данных может привести к значительным репутационным и материальным потерям.
- Быстрая реакция государственных структур позволила предупредить граждан о возможных рисках, однако инцидент показал важность полного охвата при заполнении гражданских баз.
- Утечка данных повышает вероятность целевых атак, таких как фишинг, социальная инженерия или финансовое мошенничество, что требует усиления информированности пользователей о базовых мерах кибергигиены.

Инцидент с Zaimer.kz стал тревожным сигналом для бизнеса и государства. Он подчеркнул необходимость внедрения многоуровневых систем защиты, а также повышения ответственности организаций за сохранность персональных данных. Для граждан этот инцидент - напоминание о важности цифровой безопасности и внимательного отношения к своим данным в онлайн-пространстве.

НА ФОРУМЕ «BREACHFORUMS» ВЫЯВЛЕН ПОСТ О ПРОДАЖЕ БАЗЫ ДАННЫХ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ КЛИЕНТОВ РОССИЙСКОЙ МЕДИЦИНСКОЙ ЛАБОРАТОРИИ «ГЕМОТЕСТ»

АО «ГТС» на форуме **«Breachforums»** выявлен пост от 1 мая 2022 года, опубликованный пользователем под псевдонимом «300rur», о продаже БД с персональными данными клиентов российской медицинской лаборатории «Гемотест». Утечка содержала 30 493 068 строк. В указанном списке также содержалась конфиденциальная информация граждан РК, которые пользовались услугами медицинской лаборатории, состоящая из 5272 строк. Также на форуме **«Breachforums»** пользователем под псевдонимом «jtr» была опубликована БД, которая содержала 554 млн. заказов клиентов медицинской лаборатории «Гемотест». Утечка включала ФИО, год рождения, дату оформления и состав заказа.

ОБНАРУЖЕНА НЕКОРРЕКТНАЯ РАБОТА БИОМЕТРИИ КАЗАХСТАНСКОГО МОБИЛЬНОГО ПРИЛОЖЕНИЯ

В мае 2024 года поступило обращение о проведении несанкционированных транзакций с аккаунта клиента. В ходе расследования было установлено, что при смене доверенного номера сессия по проверке биометрии была открытой. В этой связи смена номера происходит без аутентификации биометрии, что создает предпосылки для неправомерного завладения доступом в аккаунт. Данный инцидент не относится к кибербезопасности.

Ответные действия:

В оперативном порядке разработчиками мобильного приложения была отключена возможность проверки биометрии.

SMB С ПУБЛИЧНО ДОСТУПНЫМИ ФАЙЛАМИ, СОДЕРЖАЩИМИ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ

В мае 2024 года Службой KZ-CERT в ходе исследования сетевых протоколов SMB *(port 445)* для удаленного доступа к файлам и сетевым ресурсам в казахстанском сегменте Интернета был обнаружен IP-адрес, принадлежащий компании, занимающейся содействием социально-экономическому развитию города с публично доступными файлами, содержащими конфиденциальные данные с правами на запись.

В ходе анализа выявлено, что на данном IP-адресе используется уязвимая версия Samba 4.6.2, подверженная критическим уязвимостям. Эти уязвимости позволяют удаленно выполнять код и получать доступ к серверу, что несет за собой различные возможные риски и угрозы информационной безопасности.

Анализ содержимого сетевого хранилища показал, что в нем хранятся файлы и папки, содержащие чувствительные данные, включая конфигурации систем, учетные данные для доступа, схемы и чертежи спутниковых связей и различные конфиденциальные данные. Наличие незащищенных SSH-ключей и конфиденциальных паролей в файлах устройства может позволить злоумышленникам потенциально проникнуть в систему управления, выполнять вредоносные действия и в дальнейшем закрепиться в системе.

В сетевом хранилище содержались файлы, папки, связанные с автоматизированной системой коммерческого учёта электроэнергии, управления энергетики и водоснабжения одного из городов страны, сертификаты и другие ПО.

КОМПРОМЕТАЦИЯ ИНФРАСТРУКТУРЫ МИНИСТЕРСТВА: УТЕЧКА УЧЕТНЫХ ДАННЫХ ЧЕРЕЗ АТАКУ НА ДОМЕН КОНТРОЛЛЕР В ИЮНЕ

12 июня 2024 года на одном из ключевых хостов министерства была зафиксирована активность злоумышленников, указывающая на сложную кибератаку. Ключевые аспекты инцидента:

Техника атаки:

- Использование утилиты vssadmin.exe для создания теневых копий диска;
- Доступ к базе данных SAM *(Security Account Manager),* что дало злоумышленникам возможность извлечь учетные данные;
- Компрометация учетных записей, включая административные, с домена контроллера.

Последствия:

- Потенциальный полный контроль над сетевой инфраструктурой;
- Возможный доступ к конфиденциальной переписке, чувствительным данным;
- Угроза утечек, способных повлиять на репутацию и безопасность государства;
- Компрометация учетных данных на уровне домена контроллера - одна из самых серьезных угроз для любой организации.

Это позволяет злоумышленникам:

- Получить доступ к критически важным данным;
- Устанавливать дополнительные вредоносные утилиты и обеспечивать долгосрочное присутствие в инфраструктуре;
- Подменять или уничтожать данные, нанося ущерб репутации организации.
- После обнаружения инцидента были реализованы следующие шаги:
- Немедленное отключение скомпрометированного хоста от сети;
- Проведение анализа и очистки учетных записей домена, включая смену паролей;
- Мониторинг активности через SIEM-системы для выявления и блокировки дополнительных угроз.

Данный инцидент подчеркивает необходимость внедрения следующих мер:

- Многофакторная аутентификация (MFA);
- Ограничение масштабов атаки за счет изоляции ключевых узлов *(сегментация сети);*

- Создание правил, блокирующих подозрительные действия с системными утилитами, такими как vssadmin.exe;
- Превентивная проверка *(регулярные аудиты безопасности)* конфигурации домен контроллеров и учетных данных.

Этот инцидент стал тревожным сигналом для всех государственных органов. В условиях усиления кибершпионажа и целевых атак на критически важные учреждения, Казахстану необходимы инвестиции в укрепление информационной безопасности, обучение персонала, модернизация инфраструктуры и внедрение передовых систем защиты.

ИНЦИДЕНТ В НЕФТЯНОЙ КОМПАНИИ: КОМПРОМЕТАЦИЯ ЧЕРЕЗ УЯЗВИМОСТЬ WDIGEST

В июле 2024 года инфраструктура одной нефтяной компании оказалась под угрозой из-за зафиксированного изменения параметров WDigest на нескольких хостах. Это изменение позволяет операционной системе хранить пароли в памяти в открытом виде, что открывает злоумышленникам доступ к критически важным ресурсам компании.

Опасности и последствия инцидента:

- Хранение учетных данных в незашифрованном виде позволяет злоумышленникам легко извлекать их для последующих атак.
- Возможности для перемещения по сети, эскалации привилегий и компрометации дополнительных систем.
- Атака на такие ключевые объекты, как на данную нефтяную компанию, может привести к значительным экономическим и энергетическим рискам.

Вредоносная активность обнаружена с IP-адреса, классифицированного как источник malware *(по данным VirusTotal)*. На скомпрометированном хосте выявлены порты 443, 500, 80 и 1337, что указывает на возможность эксплуатации для удаленного доступа или командно-контрольной связи.

Ответные действия:

- Эксперты ОЦИБ провели детальный анализ артефактов для определения масштаба ущерба.
- Скомпрометированные хосты изолированы для предотвращения дальнейшего распространения угрозы.
- Внесены изменения в параметры WDigest и повышение уровня безопасности учетных данных.

Случай с данной нефтяной компанией демонстрирует необходимость строгого контроля за параметрами конфигурации систем, особенно в организациях критической инфраструктуры.

Рекомендации:

- Отключать устаревшие функции, такие как WDigest, если они не используются.

- Использовать мониторинг на уровне хостов и сети для быстрого выявления подозрительных изменений.
- Регулярно проверять журналы событий для выявления активности, связанной с вредоносным ПО.

Своевременное реагирование на подозрительные события, как в данном случае, является ключевым для минимизации ущерба и защиты критически важных данных.

УТЕЧКА ДАННЫХ СТУДЕНТОВ И АБИТУРИЕНТОВ УНИВЕРСИТЕТА

В июле 2024 года в мессенджере Telegram была опубликована база данных студентов и абитуриентов одного из Казахстанских ВУЗов. Данные были опубликованы пользователем с электронной почты. Также имелась ссылка на канал, где продавались другие базы данных Казахстана, включая данные компаний.

ОБНАРУЖЕНО ВНУТРЕННЕЕ СКАНИРОВАНИЕ СЕТИ В КАЗАХСТАНСКОЙ КОМПАНИИ

5 августа 2024 г. из ОЦИБ поступила информация об атаке на подведомственную организацию одной из крупных компаний. Было зафиксировано внутреннее сканирование портов, злоумышленники использовали веб-шеллы для удаленного управления скомпрометированной системой. Были найдены утилиты для внутреннего сканирования сети и зафиксирована активность по сканированию сети. В журнале веб-сервера nginx были выявлены попытки загрузки веб-шелла с помощью функции **eval()**, что указывает на попытку выполнения произвольного кода на сервере.

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Службой KZ-CERT была получена информация о публикации в августе 2024 года на одном Telegram-канале поста с базой данных системы которая, по информации администратора канала, актуальна на апрель 2024 года. База данных содержала личную и идентификационную информацию на детей от 2019 до 2024 года рождения, зарегистрированных в системе. Кроме персональных данных на детей, являющихся гражданами РК, имеются записи на детей, имеющих гражданство России, Украины, Узбекистана и других государств СНГ.

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ МОБИЛЬНОГО ОПЕРАТОРА

Летом 2024 года на Telegram-канале была размещена база данных с информацией о **1115 клиентах мобильного оператора из Казахстана.** Были скомпрометированы такие данные, как ФИО, ИИН, дата рождения, адрес проживания и телефонные номера.

УЯЗВИМОСТЬ В ПЛАТФОРМЕ ZIMBRA: ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ

В сентябре 2024 года в ходе разведки на основе открытых данных была выявлена угроза в **платформе Zimbra** - популярной системе для корпоративной электронной почты и совместной работы. Через поисковую систему **shodan.io** было обнаружено **105 платформ Zimbra**, из которых **7 являются клиентами ЕШДИ**. Эти системы оказались подвержены критической уязвимости **CVE-2024-45519.**

Zimbra - это комплексная платформа, которая включает серверы почты, LDAP для аутентификации и MTA для маршрутизации сообщений, что делает её привлекательной целью для атак. Уязвимость **CVE-2024-45519** может быть использована для компрометации серверов и получения несанкционированного доступа к корпоративным данным.

Было опубликовано предупреждение для пользователей Zimbra немедленно обновить системы для устранения уязвимости. В ходе анализа было проведено извлечение данных через **shodan.io,** что позволило своевременно выявить подверженные системы в Казахстане.

Рекомендации и выводы:

- Оперативное обновление платформы Zimbra для защиты от уязвимости.
- Применение инструментов, таких как Shodan, для своевременного обнаружения подверженных систем, что помогает предупредить возможные атаки.
- Активно взаимодействовать с организациями, использующими Zimbra, для своевременного информирования и минимизации рисков.

Данный инцидент подчеркивает значимость проактивной безопасности и использования открытых данных для быстрого реагирования на потенциальные угрозы.

ИНЦИДЕНТ С ВРЕДОНОСНОЙ РАССЫЛКОЙ

В сентябре 2024 года зафиксирована вредоносная рассылка с одного электронного адреса, что свидетельствовало о компрометации учетных данных другого почтового сервера.

Первоначальное подключение к SMTP-серверу исходило с IP-адреса *(адресное пространство Нигерии)* с использованием протокола ESMTP. Получив доступ к учетным данным, атакующий использовал их для отправки вредоносных писем через сервер, принадлежащий Аппарату акима области.

Активность исходила с сервера, что подтверждает использование легитимной инфраструктуры для вредоносных действий.

ИНЦИДЕНТ В МИНИСТЕРСТВЕ: ЦЕЛЕНАПРАВЛЕННАЯ БРУТФОРС-АТАКА

В сентябре 2024 года была получена информация об атаке на серверный центр государственных органов *(СЦГО)*.

В ходе анализа логов были выявлены попытки несанкционированного входа через **SSH** с использованием перебора учетных данных для пользователей **root, postgres и admin.** Множественные неудачные попытки авторизации фиксировались через модуль **pam_unix**, что подтвердило факт целенаправленной атаки. Обнаружена аномальная активность из сети одного из министерств, предположительно из-за зараженного локального хоста за маршрутизатором.

Ответные действия:

- В министерство направлены рекомендации по выявлению зараженного устройства и устранению уязвимостей.
- Предложены действия по локализации зараженного хоста и усилению защиты сетевой инфраструктуры СЦГО.
-

Выводы и рекомендации:

- Настроить ограничения на доступ к SSH через белый список IP-адресов, а также внедрить двухфакторную аутентификацию.
- Провести мониторинг сетевого трафика для выявления подозрительной активности, особенно на уровне маршрутизаторов и локальных хостов.
- Убедиться в актуальности модулей аутентификации и системы мониторинга.
- Провести сканирование всей локальной сети для обнаружения и изоляции скомпрометированных устройств.

Брутфорс-атаки остаются актуальной угрозой для государственных учреждений, особенно при отсутствии жестких ограничений на доступ к критическим системам.

Своевременная идентификация источника угрозы и локализация заражения помогают минимизировать риски для всей инфраструктуры.

ОБНАРУЖЕНО ОБЪЯВЛЕНИЕ О ПРОДАЖЕ ДОСТУПА К КМИС НА НЕОФИЦИАЛЬНОЙ ПЛАТФОРМЕ НЕУСТАНОВЛЕННЫМИ ЛИЦАМИ

Посредством мессенджера Telegram неустановленное лицо за финансовое вознаграждение предлагало доступ к медицинской информационной системе. Данный инцидент передан в правоохранительные органы для дальнейшего совместного расследования.

ОБНАРУЖЕНА ВРЕДОНОСНАЯ АКТИВНОСТЬ В ОДНОМ ИЗ БАНКОВ

На архивных серверах одной финансовой организации посредством антивирусного ПО Касперский был обнаружен вредоносный процесс, связанный с ВПО Cobalt Strike. НКЦИБ запрошены данные дампа ОЗУ и образы для исследования.

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ 1WIN

В ноябре 2024 года в открытом доступе появилась база данных, содержащая личную информацию пользователей **1Win**, платформы для ставок и азартных игр. В базе присутствуют **e-mail корпоративной почты клиентов**, связанных с gov.kz, что представляет особую угрозу для безопасности государственных органов.

ИНЦИДЕНТ В МИНИСТЕРСТВЕ: АТАКА БОТНЕТА PHORPIEX И УЯЗВИМОСТЬ ИНФРАСТРУКТУРЫ

Осенью 2024 года аналитики Службы KZ-CERT зафиксировали всплеск активности ботнета Phorpiex с использованием Power BI. Дополнительно с помощью EDR-системы было выявлено вредоносное ПО, которое использовало следующие пути для автозапуска и постоянного присутствия:

- %windir%\winrecsv.exe
- %userprofile%\winrecsv.exe.

Ботнет активно распространялся на другие устройства в сети через съемные носители и сетевые папки, демонстрируя низкий уровень защиты инфраструктуры. Вредоносные файлы с расширением .exe *(например, ОТВЕТ14.10.exe)*, размещались на рабочих столах пользователей, чтобы скрыть их вредоносный характер. Поддельные файлы могли быть использованы для фишинговых атак.

В ходе выезда мобильной группы в министерство было установлено, что в ведомстве отсутствует сотрудник, отвечающий за информационную безопасность, а также истечение договора с ОЦИБ, а именно завершение срока действия договора оставило критически важные системы без надлежащей защиты.

Выводы и рекомендации:

- Установить и регулярно обновлять решения для обнаружения и предотвращения вредоносной активности, такие как современные EDR и IDS/IPS-системы.
- Ограничить доступ к внешним устройствам и настроить мониторинг активности в сетевых папках.
- Незамедлительно выделить специалиста для управления ИБ, включая обновление договоров с профильными организациями.
- Проводить регулярные тренинги по кибергигиене, особенно в отношении распознавания поддельных документов и социальной инженерии.

Инцидент демонстрирует, как недостаточное внимание к организационным и техническим аспектам безопасности может привести к значительным рискам для критически важных систем.

Эффективное управление, актуальные меры защиты и обучение сотрудников - ключевые элементы устойчивой защиты от кибератак.

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ БАНКА

В ноябре 2024 года на Telegram-канале была опубликована база данных, предположительно принадлежащая Казахстанскому банку, где содержались персональные данные граждан РК, включая ИИН, ФИО и номера телефонов.

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ: ШПИОНСКОЕ ПО ОТ КИТАЙСКОЙ КОМПАНИИ

В утечке данных обсуждается шпионское ПО, разработанное китайской компанией, которое использовалось для кибершпионажа в отношении сотовых операторов Казахстана. Из устройства собиралась информация, включая журналы вызовов, данные GPS и медиафайлы.

КОМПРОМЕТАЦИЯ УПРАВЛЕНИЯ LED ЭКРАНА, СВЯЗАННАЯ С ПОДМЕНОЙ ФЛАГА

В ноябре 2024 года поступила информация о возможном инциденте ИБ, связанном с подменой флага. Была сформирована мобильная группа для оперативного выезда на место инцидента. В рамках данного инцидента информация была передана в уполномоченные органы для проведения дальнейшего расследования.

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ В «СИРЕНА-ТРЕВЕЛ»

Национальной Службой KZ-CERT из открытых источников в декабре 2024 года получена информация об утечке данных российской компании «Сирена-Тревел». Утечка затрагивает и персональные данные казахстанских граждан, которые пользовались услугами этой компании.

Полный объем утечки включает два крупных набора данных:

- «TICK_PHONE_sample» — содержит всего 3 413 726 207 записей, включающих номера телефонов, электронные почты, связанные с бронированием авиабилетов. В базе данных содержатся данные с 18 января 2007 года по 10 сентября 2023 года.

- «TICK_INFO» — содержит всего 664 651 063 записи, включающие информацию о рейсах (номера рейсов, маршруты), авиакомпаниях, тарифах, стоимости билетов, а также персональные данные пассажиров. В базе данных содержатся данные с 24 февраля 2007 года по 9 сентября 2023 года.

В утекшей базе в файле «TICK_INFO_sample» находились данные авиакомпаний Казахстана. В базе данных отсутствовало поле, указывающее на точное гражданство пассажира. В этой связи по сортировке столбца CODE_CUR, определяющего валюту страны «KZT» и «K3T», обнаружено 10 039 строк данных, потенциально принадлежащих гражданам Казахстана.

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ

В декабре 2024 года в Telegram-канале и на платформе «X» распространялось сообщение следующего содержания: «Десятки тысяч документов, презентаций и других внутренних материалов Министерства с прикрепленными ссылками на интернет-ресурсы».

Согласно текущим данным файлы, содержащие информацию, появились в открытом доступе, могли быть загружены и просмотрены любым пользователем.

Выявленная утечка затрагивает значительный объём данных. Предполагается, что слитые файлы были намеренно ограничены. Не исключено, что злоумышленники располагают дополнительными данными, которые не были включены в публикацию. Есть возможность, что часть данных была удалена с целью исключения критической информации, связанной с проникновением в инфраструктуру.

Однако среди оставшихся данных присутствует конфиденциальная информация, которая включает пароли к внутренним сервисам, сканы паспортов (*535 экземпляров, проверка на уникальность не проводилась),* документы с персональными данными сотрудников министерства, его подведомственных организаций и гостей *(ФИО), рабочие и мобильные телефоны, ИИН, должности, почтовые адреса),* проекты документов *(планы, карты, схемы, справки и т. д.)*, служебную переписку и другую внутреннюю документацию.

Необходимо обратить внимание, что среди них присутствуют e-mail корпоративной почты клиентов, относящиеся к единой платформе интернет-ресурсов государственных органов *(gov.kz),* IBAN реквизиты граждан, городские и мобильные номера телефонов, сканы паспортов, удостоверений личности.

ИНЦИДЕНТ С ВРЕДОНОСНЫМ ПО TOFSEE: РАССЛЕДОВАНИЕ В МУЗЕЕ

Была зафиксирована вредоносная активность на рабочей станции с IP-адресом. Анализ показал, что система заражена ботнетом **Tofsee** - модульным вредоносным ПО, которое используется для рассылки спама, но также способно выполнять и другие вредоносные задачи, включая загрузку дополнительных модулей.

Основной принцип работы Tofsee – это создание собственной копии в папке: %USER%\<rnd>.exe, регистрация автозапуска в реестре: Software\Microsoft\Windows\CurrentVersion\Run MSConfig=%USER%\<rnd>.exe, инъекция в процесс **svchost.exe** и установка соединения с сервером C2, откуда загружаются модули для дальнейших действий. Для коммуникации с ботмастером используется уникальный 128-байтовый ключ шифрования, что делает расшифровку данных без ключа невозможной.

После обнаружения вредоносной активности было **направлено уведомление** ответственному за информационную безопасность музея с рекомендациями по устранению угрозы: создание системного образа и локализация заражённого устройства. Ответственный сотрудник провёл сканирование системы с помощью **Dr.Web**, что привело к прекращению активности. Однако, вместо более глубокого анализа были предприняты минимальные действия.

Ключевые выводы и риски - несмотря на прекращение активности, отсутствие системного анализа и форензики оставляет вероятность скрытого присутствия угрозы. Технический персонал ограничился базовыми мерами, игнорируя риски, связанные с модульной природой Tofsee. Заражение могло привести к дальнейшему распространению вредоносного ПО и утечке данных.

Рекомендации:

- После выявления вредоносного ПО важно создавать образы систем для последующей форензики, а не ограничиваться антивирусной проверкой.
- Использовать IDS/IPS и мониторинг активности в реестре для предотвращения автозапуска вредоносных программ.

Инцидент с Tofsee подчёркивает важность комплексного подхода к реагированию на угрозы информационной безопасности.

Ограничение мер только сканированием может привести к более глубоким последствиям в будущем.

КОМПРОМЕТАЦИЯ УЧЕТНЫХ ЗАПИСЕЙ TELEGRAM

На данный момент известны следующие методы получения доступа к учетной записи пользователей Telegram:

1. Социальная инженерия

Найти в интернете номер телефона, к которому привязан ваш Telegram *(если не выключена функция определения по номеру телефона)*, не сложно. Злоумышленнику остается проявить фантазию и заполучить код доступа в Telegram, который поможет ему войти в аккаунт.

Способ взлома через голосовую почту основан на получении кода входа в Telegram с целевого телефона с использованием различных инструментов. Хакеры использовали это, чтобы получить доступ к должностным лицам Южной Америки и скомпрометировать конфиденциальную информацию, содержащую коррупционные скандалы.

Способ «запроса скриншота» также основан на получении кода входа в систему, отправленного на целевое устройство. Вместо использования сложного программного обеспечения для отправки бесшумных SMS-сообщений с целью сбоя системы на достаточное время, чтобы Telegram отправил код входа на голосовую почту, злоумышленник просто просит скриншот.

Простой метод социальной инженерии для кражи аккаунта: достаточно просто создать ***клон учетной записи с одной отличной буквой***, снабдить ее украденным контентом и фотографиями. После этого мошенникам будет гораздо легче обманывать аудиторию канала и список контактов своей жертвы, просить перейти по фишинговым ссылкам или отправлять деньги.

2. Целевая атака, использование шпионского ПО

Созданы специальные программы для взлома. В даркнете можно найти приложения для взлома Telegram, которые может купить любой пользователь. Такие программы распространяются через фишинговые ссылки или под видом документов (с расширением doc, exe, pdf, xlsx, pptx), картинок, видео, аудио (голосовых) и пересылаемых файлов или использования шпионских программ.

3. Нелегальные приложения, клоны Telegram

Неофициальные приложения - это поддельные версии Telegram, разработанные третьими лицами. Использование поддельных клонов приложений для установки вредоносного ПО — это старая стратегия взлома, до сих пор применяемая киберпреступниками по всему миру. Эти приложения-клоны известны как вредоносные.

4. Заражения устройств (сотовый телефон, персональный компьютер, ноутбук)

Большинство заражений устройств начинается с установки вредоносного ПО, скрытого внутри безобидного приложения. Это поддельное приложение может затем отслеживать все входящие файлы в Telegram. Как пример, большинство приложений, скачанные с Torrent, могут иметь установленные программы для слежки, такие как кейлоггер.

5. Перехват кода подтверждения через оператора связи

Также возможен перехват через устройство SS7, которое используется в непосредственной близости, в таком случае СМС даже не поступит на телефон.

Широко практиковались в текущем году

- Фишинговые ссылки с предложением подарочной подписки: мошенники рассылают сообщения с аккаунтов друзей, предлагая получить бесплатную подписку на Telegram Premium. Пользователи переходили по оформленной ссылке, вводили свои данные на поддельном сайте, после чего злоумышленники получали доступ к аккаунту.
- Фальшивые страницы входа в Telegram, где пользователи, не подозревая ни о чем, вводили свои учетные данные, которые затем использовались для несанкционированного доступа к аккаунтам.
- Поддельные интернет-ресурсы, где предлагалось проголосовать, требуя ввести личные данные или авторизоваться через Telegram, что приводило к компрометации аккаунта.
- Копирование личного чата «Избранное»: создается поддельный раздел «Избранное» в аккаунте пользователя в ожидании, когда тот добавит туда важную информацию, чтобы затем ею воспользоваться.
- Получение дубликатов SIM-карт жертв, перехватывая одноразовые коды из SMS, используемые для входа в Telegram, что позволяло им получить доступ к аккаунтам.

Ответные действия

Если взломали аккаунт, срочно закройте все лишние сессии доступа к аккаунту, включите и смените облачный пароль, сообщите вашим контактам о взломе любыми доступными способами.

Выводы и рекомендации

- Для защиты от подобных угроз рекомендуется соблюдать осторожность при переходе по ссылкам, не вводить личные данные на подозрительных интернет-ресурсах, использовать двухфакторную аутентификацию и устанавливать сложные пароли.
- Подсказка пароля должна быть понятна только вам.
- Рекомендуется разделять профили, предназначенные для различных целей. Официальное приложение поддерживает до трех аккаунтов.
- Включите облачный пароль в настройках безопасности.

3. **Кибергигиена и защита пользователей,** советы на 2025

Угрозы информационной безопасности в 2025 году станут всё более изощрёнными и нацеленными, что подчеркивает критическую важность кибергигиены. Осведомлённость о современных схемах мошенников и базовые знания о защите информации - залог безопасности как для организаций, так и для индивидуальных пользователей.

Одной из актуальных угроз стали дипфейк-атаки, в которых злоумышленники используют нейронные сети для имитации голоса жертвы.

Сценарий таких атак включает следующие этапы:

Этап	Описание
Поиск жертвы	Мошенники изучают публичные аккаунты в социальных сетях, собирая аудио- или видеоматериалы с голосом жертвы.
Создание синтетического голоса	Аудиодорожка длительностью всего до 3 минут позволяет синхронизировать голос через нейросети.
Регистрация поддельного аккаунта	Злоумышленники через SIM-Box арендуют казахстанские номера для регистрации аккаунтов в WhatsApp.
Рассылка аудиосообщений	Созданный голос используется для массовой рассылки сообщений среди контактов жертвы. Например, злоумышленники могут просить финансовую помощь или делиться важной информацией от имени жертвы.

Эта схема подкрепляется фишинговыми ссылками.

Среди распространённых сценариев:

- Мошенники отправляют сообщение с просьбой «проголосовать за ребёнка коллеги», предлагая пройти по ссылке, якобы ведущей на страницу голосования.
- После перехода пользователю предлагают авторизоваться через аккаунт в мессенджерах WhatsApp или Telegram для подтверждения. На самом деле реализуется атака типа «человек посередине» (MITM), где злоумышленник перехватывает сессию пользователя.

В результате они могут:

- Получить неправомерный доступ к учетной записи жертвы и начать рассылку сообщений от её имени.
- Использовать ранее сгенерированные аудиозаписи для усиления обмана среди контактов.

Советы для защиты от таких атак:

- Скрывайте личную информацию в социальных сетях. Настройте приватность аккаунтов, чтобы только друзья могли видеть ваши публикации, а также старайтесь не публиковать голосовые или видеозаписи без необходимости.
- Будьте внимательны к подозрительным сообщениям. Если сообщение от близкого человека кажется необычным или срочным, свяжитесь с ним другим способом для подтверждения, а также никогда не вводите личные данные на сомнительных интернет-ресурсах.

- Используйте двухфакторную аутентификацию, это добавляет дополнительный уровень защиты для ваших аккаунтов.
- Следите за уведомлениями безопасности, многие мессенджеры уведомляют о попытке авторизации с нового устройства.

Почему кибергигиена критически важна в 2025 году?

Сложность атак	Современные схемы включают сложные комбинации социальной инженерии и технологий, такие как нейросети и MITM-атаки.
Вектор на пользователя	В большинстве случаев конечной целью становится человек, а не техника. Это требует повышения уровня грамотности в вопросах ИБ
Сохранение репутации	Скомпрометированная учетная запись может нанести ущерб репутации, особенно если злоумышленники распространяют вредоносные ссылки или проводят финансовые махинации от имени жертвы.

Современные цифровые технологии сделали нашу жизнь проще, но вместе с этим открыли **новые пути для мошенников и кибератак.**

Чтобы защитить себя и свои данные, **важно развивать кибергигиену -** привычки, которые обеспечивают вашу **безопасность в цифровом мире.**

Начните с настройки конфиденциальности на ваших аккаунтах в социальных сетях.

Открытые профили – это подарок для злоумышленников, которые могут использовать ваши данные для создания фишинговых атак или даже кражи личности.
Убедитесь, что только доверенные люди имеют доступ к вашим публикациям, фотографиям и информации о месте работы.
Не публикуйте данные, которые могут быть использованы против вас, включая личные контакты или финансовую информацию.

С каждым годом мессенджеры становятся главной целью хакеров.

Включите уведомления о входе с нового устройства, чтобы знать, если кто-то пытается проникнуть в ваш аккаунт.
Не забывайте о резервном копировании важных чатов в облако, но делайте это только с помощью безопасных сервисов.
Будьте осторожны, если незнакомец отправляет вам сообщение.
Проверьте профиль и не открывайте подозрительные вложения.

Внимательно изучайте ссылки, прежде чем переходить по ним.

Особенно это касается электронных писем и сообщений от неизвестных отправителей.
Простой совет: наведите курсор на ссылку, чтобы увидеть её реальный адрес. Если он выглядит подозрительно, не переходите по нему, а проверьте его через сервисы, такие как VirusTotal.

Фишинговые письма могут выглядеть максимально правдоподобно: логотипы компаний, официальные названия, даже поддельные подписи известных людей.

Но их цель - украсть ваши данные. Признаки фишинга включают грамматические ошибки, настойчивые просьбы отправить данные или пройти по ссылке. Если вы получили такое письмо, не спешите отвечать.
Проверьте отправителя через официальный интернет-ресурс компании.

Ваши устройства — это ворота ко всем вашим цифровым данным.

Регулярно обновляйте операционную систему и приложения и применяйте обновления безопасности.
Установите антивирусное ПО для мониторинга подозрительной активности.
Применяйте сложные пароли или биометрию, чтобы никто не мог получить доступ к вашим данным в случае утери устройства.

Дети часто становятся лёгкой мишенью для киберпреступников.

Используйте функции родительского контроля, чтобы ограничить доступ к нежелательному контенту.
Проводите беседы с детьми и учите их критически относиться к тому, что они видят в интернете.

Утеря данных из-за вирусов или ошибок системы может стать катастрофой.

Регулярно делайте резервные копии в облаке или на внешнем носителе.
Для всех аккаунтов используйте уникальные сложные пароли.
Если их сложно запомнить, воспользуйтесь менеджерами паролей.

Подключите двухфакторную аутентификацию (2FA) там, где это возможно.

Даже если злоумышленник узнает ваш пароль, ему будет сложнее получить доступ без второго уровня защиты, будь то код из SMS или приложение-аутентификатор.

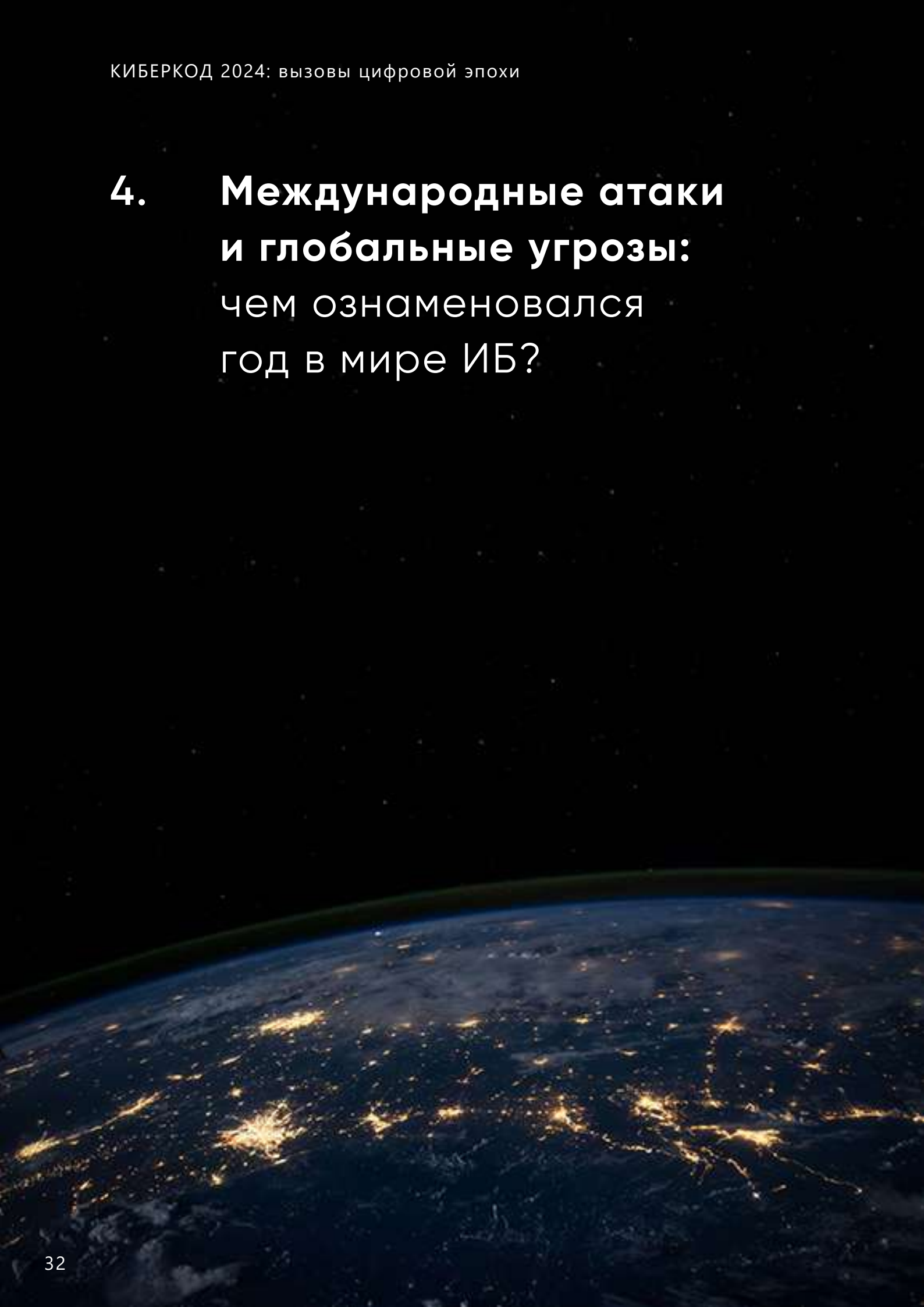
Регулярно проверяйте выписки по банковским картам.

Незначительные суммы, списанные без вашего ведома, могут быть тестовыми транзакциями мошенников.
При появившихся подозрениях немедленно блокируйте карту и свяжитесь с банком.

В 2025 году защита пользователей от угроз информационной безопасности требует комплексного подхода, включая технические меры, такие как антивирусы, VPN и системы фильтрации, а также повышение осведомленности и обучение.

Важно помнить, что самыми уязвимыми элементами в системе безопасности остаются люди, поэтому регулярные тренинги и киберучения становятся необходимыми для создания культуры информационной безопасности в организациях и среди пользователей.

4. **Международные атаки и глобальные угрозы:** чем ознаменовался год в мире ИБ?



Среди ключевых трендов 2024 года выделяются изменения в технологических предпочтениях: растёт спрос на решения, которые позволяют оперативно выявлять уязвимости и укреплять защиту.

Например, системы анализа сетевого трафика, межсетевые экраны нового поколения и инструменты защиты почты стали более востребованными, поскольку обеспечивают мгновенный эффект. Одновременно увеличилась популярность багбаунти-программ, которые используют компании самых разных сфер, от страховых организаций до государственных структур. В 2025 году ожидается удвоение числа компаний, запускающих такие программы.

Технологическим прорывом стали киберполигоны, позволяющие моделировать атаки и тестировать защитные меры. Компании внедряют такие платформы для анализа цепочек событий и оценки последствий атак. Востребованы также подходы, усложняющие путь злоумышленников через изменение ИТ-инфраструктуры.

На международном рынке продукты, ориентированные на результативную кибербезопасность, привлекают внимание компаний из разных регионов: Ближнего Востока, Латинской Америки, Юго-Восточной Азии и Африки. Кроме того, компании активно обучают сотрудников навыкам безопасной разработки приложений.

На образовательном рынке продолжает расти интерес к программам, развивающим современные компетенции в области кибербезопасности. В 2024 году компании запустили десятки образовательных инициатив, включая международные программы и магистерские направления. Появляются также краткосрочные курсы, которые помогают специалистам быстрее адаптироваться к растущему числу атак и новым технологиям.

В глобальном индексе кибербезопасности Казахстан набрал **94,04 балла из 100 возможных**

В 2025 году эксперты прогнозируют рост числа кибератак и дальнейшее развитие технологий ИИ, в связи с этим, эти вызовы потребуют от компаний не только использования передовых технологий, но и подготовки кадров, способных оперативно реагировать на угрозы.

В глобальном индексе кибербезопасности Казахстан набрал 94,04 балла из 100 возможных. Международный союз электросвязи *(ITU)* при ООН опубликовал доклад «Глобального индекса кибербезопасности 2024» *(GCI)*. Согласно новой методике, позиция Казахстана расположена во второй группе *(Tier 2 – Advancing)*.

2024 год стал настоящим испытанием для мирового сообщества в сфере информационной безопасности. С одной стороны, мы наблюдаем рост числа атак на критически важные инфраструктуры и крупные корпорации, с другой - усиление сотрудничества между странами и технологическими гигантами в борьбе с угрозами информационной безопасности. Этот год также подчеркнул необходимость обновления законодательных мер, внедрения новых технологий защиты и повышения осведомлённости среди пользователей.

В этом разделе мы рассмотрим наиболее заметные кейсы, которые не только отразили ключевые вызовы года, но и стали показательными примерами глобальных угроз в области кибербезопасности. Эти инциденты служат напоминанием о том, что кибератаки становятся всё более изощрёнными, а их последствия всё более масштабными.

Следует обратить внимание на международные кейсы утечек данных, поскольку они зачастую затрагивают и казахстанских пользователей. Такие инциденты становятся источником серьезных угроз, включая кражу личной информации, финансовые потери и риски для репутации.

Ранее мы уже описали крупные международные инциденты, которые затронули казахстанских пользователей. Среди них:

- ***Утечка данных пользователей платформы 1Win*** – значительное событие, ставшее причиной компрометации данных участников платформы для ставок, что повысило риски финансовых и личных потерь для пользователей.
- ***Инцидент с утечкой данных российской компании «Сирена-Тревел»***, где в обнародованной базе, файле «TICK_INFO_sample» оказались данные ряда авиакомпаний Казахстана. Это создало угрозы не только для пассажиров, но и для бизнес-процессов компаний.
- ***Утечка данных микрофинансовой организации zaimer.kz***, где были скомпрометированы данные более 2 миллионов казахстанцев. Этот случай стал знаковым примером того, как утечка может масштабироваться и затронуть значительную часть населения.

Важно понимать, что, несмотря на локальный характер некоторых инцидентов, злоумышленники часто используют одни и те же методы атак в разных странах. Это значит, что угроза может прийти и в Казахстан, особенно если организациям и пользователям не уделять должного внимания кибербезопасности. Среди глобальных кейсов 2024 года, которые также заслуживают упоминания, стоит выделить некоторые:

- ***Массовая утечка данных из крупнейшего банка Индии,*** где были скомпрометированы персональные и финансовые данные миллионов клиентов. Этот случай стал примером масштабной атаки на финансовый сектор.
- ***Взлом платформы криптовалютной биржи в США,*** что привело к потере активов на сумму свыше миллиарда долларов. Такие атаки показывают, насколько уязвимыми остаются даже высокотехнологичные компании.
- ***Утечка данных из образовательной платформы в Европе***, которая затронула миллионы студентов и преподавателей, а также включала персональную информацию несовершеннолетних граждан.

Эти инциденты подчёркивают, что каждая организация, независимо от её размера или географии, может стать целью атаки. Поэтому казахстанским пользователям и компаниям важно принимать превентивные меры.

Проверить, стали ли вы жертвой утечки данных, можно на отечественном ресурсе ***leak.citizensec.kz***, который анализирует базы данных, попавшие в открытый доступ. Альтернативно можно воспользоваться зарубежным сервисом ***haveibeenpwned.com***, который также проверяет ваши данные на наличие в утекших базах из DarkNet.

В условиях растущих угроз кибербезопасность перестала быть лишь технической задачей - это общая ответственность, требующая повышенного внимания как от организаций, так и от самих пользователей.

Сейчас предлагаем рассмотреть крупные инциденты в мировом масштабе, чтобы ещё раз подчеркнуть высокий уровень современных угроз и понять, как опыт других стран может быть полезен для предотвращения аналогичных атак в Казахстане.

АТАКА ВИРУСА-ВЫМОГАТЕЛЯ НА ASCENSION HEALTH SYSTEM РАСКРЫВАЕТ ДАННЫЕ ПАЦИЕНТОВ

В мае 2024 года некоммерческая медицинская система Ascension Health System, включающая 140 больниц в 19 штатах США и Вашингтоне, округ Колумбия, столкнулась с атакой вируса-вымогателя, которая парализовала её клинические операции. Инцидент начался после того, как сотрудник случайно загрузил вредоносное ПО. Это привело к перенаправлению экстренной помощи из нескольких больниц и серьезно повлияло на качество обслуживания пациентов.

Расследование показало, что злоумышленники получили доступ к конфиденциальной информации, включая медицинские данные пациентов. Взломанные файлы были размещены на сервере, используемом для рутинных задач сотрудников. Этот случай демонстрирует не только важность технических средств защиты, но и необходимость регулярного обучения персонала правилам кибербезопасности, чтобы минимизировать риск человеческого фактора.

КРУПНАЯ УТЕЧКА ДАННЫХ ВОЕННЫХ ВЕЛИКОБРИТАНИИ

В мае 2024 года Министерство обороны Великобритании столкнулось с крупной утечкой данных из системы расчета заработной платы, что затронуло конфиденциальную информацию 270 000 нынешних и бывших военнослужащих.

Среди скомпрометированных данных оказались имена, банковские реквизиты и адреса.

Атака произошла через уязвимость в системе стороннего подрядчика. В ответ министерство оперативно отключило сеть подрядчиков и уведомило пострадавших.

Премьер-министр Риши Сунак заявил о причастности «злонамеренного субъекта», а СМИ предположили связь с Китаем, что было официально опровергнуто. Несмотря на это, инцидент подчеркнул высокие риски атак со стороны национальных государств и необходимость ужесточения требований к подрядчикам в области кибербезопасности.

DELL DATA BREACH РАСКРЫЛА ИНФОРМАЦИЮ О 49 МИЛЛИОНАХ КЛИЕНТОВ В РЕЗУЛЬТАТЕ КРУПНОЙ КИБЕРАТАКИ

В мае 2024 года Dell сообщила о крупной утечке данных, которая затронула информацию примерно о 49 миллионах клиентах. Инцидент произошел из-за компрометации портала, где хранились данные о покупках клиентов. В результате утечки стали доступны имена, адреса, метки обслуживания заказов, даты заказов и гарантийная информация. Однако данные о платежах, электронные адреса и номера телефонов не пострадали, что помогло снизить потенциальные риски. Хакер, известный как Менелик, разместил украденные данные на Breach Forums, заявив, что они охватывают покупки с 2017 по 2024 год. Dell оперативно начала расследование, уведомила пострадавших и заверила, что конфиденциальная информация не была скомпрометирована. Этот инцидент подчеркивает важность защиты клиентских порталов и регулярного мониторинга их безопасности.

TICKETMASTER BREACH

В июне 2024 года Ticketmaster столкнулся с крупной утечкой данных, затронувшей 560 миллионов клиентов.

Группа хакеров ShinyHunters заявила о краже данных и потребовала выкуп в размере $500,000, угрожая продажей информации в DarkNet. Среди украденных данных оказались адреса электронной почты, имена пользователей и частичные данные кредитных карт, что поставило клиентов под угрозу мошенничества. Этот инцидент стал частью череды проблем с безопасностью компании.

В 2020 году Ticketmaster получил штраф в $10 миллионов за взлом конкурента, а в ноябре 2023 года кибератака нарушила продажу билетов на тур Taylor Swift's Era. Эти события подчеркивают недостатки в защите в индустрии развлечений и необходимость усиления мер безопасности.

УТЕЧКА ДАННЫХ SNOWFLAKE: СОТНИ ОРГАНИЗАЦИЙ ПОСТРАДАЛИ ОТ КРАЖИ УЧЕТНЫХ ДАННЫХ

В июне 2024 года Snowflake стал жертвой масштабной утечки данных, затронувшей сотни компаний, включая крупных клиентов, таких как Ticketmaster и Santander. Злоумышленники использовали украденные учетные данные для получения доступа к конфиденциальной информации, а в некоторых случаях требовали выкуп за украденные данные.

Важно отметить, что инфраструктура Snowflake не была напрямую скомпрометирована. Хакеры применяли вредоносное ПО для кражи информации, позволяя обойти даже многофакторную аутентификацию у некоторых пользователей.

Snowflake отвергла наличие уязвимостей в своих системах, подчеркнув, что атака была направлена на учетные записи клиентов. В ответ компания усилила протоколы безопасности и предложила рекомендации по защите данных.

Этот случай демонстрирует критическую важность управления идентификацией и доступом, особенно для организаций, использующих облачные сервисы. Надежные меры, такие как уникальные пароли, регулярное обновление учетных записей и многофакторная аутентификация, остаются ключевыми элементами защиты.

CDK GLOBAL RANSOMWARE ОБХОДИТСЯ ДИЛЕРАМ БОЛЕЕ ЧЕМ В 1 МИЛЛИАРД ДОЛЛАРОВ

В июне 2024 года CDK Global, крупный поставщик ПО для автомобильной отрасли стал жертвой атаки программ-вымогателей, организованной группировкой BlackSuit, связанной с Восточной Европой и Россией.

В результате загрузки вредоносного ПО сотрудником были зашифрованы важнейшие файлы, что вызвало сбой в системах компании и затронуло 15 000 автосалонов в Северной Америке.

Убытки составили более 1 млрд долларов.

Атака подчеркнула необходимость надежных мер защиты, планов реагирования на инциденты и усиленной защиты от программ-вымогателей.

AMERICAN WATER

3 октября 2024 года американская компания American Water, крупнейший поставщик воды подверглась кибератаке с использованием вымогательского ПО.
Атака привела к временной приостановке работы некоторых сервисов, включая онлайн-платформу для обслуживания клиентов, но критические операции водоснабжения и очистки сточных вод не пострадали. Расследование инцидента продолжается и среди возможных виновников рассматриваются государственно спонсируемые хакерские группировки. Этот инцидент подчеркнул уязвимость критической инфраструктуры и высокий риск для национальной безопасности, на что ранее обращали внимание власти США.

КИБЕРАТАКА НА NHS: СБОИ В МЕДИЦИНСКИХ СИСТЕМАХ ВЕЛИКОБРИТАНИИ

В июне 2024 года Национальная служба здравоохранения Великобритании (NHS) подверглась масштабной кибератаке, приведшей к сбоям в работе медицинских учреждений по всей стране.
Атака затронула критически важные медицинские данные, включая результаты анализов и данные о крови для трансфузий. Пациенты потеряли доступ к своим медицинским картам, а персонал столкнулся с проблемами при обработке данных и оказании экстренной помощи.
Инцидент подчеркнул уязвимость медицинской инфраструктуры и риски для безопасности данных пациентов.

CHANGE HEALTHCARE: УТЕЧКА ДАННЫХ 100 МИЛЛИОНОВ ЧЕЛОВЕК

24 октября 2024 года компания Change Healthcare, крупнейший поставщик решений в здравоохранении в США, стала жертвой кибератаки, затронувшей данные около 100 миллионов человек.
Злоумышленники получили доступ к персональной и медицинской информации клиентов, включая номера социального страхования, диагнозы и финансовую информацию.
Компания активировала протоколы реагирования, уведомила органы и начала сотрудничество с экспертами по кибербезопасности.
Атака подчеркнула уязвимость организаций, работающих с чувствительными данными, и необходимость усиления мер защиты.

LOANDEPOT: 16,6 МИЛЛИОНА ПОСТРАДАВШИХ КЛИЕНТОВ

В январе 2024 года американский ипотечный гигант LoanDepot стал жертвой кибератаки с использованием программ-вымогателей, затронувшей данные около 16,6 миллионов клиентов.
Атака привела к сбоям в работе компании, компрометации конфиденциальной информации, включая номера социального страхования и финансовые данные, и временной приостановке некоторых услуг.
Финансовые убытки составили 26,9 миллионов долларов, включая расходы на восстановление систем и улучшение безопасности.
Этот инцидент подчеркнул важность защиты данных и усиления мер безопасности в финансовом секторе.

КИБЕРАТАКА MIDNIGHT BLIZZARD НА MICROSOFT

В январе 2024 года корпорация Microsoft стала жертвой кибератаки, организованной группировкой Midnight Blizzard, предположительно связанной с российской Службой внешней разведки.
Злоумышленники использовали фишинговые письма с вложениями в формате RDP, подписанными сертификатом Let's Encrypt, для получения доступа к корпоративным почтовым ящикам, включая переписку руководства и сотрудников, работающих с кибербезопасностью.
Целью атаки был сбор информации о деятельности самой группировки.

БЭКДОР XZ ДЛЯ ОБХОДА SSH-АУТЕНТИФИКАЦИИ

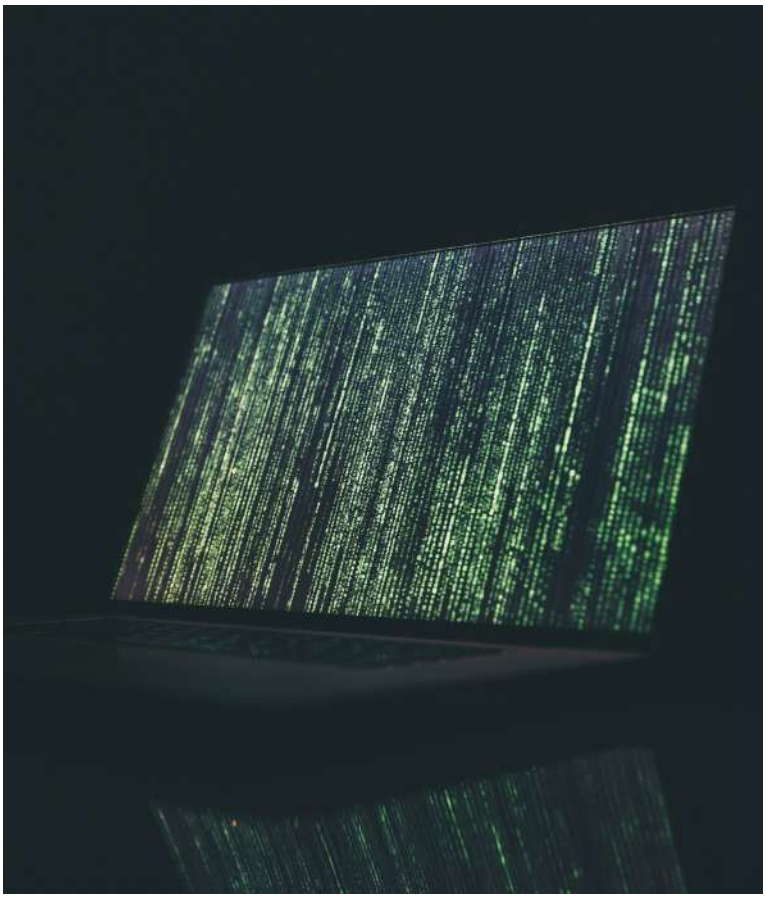
В марте 2024 года проект Openwall сообщил о бэкдоре в утилите сжатия XZ, используемой в дистрибутивах Linux. В отличие от предыдущих атак на цепочки поставок, эта была многоэтапной и затронула сотни тысяч SSH-серверов. Злоумышленники использовали социальную инженерию и подделывали участников сообщества, чтобы внедрить бэкдор.
Инцидент подчеркнул уязвимость проектов с открытым исходным кодом к таким атакам и необходимость усиления мер безопасности и контроля над участниками проектов.

КИБЕРАТАКИ НА СПУТНИКОВЫЙ ИНТЕРНЕТ

В 2024 году APT-группа провела целенаправленную атаку на космическую отрасль, используя бэкдоры.
В другом инциденте злоумышленники вызвали перебои в работе спутника финской энергоснабжающей компании Fortum. Хотя эти атаки не привели к глобальным сбоям, они подчеркивают растущие риски для спутниковой инфраструктуры.
Особенно опасными могут стать угрозы, связанные с цепочкой поставок спутникового интернета, таких как Starlink и Viasat, которые предлагают высокоскоростной интернет в удаленных районах, создавая дополнительные уязвимости для безопасности.

ЭКСПЛОЙТ ЯДРА В WINDOWS И LINUX

В 2024 году были выявлены несколько уязвимостей в ядре двух основных операционных систем, которые управляют важными объектами по всему миру.
В частности, уязвимость повышения привилегий в ядре Linux и уязвимость CVE-2024-21338 в Windows, позволяющая повысить привилегии учетной записи до уровня ядра, уже использовалась в реальных атаках.
Эти уязвимости увеличивают риск масштабных сбоев в глобальных цепочках поставок, подчеркивая важность своевременного выпуска исправлений и соблюдения лучших практик кибербезопасности для защиты стабильности цепочек поставок.



5. Искусственный интеллект в зоне риска: атаки и защита ИИ-систем

В эпоху быстрого развития искусственного интеллекта эти технологии становятся не только сильным инструментом для разрешения сложных задач, но и мишенью для многочисленных атак.

Современные угрозы становятся всё более сложными, а усиливающаяся зависимость от ИИ-систем акцентирует важность применения глубоких аналитических методов для обеспечения их защиты.

Расширение использования ИИ в различных отраслях делает его критически важным компонентом, от которого зависит устойчивость бизнеса и даже государственной инфраструктуры.

Ниже анализируются угрозы, вызванные использованием ИИ, и предлагаются меры для минимизации рисков.

АТАКИ НА ИИ: НОВЫЕ ТАКТИКИ И ОПАСНОСТИ

Полиморфные ВПО

Специалисты CyberArk продемонстрировали, как злоумышленники используют генеративные ИИ, такие как ChatGPT, для разработки полиморфных вредоносных программ. Эти программы динамически изменяют код, избегая обнаружения и адаптируясь к защитным системам. Например, ChatGPT позволяет генерировать уникальные фрагменты вредоносного кода, что усложняет его статический и поведенческий анализ. Более того, такие «вредоносы» могут быть использованы для атак на крупные организации, где защитные системы часто зависят от статического анализа. Эта угроза становится особенно актуальной для компаний, работающих в сфере финансов, медицины и государственных услуг, где компрометация данных может привести к катастрофическим последствиям.

Фишинг, усиленный ИИ

Согласно SlashNext, фишинговые атаки достигли беспрецедентных масштабов, благодаря использованию генеративных моделей ИИ. Основные тенденции включают:

- За последние 12 месяцев количество вредоносных писем выросло на 856%.
- Злоумышленники активно используют QR-коды и CAPTCHA для маскировки своих атак.
- ChatGPT позволяет создавать фишинговые письма, адаптированные под конкретных пользователей, что увеличивает вероятность успеха атак. Такие письма нередко содержат информацию, собранную из открытых источников, что делает их крайне убедительными.

Злоумышленники расширяют использование коммуникационных платформ, таких как Teams, Slack и Zoom. Это открывает новые возможности для атак, которые требуют интегрированных мер защиты. Например, атаки через мессенджеры становятся все более распространенными, так как пользователи склонны меньше обращать внимание на угрозы в личных коммуникациях.

DeepFake технологии позволяют создавать высоко реалистичные подделки изображений, видео и аудио. Эти подделки могут быть использованы для различных вредоносных целей:

- создание фальшивых новостей и видео, которые могут дестабилизировать общественное мнение и вызвать социальные беспорядки;
- использование DeepFake для шантажа, мошенничества и кражи личности;
- создание компрометирующих материалов против политиков или общественных деятелей;
- создание фальшивых видео с участием руководителей компаний для манипуляций на рынке или получения конфиденциальной информации.

Статистика

Согласно отчету за 2024 год от Security.org, количество DeepFake видео растет экспоненциально. В 2019 году было выявлено около 15,000 поддельных видео, в 2023 году - уже 145,000, что представляет собой рост на 866% за 4 года.

Применение DeepFake: 96% всех DeepFake видео в 2019 году использовались в порнографии без согласия, что является серьезным нарушением прав человека. Однако с каждым годом количество DeepFake, используемых для политических и корпоративных атак, значительно увеличивается.

Ущерб от DeepFake: в 2023 году компании по всему миру потеряли более 250 миллионов долларов из-за атак, связанных с DeepFake. Эти атаки включают в себя подделку видео и аудио, используемых для обмана партнеров и клиентов, а также для получения конфиденциальной информации.

МЕТОДЫ ЗАЩИТЫ ОТ DEEPFAKE АТАК: ТЕХНОЛОГИИ, ОБРАЗОВАНИЕ И ЗАКОНЫ

DeepFake-технологии становятся всё более сложными, что увеличивает риски их использования для мошенничества, манипуляции общественным мнением и других преступных целей. Как защититься от этих угроз? Современные подходы к борьбе с DeepFake включают комбинацию технологий, образовательных инициатив и законодательных мер.

Обнаружение DeepFake: мощь ИИ в действии.

Для выявления поддельных видео и аудио ключевую роль играют технологии анализа и алгоритмы. Современные системы, основанные на искусственном интеллекте и машинном обучении, способны анализировать такие параметры, как мимика, текстура кожи или даже мельчайшие аномалии в движениях. Например, неестественные движения глаз или ошибки в отражении света на лице часто выдают подделку.

Алгоритмы, специально разработанные для поиска артефактов, оставляемых генеративными моделями, ещё один эффективный инструмент. Они нацелены на выявление тонких несовершенств, которые остаются при создании DeepFake-контента, помогая отделить подлинное видео от фальсифицированного.

Аутентификация контента: цифровые следы.

Технологии аутентификации играют важную роль в защите медиафайлов. Один из таких методов - использование цифровых водяных знаков и блокчейн-платформ. Эти инструменты помогают отслеживать изменения в файле и подтверждать его источник. Например, верификация с помощью блокчейна может гарантировать, что видео не было подделано с момента его создания.

Методы криптографии, такие как уникальные цифровые подписи и шифрование данных, обеспечивают целостность контента и исключают возможность его подмены. Эти подходы становятся стандартом для защиты критически важных данных и предотвращения их использования в мошеннических целях.

Образование: важный элемент защиты.

Технологические меры не могут быть эффективными без участия людей. Образовательные программы для общественности и организаций помогают понять, какие риски несут DeepFake и как их распознать. Например, обучение сотрудников методам проверки подлинности видео может значительно снизить вероятность успешных атак, основанных на фальсифицированном контенте.

Кроме того, важно повышать осведомлённость населения о критическом восприятии информации. Проверка источников и анализ подозрительных материалов должны стать привычной практикой, особенно в эпоху социальных сетей, где DeepFake может распространяться мгновенно.

Законодательство и сотрудничество: глобальный подход.

Решение проблемы DeepFake невозможно без правовой базы. Законодательные меры, направленные на уголовное преследование за создание и распространение поддельных видео, формируют основу борьбы с этой угрозой. Например, установление ответственности

за использование DeepFake в целях дискредитации или вымогательства может служить мощным сдерживающим фактором.
Не менее важно сотрудничество между технологическими компаниями, правительствами и правоохранительными органами. Разработка единых стандартов и протоколов, обмен данными и совместное создание технологий для выявления подделок помогают противостоять угрозе на международном уровне.
Эффективная защита от DeepFake требует сочетания высоких технологий, грамотного образования и чёткой правовой регламентации. Эти меры не только минимизируют риски использования поддельного контента, но и способствуют формированию более безопасного цифрового пространства, где информация остаётся подлинной и достоверной.

Использование ИИ для защиты.
Для противодействия угрозам компании используют ИИ, внедряя:
- Генеративные ИИ для анализа угроз в реальном времени. Эти системы могут не только выявлять угрозы, но и прогнозировать их развитие, что особенно важно для защиты от полиморфных атак.
- Инструменты, позволяющие обнаруживать сложные схемы атак, такие как полиморфные ВПО. Например, технологии, основанные на машинном обучении, способны анализировать поведенческие данные пользователей, чтобы выявлять подозрительную активность.
- Технологии мониторинга, которые охватывают все цифровые каналы коммуникации. Это включает в себя мониторинг электронной почты, мессенджеров и облачных сервисов, которые становятся основными целями для злоумышленников.

Современные подходы.
Прогрессивные решения включают автоматизацию анализа угроз, интеграцию платформ управления доступом и создание систем, способных прогнозировать потенциальные атаки до их реализации. Например, использование решений на базе ИИ, которые интегрируются с системами управления инцидентами, позволяет значительно ускорить реакцию на угрозы. Такие системы также могут автоматизировать рутинные задачи, освобождая ресурсы для анализа более сложных инцидентов.

Обучение сотрудников.
Человеческий фактор остается уязвимым звеном. Регулярное обучение сотрудников методам распознавания фишинговых атак и защите от них является ключевым компонентом комплексной безопасности. Более того, обучение должно быть адаптировано под конкретные роли сотрудников, так как атаки часто нацелены на определенные отделы, такие как бухгалтерия или отдел кадров. Кроме того, важно регулярно проводить симуляции атак, чтобы сотрудники могли лучше подготовиться к реальным угрозам.
Искусственный интеллект открывает новые горизонты как для инноваций, так и для угроз информационной безопасности. Только внедрение интегрированных решений, использование передовых технологий и активное обучение персонала позволят минимизировать риски и обеспечить устойчивое развитие этой критически важной области. Важно понимать, что угрозы эволюционируют и защита должна развиваться вместе с ними. Организации, которые активно инвестируют в защиту своих ИИ-систем, не только минимизируют риски, но и укрепляют доверие своих клиентов и партнеров, создавая устойчивую и безопасную цифровую среду.

6. Защита АСУ ТП: текущие риски и наилучшие практики

Автоматизированные системы управления технологическими процессами играют ключевую роль в современной промышленности. АСУ ТП стали неотъемлемой частью многих отраслей, включая промышленность, энергетику, транспорт и инфраструктуру. Эффективность работы с АСУ ТП заключается в обеспечении управления, мониторинга и оптимизации производственных процессов в реальном времени. Однако их использование сопряжено с растущими угрозами информационной безопасности, требующими оперативного реагирования и внедрения эффективных мер защиты.

Исследователи Лаборатории Касперского выделили три способа распространения вредоносных объектов на компьютерах АСУ ТП:

- Вредоносные объекты, используемые для первичного заражения. Это опасные веб-ресурсы, вредоносные скрипты и вредоносные документы.
- Вредоносное ПО следующего этапа. Это шпионское ПО, программы-вымогатели и майнеры.
- Самораспространяющееся вредоносное ПО. Это черви и вирусы.

Также исследователи Лаборатории Касперского отмечают, что отрасль автоматизации зданий продолжает оставаться лидером по доле заражений вредоносным ПО среди всех секторов АСУ ТП, в то время как по всем исследуемым отраслям наблюдается снижение уровня угроз уже второй квартал *(2024 года)* подряд. Основными источниками угроз для компьютерных систем в технологической инфраструктуре организаций остаются интернет, почтовые клиенты и съемные носители.

Исследователи компании Positive Technologies отметили ключевые риски и угрозы в АСУ ТП.

- Нарушение сетевого периметра. Выход в Интернет, особенно с устройств, не защищенных средствами защиты конечных точек, может привести к заражению вирусами-шифровальщиками или появлению бэкдоров, которые злоумышленники смогут использовать для обхода других уровней защиты.
- Использование уязвимых протоколов связи. Поскольку на устройствах верхнего уровня технологической сети *(на АРМ инженеров и операторов, SCADA-серверах)* специализированное ПО, необходимое для осуществления технологического процесса, установлено поверх классических ОС - Windows и Linux. Это означает, что большая часть атак будет нацелена на устройства верхнего уровня с использованием эксплойтов.
- Атаки на программируемые логические контроллеры (далее - ПЛК). Злоумышленник, имея доступ к ПЛК, может вызвать различные последствия: изменить индикации для оператора, что приведет к незаметным проблемам; отправить команду для перевода процесса в аварийное состояние; изменить настройки оборудования, ускорив его износ или позволив кражу ресурсов; заблокировать отправку команд на ПЛК, нарушив управление процессом.
- Эксплуатация дефолтных паролей. Программируются ПЛК с помощью специализированных IDE и имеют свои API, через которые IDE и выполняет настройку. В связи с этим могут возникнуть риски использования уязвимостей API.

- Использование слабых и словарных паролей в устройствах. В случаях, когда учетная запись, используемая для доступа, имеет дефолтный пароль, то злоумышленник может получить доступ к ПЛК с любого устройства, которое имеет сетевой доступ к контроллеру.
- Использование слабозащищенных версий протоколов.
- Неавторизованные чтения и записи тегов в ПЛК. Манипулируя значениями тегов, злоумышленники могут прослушивать сетевой трафик через протокол IEC 104, что может привести к коллапсу части распределительной сети.
- Неавторизованное взаимодействие по протоколам удаленного доступа.
- Подмена файлов проектов в системах SCADA и HMI. Риски подмены файлов проектов, такие как мнемосхемы *(пользовательский интерфейс),* которые видит оператор, алгоритмы, по которым SCADA-система обрабатывает данные от ПЛК и от оператора и учетные записи, имеющие доступ к пользовательскому интерфейсу, операции, которые они могут выполнять.
- Запуск инженерного и управляющего ПО в АСУ ТП.

НАИЛУЧШИЕ ПРАКТИКИ ЗАЩИТЫ: КАК МИНИМИЗИРОВАТЬ РИСКИ И УКРЕПИТЬ КИБЕРБЕЗОПАСНОСТЬ

Эффективная защита технологических систем требует внедрения комплексных и структурированных мер, которые охватывают все аспекты безопасности - от проектирования до эксплуатации.

Рассмотрим ключевые рекомендации для минимизации рисков и повышения устойчивости.

Сегментация сетей и контроль доступа

Разделение сети на зоны с разным уровнем доверия - важный шаг в предотвращении распространения угроз. Контроль взаимодействия между сегментами сети позволяет минимизировать последствия возможных атак. Для этого рекомендуется использовать промышленные межсетевые экраны, внедрять VPN для удалённого доступа и обязательно применять многофакторную аутентификацию для критически важных узлов. Такой подход создаёт дополнительные барьеры для злоумышленников, усложняя несанкционированный доступ.

Моделирование угроз и оценка рисков

Регулярное обновление моделей угроз и оценка рисков позволяют оставаться на шаг впереди злоумышленников. Модели угроз помогают выявлять новые уязвимости и классифицировать их по степени критичности. Это, в свою очередь, даёт возможность разрабатывать чёткий план действий для устранения наиболее опасных угроз и предотвращения возможных атак.

Комплексный подход к безопасности

Кибербезопасность должна быть встроена на всех этапах жизненного цикла АСУ ТП. Это включает:

- проектирование систем с учётом требований кибербезопасности;

- внедрение технологий защиты, таких как системы обнаружения вторжений *(IDS);*
- постоянный аудит и тестирование систем на уязвимости.

Такой комплексный подход позволяет создавать устойчивую архитектуру безопасности, готовую к противодействию современным угрозам информационной безопасности.

Автоматизация мониторинга и реагирования

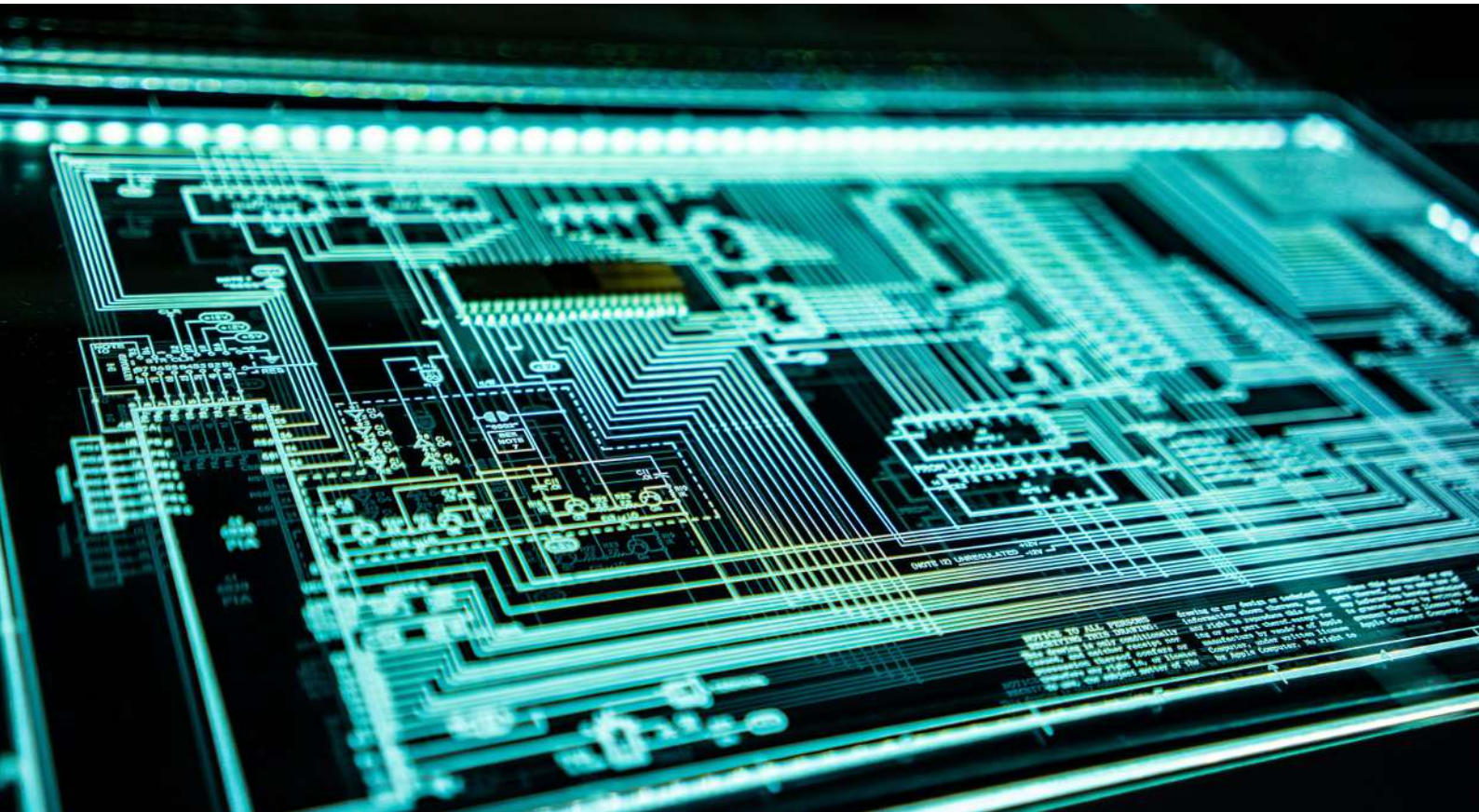
Использование SIEM-систем *(Security Information and Event Management)* и средств автоматизированного реагирования на инциденты обеспечивает оперативное выявление и блокировку угроз. DFIR-технологии *(Digital Forensics and Incident Response)* играют ключевую роль в расследовании инцидентов, помогая не только устранить последствия, но и разрабатывать превентивные меры для будущих атак.

Анализ внешнего трафика

Необходимость отслеживания внешнего сетевого трафика технологической сети очевидна: это помогает обнаружить возможные нарушения периметра безопасности. Регулярный мониторинг позволяет своевременно выявлять подозрительную активность и принимать меры по защите от несанкционированного доступа.

Регулярные обновления безопасности

Обновление устройств верхнего уровня технологической сети, таких как рабочие станции инженеров, операторы SCADA-серверов и другие критические узлы - важный аспект защиты. Регулярные патчи и обновления безопасности устраняют известные уязвимости и минимизируют риск успешных атак.



ОПРЕДЕЛЕНИЕ ГРАНИЦ И ИНВЕНТАРИЗАЦИЯ АКТИВОВ АСУ ТП: ШАГИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

1. Определение границ АСУ ТП

Необходимо четко определить, где заканчивается зона ответственности вашей системы. Это могут быть физические границы объектов, адреса подсетей или логические границы. Важно выделить активы внутри и за пределами системы, а также установить потоки данных *(входящие и исходящие)*.

2. Инвентаризация активов

Проводится полный учет всех устройств и систем, входящих в АСУ ТП, чтобы уточнить границы. Однако при использовании систем защиты информации важно учитывать, что их воздействие на оборудование может быть непредсказуемым, например, приводить к сбоям в работе. Для минимизации рисков рекомендуется использовать решения класса NTA *(Network Traffic Analyzer)*, которые анализируют копию трафика вместо прямого воздействия на устройства.

3. Контроль границ системы

Для защиты АСУ ТП необходимо контролировать входящий и исходящий трафик. Оптимальным решением является полная изоляция системы от внешней среды. Если изоляция невозможна, использовать диоды данных, которые позволяют передавать информацию только в одном направлении, исключая возможность обратного доступа.

4. Защита от вредоносного ПО

Все серверы и компьютеры должны быть защищены антивирусами и решениями класса EDR *(Endpoint Detection & Response)*. Но при внедрении этих инструментов нужно учитывать ограничения старых операционных систем, которые часто используются в АСУ ТП. Современные антивирусы могут быть несовместимы с устаревшими системами из-за высоких требований к ресурсам и отсутствия нужного функционала. Здесь помогут специализированные антивирусы, разработанные для таких условий.

5. Резервное копирование

Создание резервных копий – важнейший этап защиты, который включает:

- образы операционных систем серверов и компьютеров;
- конфигурационные файлы сетевого оборудования;
- проекты контроллеров;
- дистрибутивы ПО;
- базы данных, логины и пароли.

Системы резервного копирования и управления версиями конфигурационных файлов позволят быстро восстановить работоспособность системы в случае сбоев.

7. **Статистика угроз и инцидентов:** ТОП-5 информационной безопасности и их динамика

Самой значимой угрозой в сфере кибербезопасности остаются человеческие риски

Люди, как ключевой элемент всех бизнес-процессов, продолжают быть самым уязвимым звеном. Халатность, слабые или повторно используемые пароли, ошибки при обращении с конфиденциальной информацией и неосторожное поведение в Интернете создают огромные риски для организаций.

Согласно исследованию компании Mimecast, в 2023 году более 70% кибервзломов произошли из-за человеческих ошибок.

Это подтверждают данные Ponemon Institute, где среди главных причин инцидентов с инсайдерами выделены халатность, кража учетных данных и злой умысел. Такие угрозы показывают необходимость постоянного обучения сотрудников и внедрения строгих правил кибергигиены.

Фишинговые атаки продолжают оставаться одними из самых распространенных и эффективных.

Они успешно эксплуатируют человеческую психологию, а не технологические уязвимости. Злоумышленники создают убедительные письма, имитирующие сообщения от авторитетных компаний или партнеров, чтобы обманом заставить пользователей раскрыть конфиденциальные данные или установить вредоносное ПО.

В 2022 году число фишинговых атак выросло на 47,2%, а атаки на образовательный сектор увеличились на 576%.

Эти данные указывают на усложнение методов фишинга, включая использование ИИ для автоматизации атак, что требует от организаций усиленного контроля и постоянного повышения осведомленности сотрудников.

Программы-вымогатели стали символом роста числа сложных атак, приносящих злоумышленникам огромные прибыли.

В период с августа 2022 по май 2023 года число таких инцидентов выросло на 101,84%.

Эти атаки не только блокируют доступ к критически важным данным, но и вынуждают компании выплачивать значительные суммы в качестве выкупа. Пик активности пришелся на начало 2023 года, когда рост составил 65% по сравнению с аналогичным периодом 2021 года. Чтобы противостоять этой угрозе, организациям важно регулярно делать резервные копии данных и тестировать сценарии реагирования на инциденты.

Искусственный интеллект становится оружием в руках злоумышленников.

Он позволяет автоматизировать сложные атаки, такие как создание правдоподобных фишинговых писем или выявление уязвимостей в системах.

Особую опасность представляют атаки с использованием технологий Deepfake, которые могут обмануть даже опытных специалистов.

Эти угрозы динамичны: они развиваются вместе с мерами защиты, что делает их особенно сложными для нейтрализации. Это подчеркивает важность внедрения передовых технологий противодействия ИИ-угрозам.

Одной из самых разрушительных угроз остается компрометация деловой электронной почты (BEC). Атаки BEC, нацеленные на компании с международными поставщиками или активными банковскими переводами, привели к убыткам на сумму свыше 3 миллиардов долларов в 2023 году.

Злоумышленники выдают себя за руководителей или партнеров, чтобы обманом заставить сотрудников переводить средства или разглашать конфиденциальные данные. Эти атаки становятся все более изощренными и дорогими, подчеркивая необходимость строгого контроля операций и внедрения многофакторной аутентификации.

Все эти угрозы иллюстрируют текущие тенденции угроз информационной безопасности и подчеркивают важность системного подхода к их предотвращению.

Только сочетание технологий, обучения и проактивного управления безопасностью может помочь минимизировать риски и последствия таких атак

ТОП-5 угроз от ОЦИБ *(в КВОИКИ)*

Источник: ***misp.sts.kz***

Согласно информации, предоставляемой оперативными центрами информационной безопасности *(далее - ОЦИБ)* в 2024 году наиболее распространенными угрозами информационной безопасности для организаций *(в т.ч. КВОИКИ)* и пользователей Казахстана остаются вредоносное **ПО**, эксплуатация уязвимостей, спам-рассылки с вредоносными вложениями, несанкционированный доступ и Brute-force атаки. Наибольшую угрозу продолжает представлять вредоносное ПО, на долю которого приходится **49%** от всех зарегистрированных инцидентов ИБ, полученных от ОЦИБ. В первую очередь, это программы-вымогатели, вирусы и трояны, которые используются для блокировки данных и промышленного шпионажа. Анализ динамики демонстрирует, что активность вредоносного ПО была на пике в начале года *(январь-февраль)*, а затем снижалась до середины года, с новым ростом в сентябре и октябре, что совпадает с усилением атак на корпоративные сети в сезон высокой нагрузки.

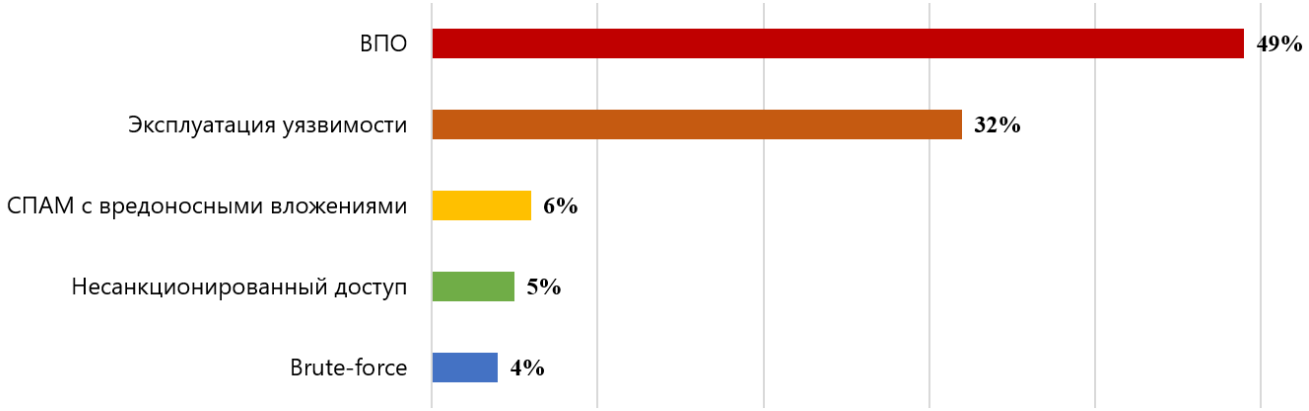
Второе место среди угроз занимает **эксплуатация уязвимости**, которая составляет **32%** от всех инцидентов. Данный вектор демонстрирует стремительный рост в течение всего года, особенно начиная с апреля и достигая максимума в декабре. Хакеры активно используют слабые места в устаревших системах и уязвимости нулевого дня, что позволяет им проникать в сети организаций до выхода необходимых обновлений безопасности.

Спам с вредоносными вложениями, несмотря на более низкие показатели *(6%)*, остаётся стабильным источником угроз на протяжении всего года. Небольшие всплески активности фиксировались летом, особенно в июне и августе, когда наблюдался рост фишинговых кампаний. Основной вектор атаки - распространение вредоносного ПО через электронные письма и ссылки, нацеленные на человеческий фактор.

Несанкционированный доступ занимает четвёртое место с долей **5%** от общего числа инцидентов. Пик активности был зафиксирован в феврале и марте, после чего наблюдается значительный спад, связанный с более активным внедрением многофакторной аутентификации и усилением контроля доступа во многих организациях РК, что позволило снизить количество успешных атак.

Замыкают список **Brute-force** атаки *(4%)*, направленные на подбор паролей методом перебора. Данный тип атак сохраняет стабильный уровень угроз с небольшим ростом в сентябре и октябре. Они остаются опасными для слабо защищённых учётных записей и систем с простыми паролями.

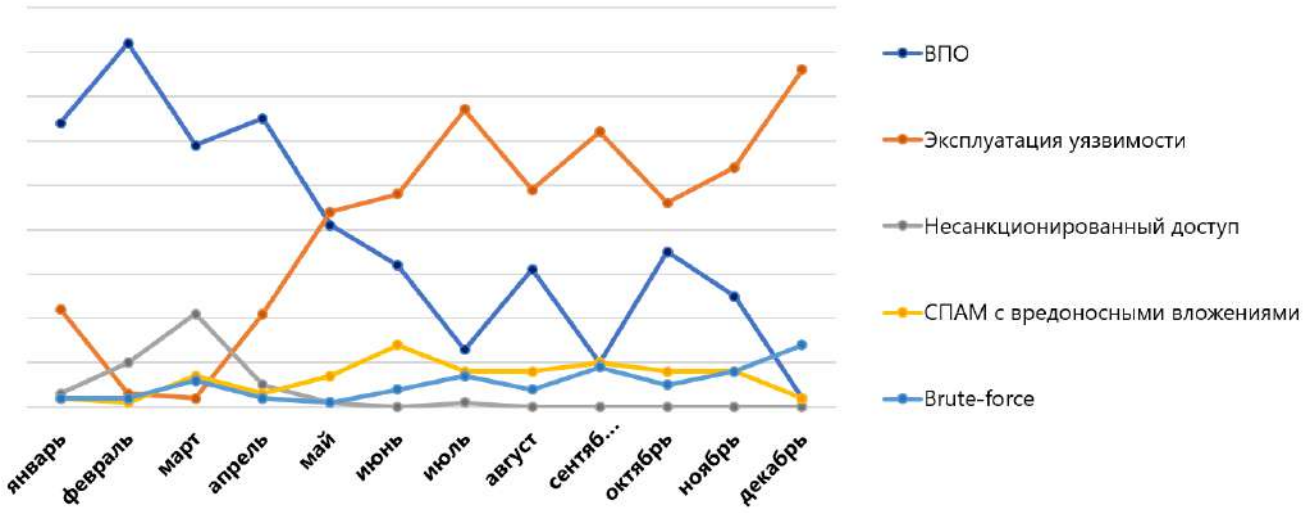
ТОП-5 угроз информационной безопасности от ОЦИБ



Анализ угроз информационной безопасности за 2024 год демонстрирует, что Казахстан, как и другие страны, продолжает сталкиваться с растущей сложностью угроз. Особенно заметным становится активный рост атак на информационные системы, которые не успели адаптироваться к современным вызовам, что подчёркивает необходимость своевременного обновления программного обеспечения и внедрения более надёжных защитных мер.

Также важно отметить, что совместная работа НКЦИБ, ОЦИБ и их клиентов создаёт основу для устойчивой и эффективной системы защиты, способной противостоять современным вызовам и обеспечивать стабильность цифровой среды.

Динамика изменения угроз от ОЦИБ



Статистика угроз и инцидентов:
Топ-5 угроз информационной безопасности и их динамика

Угрозы информационной безопасности продолжают набирать обороты, о чём свидетельствует динамика инцидентов и событий информационной безопасности.

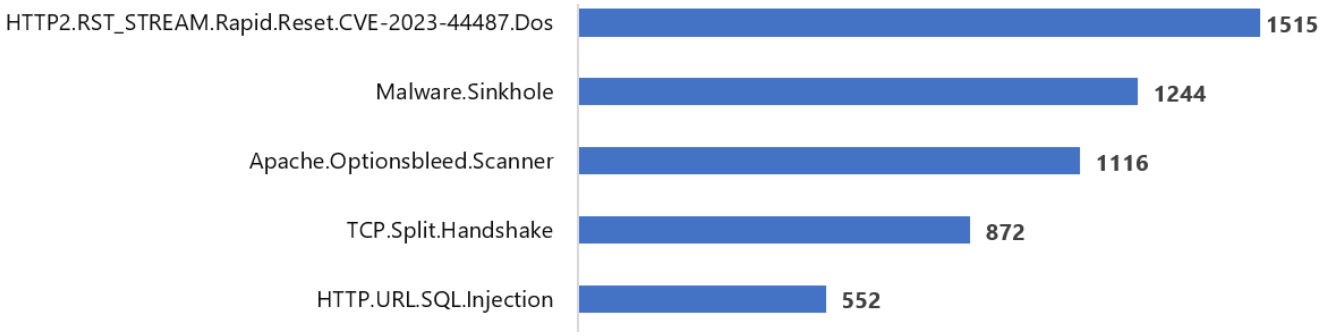
С января 2024 года на веб-платформе информационного взаимодействия НКЦИБ было зарегистрировано более 29,6 тысяч инцидентов, отражающих разнообразие и сложность современных атак.

Анализ показывает, что наибольшую активность демонстрируют пять ключевых типов угроз, формирующих основные вызовы для организаций по всему миру. Лидером остаётся вредоносное ПО, которое охватывает более трети всех инцидентов и становится инструментом для компрометации данных, систем и инфраструктур.

Рассмотрим подробнее основные угрозы и их влияние на информационную безопасность.

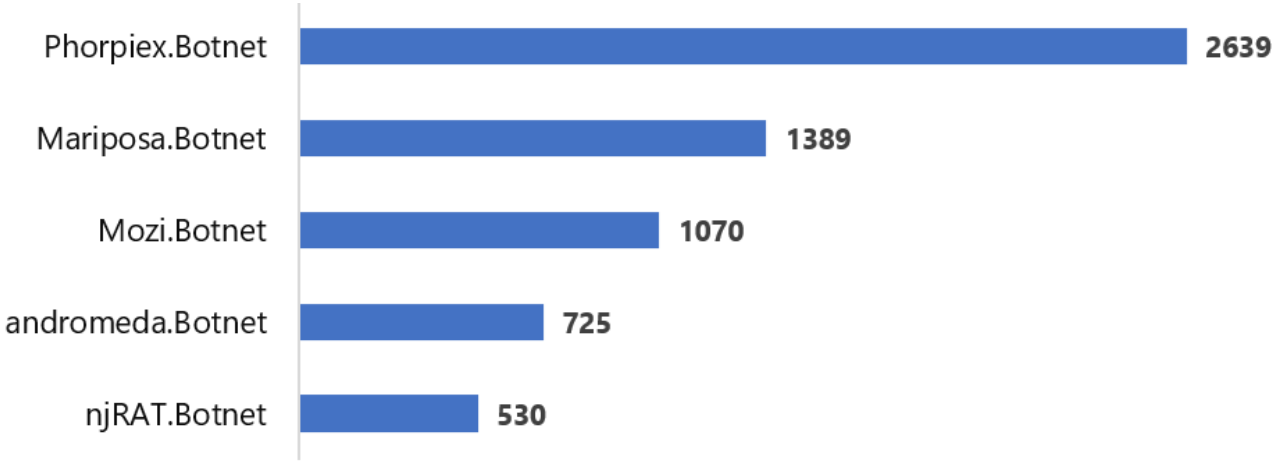
Вредоносное ПО – 10 700

Наиболее распространённые типы вредоносных ПО:



Ботнет – 8 420

Наиболее распространённые типы ботнета:



Эксплуатация уязвимости – 3 877

Наиболее распространённые типы RFI/LFI/Directory Traversal, XSS, Command Injection, SQL Injection.

49,6 % зафиксированных событий направлены на квазигосударственный сектор и 48 % направлены на государственный сектор.

Фишинговая атака – 3 720

Большинство фишинговых ресурсов использует такие типы имитации фишинга, как клоны интернет-ресурсов, розыгрыши и лотереи, формы авторизации.

В 2024 году количество фишинговых интернет-ресурсов, эмулирующих деятельность банков второго уровня РК, составляет 95.

DoS/DDoS-атака – 117

Наиболее распространёнными типами зафиксированных DoS/DDoS-атак являются ACK flood, SYN flood (TCP/SYN) и UDP flood.

35 % зафиксированных DoS/DDoS-атак направлены на банки второго уровня РК и 22 % на государственный сектор.

8. **Уязвимости и эксплойты года:** наиболее опасные точки входа

Начало I квартала 2024 года ознаменовалось «наводнением» уязвимостей 0-day

Отметим массовую эксплуатацию уязвимостей серверов ScreenConnect - ПО для удаленного управления компьютерами и другими устройствами. Раскрытые в феврале недостатки получили идентификаторы CVE-2024-1709 и CVE-2024-1708 и оценки 10 баллов *(критический уровень опасности)* и 8,4 балла *(высокий уровень опасности)* по CVSS соответственно.

Первая уязвимость позволяет злоумышленнику удаленно выполнить код в системе, а вторая-создать учетную запись с правами администратора и затем получить доступ к внутренним ресурсам компании. В CISA уязвимость CVE-2024-1709 внесли в каталог известных эксплуатируемых уязвимостей и обязали федеральные агентства США обеспечить безопасность своих серверов в срок до 29 февраля.

Операторы шифровальщиков сразу взяли обнаруженные недостатки ScreenConnect на вооружение.

Аналитики Sophos X-Ops сообщили, что злоумышленники активно эксплуатировали эти уязвимости и внедряли созданную на основе утекшего в 2022 году исходного кода LockBit программу-вымогатель.

Исследователи Trend Micro также сообщили о том, что известные группировки Black Basta и Bl00dy после раскрытия уязвимостей начали активно использовать недостатки ScreenConnect в своих атаках. Наравне с упомянутыми группировками, Trend Micro были замечены злоумышленники, использующие модульное ВПО XWorm, обладающее возможностями для удаленного доступа и функциями программ-вымогателей.

Уязвимости ScreenConnect не остались без внимания и у APT-группировок.

Так, по сообщениям аналитиков Kroll, группировка Kimsuky *(также известная как APT43)* использовала CVE-2024-1709 и CVE-2024-1708 для последующего заражения целевой системы новым вариантом вредоносного ПО, получившим название ToddlerShark.

Помимо уже описанных недостатков решений Ivanti и ScreenConnect, мы отмечаем и другие уязвимости, актуальные для первого квартала 2024 года:

CVE-2023-48022 Согласно отчету Oligo, злоумышленники используют уязвимость в популярном фреймворке Ray с открытым исходным кодом (он используется для машинного обучения, научных вычислений и обработки данных). Исследователи обнаружили, что сотни общедоступных Ray-серверов были скомпрометированы с помощью CVE-2023-48022, что позволило злоумышленникам получить доступ к конфиденциальной информации, включая исходный код моделей искусственного интеллекта, учетные данные базы данных и токены доступа к облачной среде.

CVE-2023-48788 Эта широко эксплуатируемая уязвимость представляет собой SQL-инъекцию в программное обеспечение FortiClient EMS и позволяет выполнять произвольный код или команды с помощью специально созданных запросов, обеспечивая первоначальный доступ в корпоративные сети организации.

CVE-2024-21893 Активно эксплуатируемая уязвимость была раскрыта 31 января. Она позволяет злоумышленнику обойти аутентификацию и получить доступ к шлюзам Ivanti. Исследователи Orange Cyberdefense пишут об успешной эксплуатации уязвимости для последующего развертывания бэкдора DSLog.

CVE-2024-27198 Уязвимость, получившая 9,8 баллов (критический уровень) по CVSS, затрагивает множество версий TeamCity, позволяя злоумышленнику получить контроль над уязвимым сервером с правами администратора. Эксперты Trend Micro отмечают, что после успешной эксплуатации злоумышленники устанавливали различное ВПО: шифровальщики BianLian и Jasmin, майнер XMRig и ВПО для удаленного управления SparkRAT.

CVE-2024-21762 Это уязвимость в FortiOS, операционной системе, используемой на устройствах Fortinet, включая FortiGate SSL VPNs. Классифицированная как out-of-bounds write, позволяет удаленным неаутентифицированным злоумышленникам выполнять произвольный код или команды на устройствах FortiGate. Атака может быть осуществлена через специально подготовленные HTTP-запросы, что открывает возможность для взлома и использования устройства для дальнейших атак. С момента раскрытия она была включена в список известных уязвимостей (KEV) CISA, что подтверждает ее активное использование в реальных атаках. Продукты, которые подвержены этой уязвимости, включают FortiOS версии с 6.0 по 7.4.2, а также FortiProxy. Чтобы устранить проблему, рекомендуется обновить FortiOS до версии 7.4.3 или выше, а также другие версии, указанные в рекомендациях Fortinet.

CVE-2024-36401 Это уязвимость удаленного выполнения кода (RCE), которая была обнаружена в популярных версиях сервера GeoServer (до 2.23.6, 2.24.4 и 2.25.2). Геосервер используется для обмена и обработки геопространственных данных. Уязвимость возникает из-за проблем в API библиотеки GeoTools, который небезопасно передает имена атрибутов в библиотеку commons-jxpath, что позволяет выполнить произвольный код через специально подготовленные запросы. Атака может быть использована для получения несанкционированного доступа к серверу с возможностью выполнения произвольных команд, что может привести к компрометации сервера или утечке данных. Для защиты от этой уязвимости GeoServer выпустил патчи, устраняющие проблему. Пользователям рекомендуется обновить сервер до версий 2.23.6, 2.24.4 или 2.25.2. Если обновление невозможно, временным решением является удаление уязвимой части кода, что, однако, может нарушить функциональность сервера.

CVE-2024-21683 Представляет собой уязвимость удалённого выполнения кода (RCE), обнаруженную в Atlassian Confluence Data Center и Confluence Server. Уязвимость с высокой степенью критичности (CVSS 8.3) позволяет авторизованному злоумышленнику выполнить произвольный код на целевой системе без взаимодействия с пользователем, что может существенно повлиять на конфиденциальность, целостность и доступность данных. Это делает её особенно опасной для корпоративных сред, где Confluence часто используется как внешняя платформа для взаимодействия и обмена информацией.
Проблема была обнаружена в версии Confluence 5.2 и публично раскрыта с кодом для эксплуатации, что значительно увеличивает риск её использования в реальных атаках. Чтобы устранить уязвимость, рекомендуется немедленно обновить системы до последних исправленных версий Confluence.

CVE-2024-24919 Уязвимость в Check Point Security Gateways может позволить злоумышленникам получить доступ к конфиденциальной информации при условии, что устройство подключено к интернету и включены Remote Access VPN или Mobile Access Software Blades. Приводит к утечке данных и может быть использована для дальнейших атак, если ее не устранить.

CVE-2024-21378 Уязвимость удаленного выполнения кода (RCE) в Microsoft Outlook. Для ее эксплуатации злоумышленнику необходимо быть аутентифицированным пользователем в сети и отправить вредоносный файл, который пользователь должен открыть. Уязвимость также может быть активирована через панель предварительного просмотра, что делает её опасной, поскольку достаточно простого открытия файла, чтобы атака сработала. Эта уязвимость получила рейтинг 8.8 по шкале CVSS и относится к категории высоких рисков.

Бэкдор XZ **Был обнаружен 29 марта 2024 года разработчиком Андресом Фройндом, который работал над устранением проблем с производительностью в Debian Sid.**

Он заметил, что SSH-соединения потребляют слишком много ресурсов процессора и вызывают ошибки в Valgrind. После тщательного анализа Фройнд обнаружил, что причиной этих проблем были изменения в библиотеке liblzma, используемой утилитой сжатия XZ. Бэкдор был внедрен в версии 5.6.0 и 5.6.1 XZ Utils. Его целью было обеспечение удаленного выполнения кода на сервере через SSH. Злоумышленник, использующий псевдоним Jia Tan, смог внедрить вредоносный компонент в легитимную библиотеку, используя сложные методы социальной инженерии и длительную кампанию по завоеванию доверия в проекте. Вредоносный код был скрыт в тестовых файлах и активировался во время процесса сборки.

Этот инцидент стал одной из самых сложных и продуманных атак на цепочку поставок, почти достигнув глобального масштаба.

Вредоносные версии XZ были обнаружены в нескольких дистрибутивах Linux, включая Fedora и Debian. Атака на проект XZ Utils была тщательно спланирована и включала использование нескольких фиктивных личностей, таких как Jia Cheong Tan, Dennis Ens и Jigar Kumar, для завоевания доверия и получения доступа к исходному коду проекта. Основная цель атаки заключалась в том, чтобы внедрить бэкдор в процесс сборки XZ Utils и распространить его через крупные дистрибутивы Linux. Вредоносный код был внедрен в феврале и марте 2024 года и атака была сравнима с инцидентами, такими как компрометация SolarWinds. Фиктивные личности активно взаимодействовали друг с другом и с создателем проекта Лассе Коллином, создавая видимость необходимости смены мейнтейнера, что позволило Jia Cheong Tan получить доступ к исходному коду и внедрить бэкдор.

Бэкдор использует несколько хитрых методов для скрытия своей активности и обеспечения доступа злоумышленника к зараженному серверу. Одним из ключевых аспектов является использование стеганографии в x86-коде для скрытия публичного ключа, что затрудняет его обнаружение. Бэкдор также перехватывает функции аутентификации по паролю и публичному ключу, позволяя злоумышленнику входить на сервер с любым именем пользователя и паролем.

Кроме того, он имеет возможности удаленного выполнения кода, что позволяет злоумышленнику выполнять любые системные команды на зараженном сервере. Для предотвращения перехвата или подмены коммуникаций бэкдор использует функцию анти-повтора. Логи несанкционированных подключений скрываются путем перехвата функции логирования. Основная нагрузка бэкдора активируется только один раз во время сессии предварительной аутентификации клиента, когда выполняются проверки аутентификации на основе RSA. Бэкдор также включает функции для обхода аутентификации SSH и выполнения команд через вызов функции system.

Таким образом, бэкдор XZ представляет собой сложную угрозу с множеством уникальных особенностей, таких как встраивание информации о публичном ключе в бинарный код и тщательная подготовка операции, включающая длительную кампанию социальной инженерии.

По ряду из перечисленных CVE проведена значительная работа, включая мониторинг казахстанского сегмента Интернета, выявление уязвимостей и оповещение владельцев уязвимых объектов информатизации. В рамках проводимых мероприятий обеспечивается оперативное информирование и помощь в устранении уязвимостей. Кроме того, Бюллетени с детальной информацией о выявленных уязвимостях регулярно публикуются для ГО РК, МИО, квазигосударственного сектора, КВОИКИ, БВУ РК, а также для ОЦИБ и ОтЦИБ.

Смотреть «Бюллетени» на CERT.GOV.KZ

Все материалы размещаются на веб-платформе информационного взаимодействия НКЦИБ, что позволяет организациям своевременно реагировать на возникающие угрозы.

9. **Методы и тактики атак:** что нового в арсенале киберпреступников?

В 2024 году киберпреступники в Казахстане продолжили совершенствовать свои методы и тактики, используя новые инструменты и подходы для обхода традиционных мер защиты.

Угрозы стали более изощренными: акцент сместился на точечные атаки, основанные на социальной инженерии, эксплуатации уязвимостей в ПО и применении сложных техник уклонения от обнаружения. Эта эволюция кибератак отражает глобальные тренды, но при этом учитывает локальные особенности, создавая новые вызовы для специалистов по киберзащите, подчеркивая необходимость внедрения адаптивных и проактивных мер противодействия.

Использование общедоступных приложений

ATT&CK техника: T1190, тактика: TA0001 *(первичный доступ)* - эксплуатация уязвимостей в приложениях организации, доступных из Интернета. Наиболее частыми целями являются веб-серверы, серверы Exchange, базы данных и точки доступа VPN. Злоумышленники также активно ищут и эксплуатируют публично доступные панели управления ИТ-инфраструктурой, включая SSH-серверы и SNMP.

Фишинг

В 2024 году киберпреступники довели до совершенства методы социальной инженерии, делая фишинг более сложным для обнаружения. **ATT&CK техника:** T1566, **тактика:** TA0001 *(первичный доступ)* – это рассылка сообщений по электронной почте, SMS или через мессенджеры. Цель таких атак – обман сотрудников для получения учетных данных, загрузки вредоносного ПО или выполнения других действий, которые открывают злоумышленникам доступ к корпоративным системам. Атаки становятся все более персонализированными, часто используют поддельные веб-сайты и адаптируются под локальные особенности, что требует более проактивных подходов к защите.

Действительные учетные записи, скомпрометированные злоумышленниками

Техника ATT&CK: T1078, тактика: TA0001, TA0003, TA0004, TA0005 *(первоначальный доступ, настойчивость, повышение привилегий, уклонение от защиты)*. Использование действительных учетных записей, скомпрометированных с использованием социальной инженерии, фишинга или вредоносного ПО, стало одной из ключевых тактик киберпреступников. Получив доступ к легитимным учетным данным, злоумышленники могут проникать в сеть организации, закрепляться в инфраструктуре, повышать привилегии для расширения контроля и обходить системы безопасности. Такая тактика затрудняет обнаружение атаки, так как действия атакующих маскируются под обычную активность сотрудников, что требует усиленного мониторинга и внедрения строгих политик управления доступом.

ATT&CK техника: T1110, тактика: TA0006

(доступ с использованием учетных данных)

Злоумышленники активно используют метод подбора паролей для получения несанкционированного доступа к учетным записям, пытаясь угадать правильные комбинации через массовые попытки. В некоторых случаях они применяют известные хэши паролей или используют распространенные пароли в целях ускорения процесса. Также широко используется техника распыления, когда однотипные пароли проверяются на множестве аккаунтов, что позволяет атакующим найти те, где используются легко угадываемые пароли. Это подчеркивает необходимость применения сложных паролей и внедрения дополнительных мер безопасности, таких как ограничение количества попыток входа.

Программное обеспечение-вымогатель, MITRE ATT&CK: T1486 - Data Encrypted for Impact

ПО-вымогатель продолжает оставаться одной из главных угроз, часто являясь «визитной карточкой» после первичной компрометации сети. Злоумышленники развертывают ПО-вымогатель для шифрования критичных данных и требуют выкуп за их восстановление. Расцвет программ-вымогателей как услуги *(RaaS)* снизил порог входа для киберпреступников, увеличив частоту атак. Организациям следует сосредоточиться на надёжных стратегиях резервного копирования, сегментации сети и регулярных аудиторских проверках безопасности для смягчения рисков программ-вымогателей.

Использование LOLBins *(Living Off the Land Binaries)*, ATT&CK техника: T1218, тактика: TA0005 *(уклонение от защиты)*

Злоумышленники часто используют легитимные системные утилиты, уже присутствующие на устройствах, для выполнения вредоносных действий. Эти инструменты, называемые LOLBins, позволяют обходить системы обнаружения, не требуя загрузки внешнего вредоносного ПО. В 2024 году злоумышленники активнее используют такие файлы для эксплуатации уязвимостей и установки постоянного присутствия. Это усложняет обнаружение атак, так как используется уже доступное ПО, например, PowerShell, командный процессор и WMI.

Фишинг как услуга *(PHaaS)*

Появление платформ PHaaS значительно упростило проведение фишинговых атак. Такие сервисы предоставляют готовые шаблоны и инструменты для создания фишинговых страниц, что приводит к росту числа атак на организации и частных лиц. Например, платформа Sniper Dz предложила бесплатные фиш-киты, способствуя созданию около 140 000 фишинговых сайтов в 2024 году.

Кибербезопасность — это постоянный процесс, а не одноразовая мера

Постоянное отслеживание новых векторов атак, внедрение надежных стратегий обнаружения и реагирования, а также развитие культуры осведомленности о безопасности в вашей организации помогут существенно снизить риск стать жертвой кибератак.

Не забывайте, что даже самые сложные системы защиты могут быть взломаны. **Наличие четко разработанного плана реагирования** на инциденты обеспечивает быструю и эффективную реакцию, минимизируя ущерб, восстанавливая критически важные системы и обеспечивая непрерывность бизнеса.

10. **Технологические новшества (Bug Bounty):** прорывы года в ИБ

Bug Bounty программы для государственных систем в 2024 году продолжают становиться неотъемлемой частью стратегии кибербезопасности в различных странах.

Государства активно развивают и внедряют программы, предназначенные для выявления и устранения уязвимостей в государственных информационных системах, сотрудничая с независимыми исследователями и хакерами для обеспечения высокого уровня безопасности.

В 2024 году «Hack the Pentagon» *(Bug Bounty программа Министерства обороны США)* продолжает работать и расширяться. В рамках этой программы исследователи безопасности выявляют уязвимости в веб-приложениях и других компонентах инфраструктуры Пентагона. США развивают «Hack the Army» и другие подобные инициативы для вооруженных сил, федеральных агентств и ведомств. Программы проводят на платформах, таких как «HackerOne» и «Bugcrowd», участвуют в них только сертифицированные исследователи.

Великобритания, Эстония, Канада, Франция, Австралия проводят программы Bug Bounty через платформы «HackerOne» и «Bugcrowd», которые обеспечивают строгое соблюдение безопасности и конфиденциальности.

В 2024 году Великобритания продолжает разрабатывать и внедрять Bug Bounty программы для различных государственных ведомств. Одна из таких инициатив «Government Cyber Security Programme», направленная на использование исследовательских сообществ для поиска уязвимостей в государственных сервисах.

С ноября 2023 года Минцифры Российской Федерации проводит второй этап программ Bug bounty. 16 тысяч специалистов ищут уязвимости на Госуслугах, Единой системе идентификации и аутентификации, Единой биометрической системе, Платформе обратной связи, Системе межведомственного электронного взаимодействия, Национальной системе управления данными и других государственных системах. Согласно промежуточным итогам второго этапа, обнаружено около 100 уязвимостей в 10 системах. Большинство из них с низкой степенью критичности. Специалисты проверяют только внешний периметр систем и не имеют доступа к внутренним данным, а системы мониторинга контролируют работу багхантеров, поэтому найденные уязвимости нельзя использовать для взлома.

Участие в этих программах позволяет государствам выявлять и устранять уязвимости в своих информационных системах, повышать уровень доверия граждан к цифровым государственным сервисам и строить более безопасные и устойчивые киберструктуры.

Технологические новшества в Bug Bounty программах в 2024 году отражают продолжающееся развитие и адаптацию этой практики к новейшим вызовам в области кибербезопасности. Новые технологии, улучшенные процессы и повышенные стандарты безопасности позволяют улучшать эффективность этих программ и обеспечивать более высокую степень защиты для государственных и частных организаций. Рассмотрим ключевые технологические новшества и тренды в Bug Bounty в 2024 году.

Использование искусственного интеллекта (ИИ) и машинного обучения

ИИ и машинное обучение становятся важными инструментами для повышения эффективности Bug Bounty программ и имеют определенные преимущества.

- **Автоматизация процесса анализа отчетов:**

системы на основе ИИ могут автоматически классифицировать и анализировать отчеты о найденных уязвимостях, выделяя наиболее критичные. Это позволяет значительно ускорить процесс оценки уязвимостей и их устранения.

- **Прогнозирование уязвимостей:**

Машинное обучение позволяет предсказать, какие уязвимости могут возникнуть в будущем, анализируя исторические данные и паттерны. Это дает возможность предварительно тестировать системы и предотвращать потенциальные угрозы еще до их появления.

- **Обработка больших данных:**

ИИ помогает эффективно обрабатывать огромное количество отчетов об уязвимостях, поступающих от участников Bug Bounty программ. Это позволяет снижать нагрузку на команду безопасности и ускорять решение проблем.

Интеграция с платформами управления уязвимостями *(Vulnerability Management Platforms)*

2024 год принес развитие интеграции Bug Bounty с различными платформами управления уязвимостями (VMP), такими как «Tenable», «Qualys», «Rapid7», и «Acunetix».

- Взаимодействие между Bug Bounty программами и платформами управления уязвимостями позволяет автоматически передавать найденные уязвимости в систему для дальнейшего анализа, оценки рисков и устранения.
- Интеграция таких платформ с системами Bug Bounty позволяет организациям получать полную картину текущих уязвимостей в их инфраструктуре и быстро реагировать на угрозы.

Становятся популярными многоуровневые Bug Bounty программы, где тестирование безопасности охватывает не только веб-приложения, но и дополнительные слои инфраструктуры, такие как:

- IoT (Интернет вещей): из-за быстрого роста числа подключенных устройств Bug Bounty программы начинают охватывать уязвимости в IoT устройствах, таких как умные дома, камеры видеонаблюдения и другие элементы умных городов.
- Блокчейн и криптовалюты: в связи с ростом популярности блокчейн-технологий и криптовалют Bug Bounty программы начинают работать с протоколами и приложениями на базе блокчейна, включая криптовалютные биржи и DeFi платформы.
- API-тестирование: с развитием микросервисной архитектуры и API-first подхода фокус Bug Bounty программ также смещается в сторону безопасности API, чтобы избежать утечек данных и атак, таких как SQL-инъекции и манипуляции с запросами.

Блокчейн и смарт-контракты в Bug Bounty

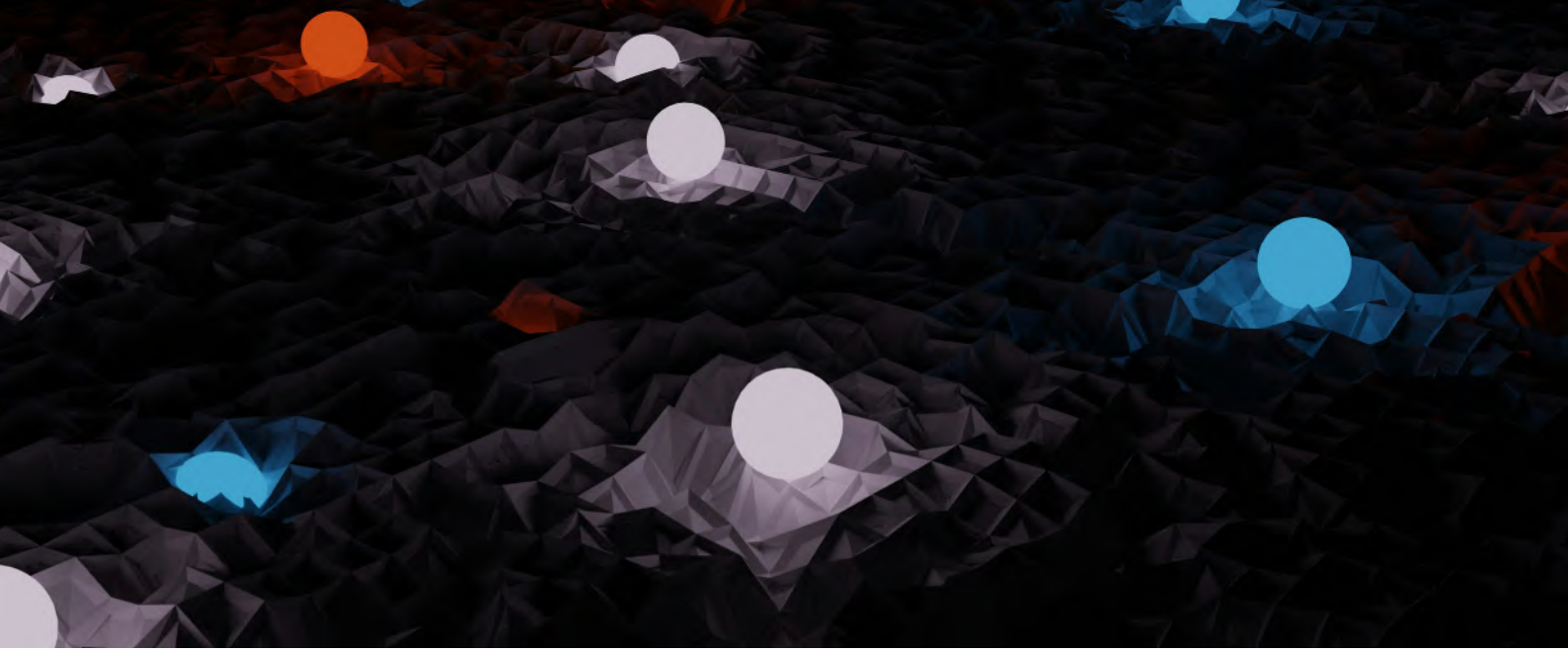
С ростом популярности блокчейна и децентрализованных финансов (DeFi) Bug Bounty программы становятся более интегрированными с этой технологией:

- Тестирование смарт-контрактов: с развитием DeFi и токенизированных активов в блокчейне смарт-контракты стали частой целью Bug Bounty программ. Ошибки в смарт-контрактах могут приводить к потере миллионов долларов. Платформы, такие как «HackerOne» и «Immunefi», начинают предлагать специализированные Bug Bounty программы для смарт-контрактов.
- Проверка безопасности протоколов: в рамках Bug Bounty исследований уделяется внимание новым блокчейн-протоколам и их уязвимостям, особенно в контексте совместимости с другими системами и масштабируемости.

Поддержка и защита от угроз социальной инженерии

Социальная инженерия остается одной из наиболее опасных угроз для безопасности организаций. Bug Bounty программы начинают включать компоненты, направленные на проверку устойчивости системы к таким атакам, как фишинг и инсайдерские угрозы.

Гибридные подходы, объединение открытых и закрытых Bug Bounty программ.



Упрощение взаимодействия с исследователями через новые инструменты и интерфейсы:

- Интерфейсы для автоматической подачи отчетов: новые платформы и инструменты позволяют исследователям легко подавать отчеты о найденных уязвимостях с автоматическим формированием деталей о проблемах, что значительно ускоряет процесс.
- Шифрование отчетов и конфиденциальности: для повышения безопасности внедряются системы автоматического шифрования отчетов и данных о найденных уязвимостях, чтобы гарантировать защиту конфиденциальной информации.

Интеграция с DevOps и CI/CD процессами

С развитием DevOps и CI/CD (непрерывной интеграции и поставки) Bug Bounty программы интегрируются с этими процессами для обеспечения безопасности на всех этапах разработки.

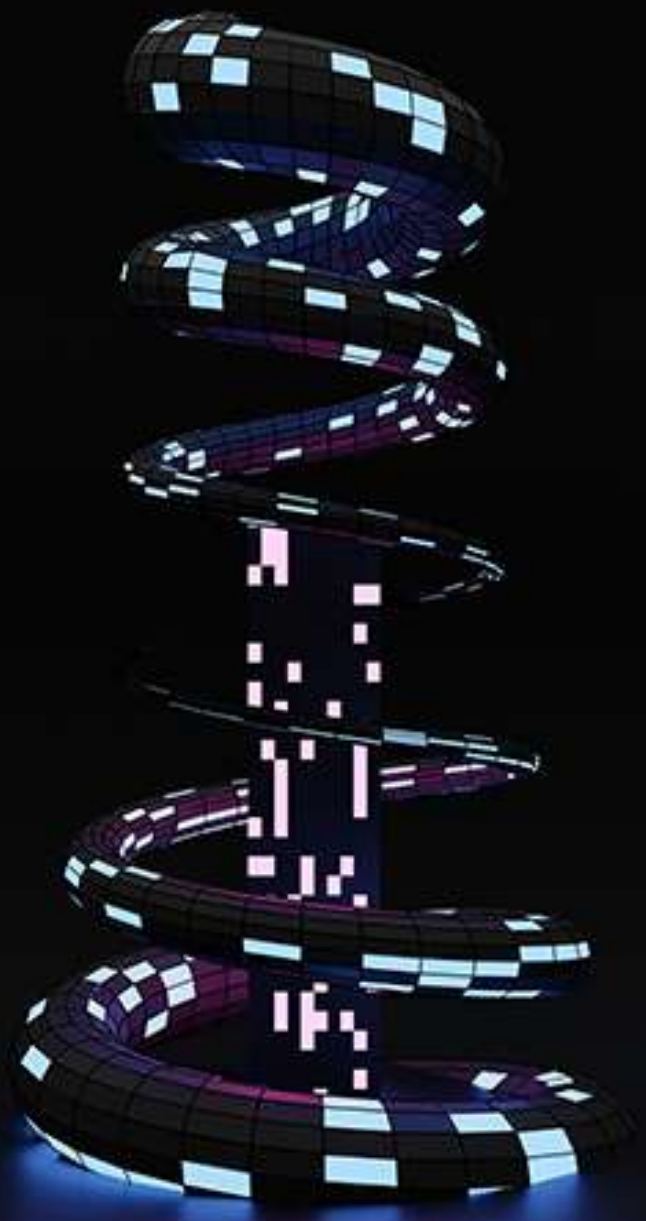
- Внедрение принципов «Security-as-Code» помогает интегрировать безопасность в процессы разработки на более ранних этапах. Программы Bug Bounty становятся неотъемлемой частью CI/CD цепочек, автоматизируя процесс выявления уязвимостей еще до их появления в производственной среде.
- Разработчики могут автоматически запускать тесты на уязвимости в реальном времени, непосредственно в процессе разработки и тестирования программного обеспечения.

Использование новых платформ и технологий

2024 год приносит развитие новых платформ для проведения Bug Bounty программ, таких как «GitHub Security Lab», которые фокусируются на открытых исходных кодах, и обеспечения их безопасности.

Эти платформы позволяют разработчикам и исследователям взаимодействовать напрямую, выявлять уязвимости в коде и улучшать общую безопасность.

11. **Инструменты защиты и рекомендации:** как противостоять современным угрозам?



В современном цифровом мире, где технологии становятся неотъемлемой частью бизнеса, государственных институтов и личной жизни, угрозы информационной безопасности приобретают всё большую сложность и масштаб. От ранних вирусов и червей до современных угроз, основанных на искусственном интеллекте, кибератаки сегодня используют широкий спектр методов, включая эксплуатацию технических уязвимостей и человеческий фактор. Для защиты от этих угроз необходимы не только передовые технологии, но и грамотное управление рисками, обучение сотрудников и проактивный подход к безопасности.

Современные инструменты защиты

Эффективная защита от угроз информационной безопасности требует внедрения комплексных решений, которые могут справляться с многогранными атаками. Рассмотрим наиболее популярные технологии и их особенности.

XDR *(Extended Detection and Response)*

расширенное обнаружение и реагирование — это решение нового поколения, объединяющее возможности антивирусов, систем EDR *(Endpoint Detection and Response)*, SIEM *(Security Information and Event Management)* и сетевых анализаторов. Основное преимущество XDR заключается в интеграции различных источников данных, что позволяет:

- Обнаруживать атаки на уровне конечных устройств, сети и облачной инфраструктуры;
- Ускорять процесс анализа инцидентов за счёт корреляции событий;
- Реагировать на угрозы в реальном времени, минимизируя последствия.

Например, XDR-системы могут автоматически изолировать заражённые устройства, предотвращая распространение вредоносного ПО. Они также способны выявлять сложные угрозы, такие как APT *(Advanced Persistent Threats)*, за счёт анализа поведенческих аномалий.

NGFW *(Next-Generation Firewalls):* **Межсетевые экраны нового поколения**

представляют собой эволюцию традиционных фаерволов. Их ключевые особенности включают:

- Глубокую инспекцию пакетов *(DPI)*, позволяющую анализировать содержимое трафика;
- Фильтрацию приложений и контроль доступа на уровне пользователей;
- Интеграцию с системами предотвращения вторжений *(IPS)*.

NGFW обеспечивают защиту от целевых атак, таких как эксплуатация уязвимостей в веб-приложениях или использование вредоносного трафика. Например, они могут блокировать SQL-инъекции или межсайтовый скриптинг *(XSS)*, предотвращая компрометацию серверов.

DLP *(Data Loss Prevention)*: Системы предотвращения утечек данных

- это технологии, которые защищают конфиденциальную информацию от утечек. DLP-решения отслеживают перемещение данных внутри и за пределы организации, анализируют содержимое файлов и сообщений, а также блокируют:

- Передачу данных через небезопасные каналы *(например, USB-накопители);*
- Отправку корпоративной информации через личные email-аккаунты;
- Загрузку конфиденциальных файлов в публичные облачные хранилища.

SIEM *(Security Information and Event Management)* **и SOAR** *(Security Orchestration, Automation and Response)*

помогают централизованно управлять событиями безопасности. SIEM-системы собирают логи с различных устройств, анализируют их в реальном времени и выявляют угрозы на основе корреляции данных. SOAR добавляет возможность автоматизации реагирования на инциденты, что:

- Ускоряет устранение угроз;
- Снижает нагрузку на специалистов по безопасности;
- Улучшает документирование процессов для аудита.

Рекомендации для повышения устойчивости:

наряду с внедрением технологий, важно следовать стратегическим рекомендациям для обеспечения комплексной безопасности. Ниже представлены ключевые меры:

Принцип «нулевого доверия» *(Zero Trust)*

- этот подход предполагает, что никакие пользователи, устройства или системы не заслуживают доверия по умолчанию, даже если они находятся внутри корпоративной сети. Реализация Zero Trust включает:

- Строгую аутентификацию и авторизацию для всех действий;
- Сегментирование сети для ограничения горизонтального перемещения атакующих;
- Постоянный мониторинг активности пользователей и устройств.

Многофакторная аутентификация *(MFA)*

- использование двух или более факторов для подтверждения личности снижает риск компрометации учётных записей. MFA должна быть обязательной для доступа к критическим системам и сервисам.

Регулярное обновление программного обеспечения

- патч-менеджмент играет ключевую роль в предотвращении атак, основанных на эксплуатации известных уязвимостей. Регулярное обновление операционных систем, приложений и оборудования - залог минимизации рисков.

Сегментация сети

- разделение корпоративной сети на изолированные сегменты затрудняет распространение угроз. Например, IoT-устройства должны быть изолированы от основной корпоративной инфраструктуры.

Резервное копирование данных

- создание регулярных резервных копий критически важных данных помогает восстановить системы после атак вымогателей *(Ransomware)* и других инцидентов. Важно хранить резервные копии в изолированных средах.

Обучение сотрудников

- человеческий фактор остаётся одной из главных причин успешных кибератак. Регулярное обучение персонала основам кибербезопасности, включая распознавание фишинговых писем и применение принципов кибергигиены, снижает вероятность инцидентов.

Киберучения и тестирование на проникновение

- проведение регулярных учений помогает оценить готовность сотрудников и технологий к отражению атак. Тестирование на проникновение выявляет слабые места в защите до того, как ими воспользуются злоумышленники.

Аудит безопасности на основе CIS Benchmarks

- использование рекомендаций Центра Интернет-безопасности *(CIS Benchmarks)* позволяет:

- Оптимизировать настройки систем;
- Устранить потенциальные уязвимости;
- Соответствовать международным стандартам безопасности.

Киберполигоны: развитие технологий и реалистичное моделирование инфраструктур

Современные киберполигоны представляют собой инновационные платформы, созданные для имитации сложных сценариев кибератак в условиях, максимально приближенных к реальной инфраструктуре. Они предоставляют уникальную возможность моделировать работу критически важных объектов информационной инфраструктуры (КВОИКИ) и АСУ ТП. Такой подход позволяет исследовать уязвимости, тестировать защитные меры и повышать уровень подготовки специалистов.

Особое внимание уделяется созданию сценариев, которые отражают актуальные угрозы для промышленности, энергетики, транспорта и других секторов, критически зависящих от ИТ-систем. Киберполигоны позволяют:

- Проигрывать атаки на SCADA-системы, PLC-контроллеры и другие ключевые элементы инфраструктуры;
- Проверять эффективность средств защиты, таких как системы обнаружения вторжений, сегментация сети и резервирование данных;
- Подготавливать специалистов к реагированию на реальные инциденты, включая устранение последствий и восстановление работоспособности систем.

Спрос на киберполигоны растёт, что стимулирует их развитие. Будущее этого направления связано с интеграцией технологий искусственного интеллекта, которые помогут автоматизировать генерацию сложных сценариев атак и анализировать результаты. Развитие облачных технологий также способствует созданию доступных и масштабируемых виртуальных полигонов, что расширяет их применение в обучении и тестировании на национальном и международном уровнях.

Необходимость внедрения SOAR и искусственного интеллекта в процессы реагирования на инциденты

Современные кибератаки требуют от организаций оперативного и комплексного реагирования. В этой связи использование систем SOAR становится неотъемлемой частью эффективного управления безопасностью. SOAR позволяет автоматизировать рутинные процессы, такие как сбор информации, анализ инцидентов и первичное реагирование. Это помогает значительно снизить нагрузку на специалистов, минимизировать время реакции и повысить точность обработки угроз. Например, SOAR-системы могут автоматически изолировать скомпрометированные устройства, заблокировать подозрительные IP-адреса и уведомить ответственных лиц о развитии ситуации.

Помимо автоматизации, SOAR способствует стандартизации процессов реагирования. Это особенно важно для крупных организаций, где необходимо согласовывать действия между разными отделами и филиалами. Внедрение таких систем не только повышает оперативность, но и ***обеспечивает*** прозрачность и документирование всех этапов реагирования, что упрощает аудит и дальнейшую оптимизацию.

Роль искусственного интеллекта в реагировании на угрозы

ИИ уже активно используется для анализа больших объёмов данных, что делает его незаменимым инструментом в борьбе с кибератаками. Современные системы на базе ИИ способны в реальном времени выявлять аномалии в поведении пользователей и устройств, предсказывать возможные сценарии атак и рекомендовать наиболее эффективные меры реагирования. Например, алгоритмы машинного обучения позволяют быстрее и точнее определять угрозы, такие как продвинутые атаки типа APT, которые сложно обнаружить традиционными методами.
Кроме того, ИИ способен адаптироваться к новым видам угроз, что особенно актуально в условиях стремительного появления новых техник взлома. Интеграция ИИ в SOAR-системы позволяет создать гибкую и высокоэффективную инфраструктуру защиты, способную реагировать на вызовы будущего.

Контроль ИИ: необходимость аттестации и проверки моделей

С развитием технологий ИИ всё больше задач в сфере кибербезопасности автоматизируются, однако это создаёт новые риски. Используемые модели ИИ сами могут стать мишенью для атак, например, путём внедрения вредоносных данных в обучающие выборки или эксплуатации уязвимостей в алгоритмах. В этой связи особую важность приобретает аттестация и проверка ИИ-моделей. Контроль ИИ должен включать:

- Оценку надёжности и точности алгоритмов, чтобы предотвратить ошибки, которые могут привести к пропуску угроз.
- Тестирование на устойчивость к различным типам атак, таким как эксплуатация уязвимостей или манипуляции входными данными.
- Регулярный аудит процессов работы ИИ, чтобы исключить риски, связанные с некорректной обработкой данных или предвзятостью алгоритмов.

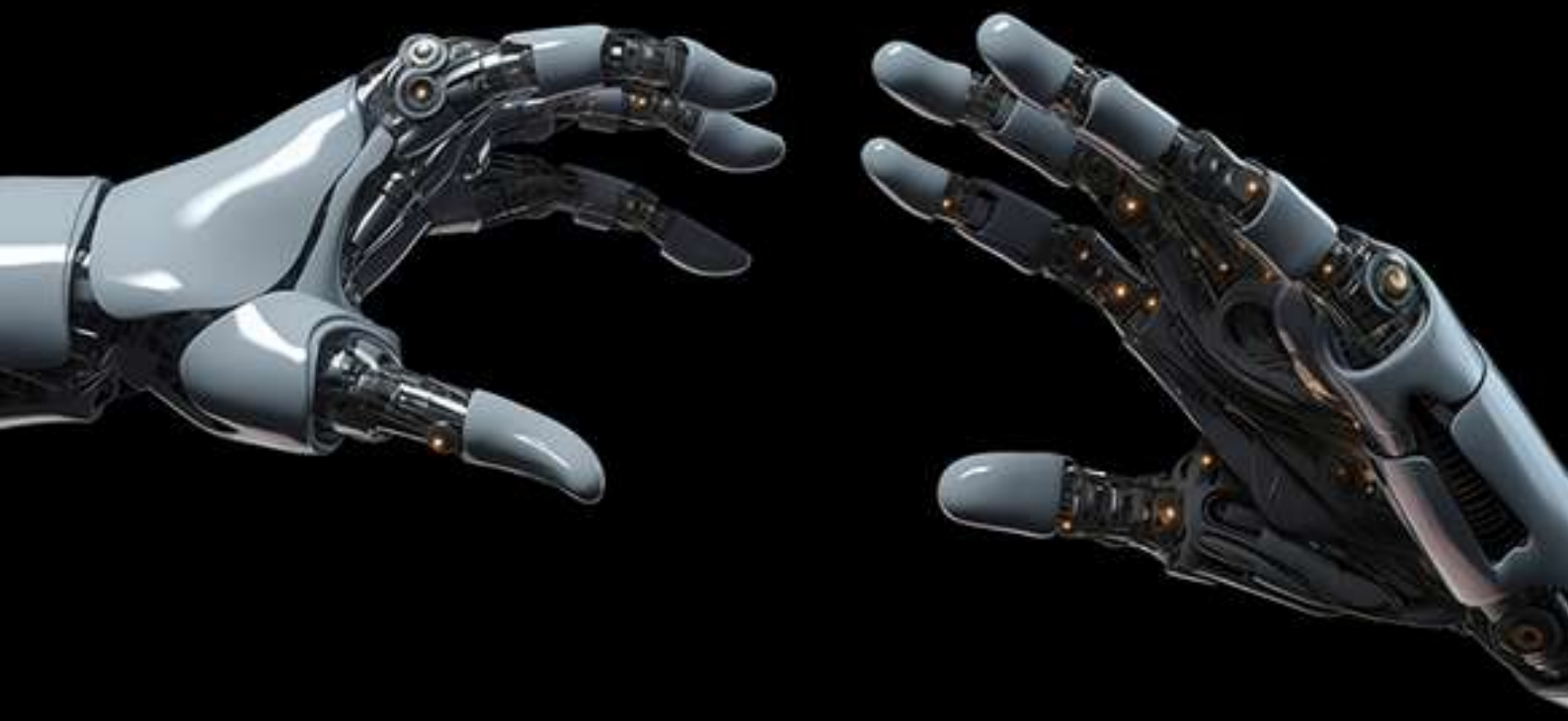
На уровне государственных и корпоративных стандартов следует разработать регламенты, обеспечивающие безопасность применения ИИ. Это включает обязательную сертификацию моделей и регулярное тестирование их на соответствие установленным требованиям. Такой подход позволит не только повысить доверие к технологиям, но и минимизировать риски, связанные с их использованием.

Будущее ИИ и SOAR в кибербезопасности

- сочетание возможностей SOAR и ИИ открывает новые горизонты для проактивной защиты. Например, в ближайшие годы ожидается интеграция технологий генеративного ИИ для моделирования потенциальных атак и разработки стратегий их предотвращения. Это позволит организациям не только реагировать на инциденты, но и предугадывать их, что кардинально меняет подход к обеспечению безопасности.

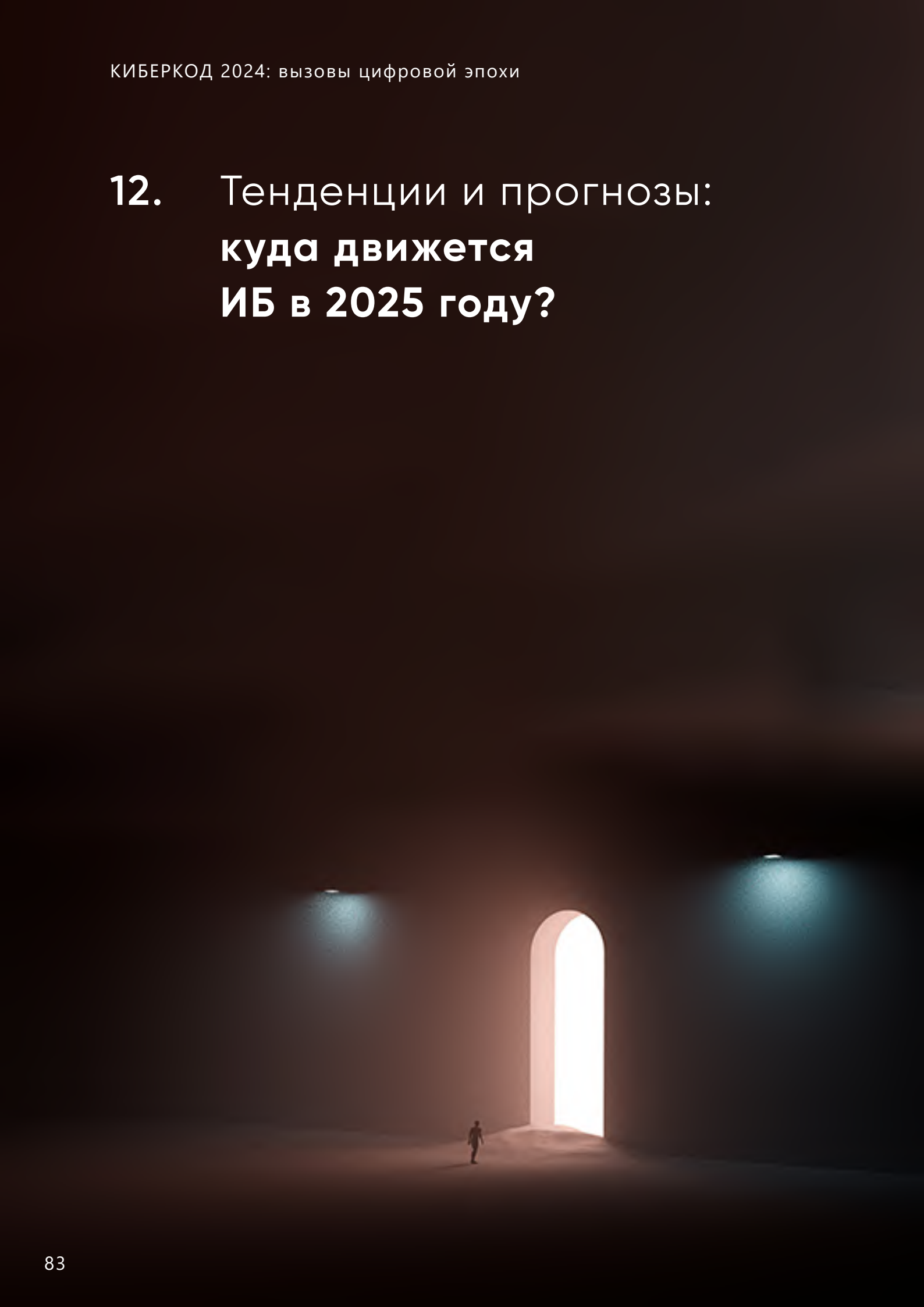
Противостояние современным угрозам информационной безопасности требует от организаций не только внедрения передовых технологий, но и системного подхода к управлению безопасностью.

Регулярное обновление инфраструктуры, проактивное обучение сотрудников и использование многоуровневых решений позволяют существенно снизить риски и повысить устойчивость к атакам.



В условиях стремительного роста числа угроз проактивная защита становится не просто приоритетом, а необходимостью для успешного ведения бизнеса.

12. Тенденции и прогнозы: **куда движется ИБ в 2025 году?**



АТАКИ НА ГОСУДАРСТВЕННЫЕ И КОРПОРАТИВНЫЕ СИСТЕМЫ

За последние два года в Казахстане наблюдался рост числа кибератак на различные секторы экономики.

Среди наиболее пострадавших можно выделить:

- СМИ - 19% от общего числа атак, с ноября 2023 года независимые казахстанские СМИ подверглись серии DDoS-атак, затронувших как минимум девять изданий и аккаунты нескольких журналистов в мессенджерах и социальных сетях *(источник: PT Security);*
- государственные учреждения - 12% атак, приведших к утечке конфиденциальной информации и нарушению работы информационных систем;
- финансовые организации - 12% атак, в числе которых кража данных и денежных средств;
- социальная инженерия - в январе 2024 года в Казахстане было зафиксировано почти 600 фишинговых атак *(источник: Khabar).* Фишинг и целевые атаки через электронную почту и мессенджеры набирают популярность, что увеличивает риск компрометации пользователей.

Одними из наиболее распространённых и разрушительных видов кибератак, направленных на нарушение работы сетей, веб-сайтов и онлайн-сервисов, остаются **DDoS-атаки (Distributed Denial of Service).**

Если ранее основной целью таких атак была перегрузка серверов и сетей с целью временного отключения ресурса, то сегодня киберпреступники используют их как инструмент шантажа, отвлечения внимания от других атак или как часть геополитических конфликтов.

В 2024 году они составили 64% от общего количества атак для государственного сектора и 17% - для финансового.

Современные тенденции, такие как развитие Интернета вещей *(IoT)*, облачных технологий и усложнение цифровой инфраструктуры способствуют повышению доступности инструментов для DDoS-атак. Эти атаки стали более масштабными, сложными и целенаправленными, поражая не только бизнес, но и критически важную инфраструктуру: государственные порталы, медицинские системы и финансовые учреждения.

Прогноз на 2025 год

- Прогнозируется дальнейший рост числа атак, в том числе DDoS-атак на государственные и корпоративные информационные системы, что связано с активной цифровизацией и увеличением числа точек доступа к критически важным системам.
- Все более распространенными будут становиться атаки на цепочки поставок. Отсутствие в законодательстве Казахстана требований к уровню обеспечения информационной безопасности поставщиков услуг создает условия для распространения вредоносного ПО среди клиентов и партнеров, на которых распространяются Единые требования, утвержденные постановлением Правительства РК.
- Расширение сферы использования цифровых валют и финансовых технологий создаёт дополнительные точки уязвимости, что повышает привлекательность финансового сектора для злоумышленников.
- Ожидается использование более изощренных методов социальной инженерии и рост числа мошеннических схем, например, таких как «мамонт», когда злоумышленники используют подмену реальных данных для получения финансовой выгоды.

МОБИЛЬНЫЕ УГРОЗЫ

Приоритетной целью для злоумышленников становятся мобильные устройства, особенно в финансовом секторе.

- Банковские приложения: увеличивается количество атак на мобильные банковские приложения, направленных на хищение пользовательских данных и финансовых средств. В качестве защиты всё чаще внедряются биометрические системы идентификации, однако отсутствие стандартов снижает их надёжность и устойчивость к обходу. Перспективным решением является применение технологий подтверждения «живого разума» *(liveness detection),* требующих динамических действий, таких как моргание или поворот головы. Такие системы затрудняют использование подделок и повышают уровень защиты мобильных приложений.
- Android-устройства: во втором полугодии 2024 года наиболее распространенной угрозой кражи данных стала вредоносная программа Formbook *(источник: ESET)*.

Прогноз на 2025 год

- Рост числа атак на мобильные платформы электронных платежей и банковские приложения.
- Увеличение числа вредоносных программ, направленных на взлом Android.

УГРОЗЫ ДЛЯ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Мишенью для кибератак становится **критическая инфраструктура,** включая энергетику и транспорт. Так, за прошедший год были реализованы целевые атаки на энергетический сектор, силовые структуры, государственные органы, в том числе и на операторов связи. Уязвимости в системах автоматизированного управления технологическими процессами приводят к сбоям в работе критической инфраструктуры:

- **Энергетика:** атаки на энергетические системы могут вызвать перебои в поставке энергии, что негативно скажется на экономике и безопасности.
- **Транспорт:** кибератаки на транспортные системы могут нарушить логистику и передвижение, создавая хаос и провоцируя экономические потери.

Многочисленные IoT-устройства, включая промышленные, характеризуются слабой защитой, что делает их привлекательными целями для злоумышленников. Например, ботнет Mirai, использующий уязвимости в IoT-устройствах для создания массовых атак, был задействован в 2024 году для организации DDoS-атаки на телекоммуникационную компанию.

Прогноз на 2025 год

- Прогнозируется усиление атак посредством IoT-устройства в промышленности и энергетике. Кроме того, ожидается рост числа атак на IoT-устройства как точки входа в корпоративные сети.
- С большой долей вероятности можно ожидать значительного роста активности APT-группировок, специализирующихся на кибершпионаже, роста количества целевых атак на энергетический сектор.

ДЕЗИНФОРМАЦИЯ И АТАКИ НА СОЦИАЛЬНЫЕ СЕТИ

- Распространение фейков: использование фейковых аккаунтов, deepfake-контента и поддельных новостей для манипуляции общественным мнением.
- Социальные сети как инструмент: злоумышленники используют соцсети для фишинга и распространения вредоносных ссылок.

Прогноз на 2025 год

- Автоматизация дезинформации: использование ИИ для проведения масштабных кампаний по распространению ложной информации.
- Усиление атак на крупные платформы для саботажа работы или кражи данных.

ЭВОЛЮЦИЯ КИБЕРУГРОЗ

В последнее время наблюдается устойчивый тренд на усложнение методов атак. Злоумышленники активно используют скрытные техники, включая невидимые бэкдоры, облачные платформы для управления атаками и социальную инженерию, что позволяет им оставаться незамеченными длительное время и делает их обнаружение стандартными средствами защиты крайне сложным. Эти группы целенаправленно атакуют государственные структуры, спецслужбы, критически важные системы и поставщиков услуг, чтобы получить доступ к конфиденциальным данным. Киберугрозы усложняются за счёт внедрения современных технологий, что требует более продвинутых методов противодействия:

- Искусственный интеллект и машинное обучение: злоумышленники применяют ИИ для создания адаптивного вредоносного ПО.
- Deepfake: используются для распространения дезинформации и манипуляции общественным мнением.
- Уязвимости нулевого дня: остаются серьезной проблемой, позволяя атакующим проникать в системы до выпуска обновлений безопасности.

Прогноз на 2025 год

- Активизация использования ИИ в кибератаках потребует разработки новых методов защиты.
- Растущую угрозу будут представлять технологии Deepfake, требуя развития средств для их обнаружения.

УТЕЧКА ДАННЫХ

- Финансовый сектор: в 2024 году одна из казахстанских финансовых организаций потеряла данные 50 тысяч клиентов из-за уязвимости в мобильном приложении.
- Государственные системы: утечка конфиденциальной информации из госструктур несет угрозу национальной безопасности. В сентябре этого года эксперты по кибербезопасности отмечали, что Казахстан оказался на втором месте среди стран СНГ по числу упоминаний мошенниками в DarkNet. А данные граждан продаются по цене от 100$ до 50 000$.

Прогноз на 2025 год

- Рост атак через API: уязвимости в приложениях станут ключевым каналом для утечки данных.
- Целевые атаки на крупные организации с большими массивами персональных данных.

ТЕХНОЛОГИЧЕСКИЕ УГРОЗЫ

Языки программирования, такие как C++ и Go, активно используются для создания сложных вредоносных программ, включая руткиты и эксплойты для драйверов.

ПРОГНОЗ НА 2025 ГОД

- Активное использование уязвимостей драйверов для обхода систем защиты.
- Разработка более сложных атак с использованием этих языков программирования.

МЕРЫ ПРОТИВОДЕЙСТВИЯ

- Развитие киберобразования: повышение осведомленности о современных киберугрозах.
- Передовые технологии защиты: использование ИИ и машинного обучения для обнаружения угроз в режиме реального времени.
- Международное сотрудничество: участие в глобальных инициативах и обмен опытом.
- Безопасность IoT: стандарты для подключенных устройств.
- Контроль цепочек поставок: обязательные аудиты безопасности поставщиков, а также законодательное закрепление обязательства для поставщиков услуг субъектам государственного и квазигосударственного секторов выполнять требования по обеспечению информационной безопасности в соответствии с утвержденными нормами.

ЗАКЛЮЧЕНИЕ

Прогнозы на 2025 год указывают на увеличение числа и сложности киберугроз, что диктует для Казахстана необходимость:

- Развития национальной инфраструктуры кибербезопасности.
- Повышения квалификации специалистов в области информационной безопасности.
- Внедрения передовых технологий для обнаружения и предотвращения атак.
- Усиления законодательных и регуляторных механизмов защиты критической инфраструктуры.

Комплексный подход к кибербезопасности станет ключевым фактором устойчивости к современным вызовам и позволит повысить эффективность защиты национальных интересов Казахстана.

13. **Киберучения-2024:** проверка готовности и повышение культуры ИБ

В рамках реализации национальной стратегии по укреплению цифровой безопасности и развитию информационной культуры КНБ РК, КИБ МЦРИАП РК и АО «ГТС» активно внедряют подходы для повышения уровня защищенности государственных информационных систем и ресурсов, а также осведомленности организаций о современных угрозах информационной безопасности.

Одним из ключевых мероприятий в этом направлении стало формирование Реестра киберучений для казахстанских организаций, включая государственные органы Республики Казахстан, местные исполнительные органы и организации квазигосударственного сектора.

ОСНОВНАЯ ЦЕЛЬ ПРОВЕДЕНИЯ КИБЕРУЧЕНИЙ В 2024 ГОДУ

Популяризация мер «кибергигиены» и развитие культуры информационной безопасности в государственных структурах и организациях. Для достижения этой цели мероприятия были организованы в два этапа.

1

На первом этапе участники проходили проверку на подверженность «фишингу». Это включало практическое тестирование с использованием имитации фишинговых атак: рассылка электронных писем со ссылками на поддельные ресурсы или вредоносные файлы. Результаты позволяли оценить, насколько сотрудники организаций способны распознать и предотвратить такие угрозы.

2

На втором этапе реализовывался теоретический обучающий курс. Лекции охватывали ключевые темы.

- Основные аспекты информационной безопасности.
- Анализ основных векторов атак на Казахстан.
- Актуальные вопросы и практики в области ИБ.
- Разбор проведенных киберучений и рекомендации по улучшению защиты.

Итогами стали **36 проведенных практических киберучений и 41 лекция,** направленные на повышение осведомленности сотрудников, укрепление знаний в области ИБ и развитие общей киберкультуры в организациях.

КИБЕРУЧЕНИЯ НА КИБЕРПОЛИГОНЕ ДЛЯ ОЦИБ:

19-20 августа 2024 года по инициативе АО «ГТС» были проведены киберучения для ОЦИБ.

Учения стали важным мероприятием для оценки и улучшения навыков участников в области киберзащиты с имитацией реальных сценариев атак и защиты информационных систем.

Участники были разделены на две группы: Red Team *(команды атакующих)* и Blue Team *(команды защитников)* и каждая группа работала на одной из двух инфраструктур - «IT-компания» и «Министерство образования».

Основной задачей было создание условий для практической тренировки в условиях, приближенных к реальной угрозе кибератак.

Учения проводились на двух инфраструктурах, каждая из которых была спроектирована с учетом различных угроз и уязвимостей. Так, для проверки навыков команд защиты, каждая из инфраструктур включала в себя сегментированную сеть с зонами DMZ и Corp, а также имела заранее заложенные уязвимости различных типов, таких как Web и Local Privilege Escalation *(LPE)*. В рамках этих условий команды Red Team должны были попытаться проникнуть в инфраструктуру и получить доступ к чувствительным данным, таким как персональная информация пользователей и финансовые документы, в то время как команды Blue Team должны были своевременно фиксировать и реагировать на инциденты безопасности, передавая отчет в НКЦИБ в течение 15 минут с момента подтверждения инцидента.

Каждой команде предоставлялись необходимые инструменты и ресурсы для работы. Для команд Red Team это были VPN-конфигурации, а для Blue Team - ограниченный доступ к SIEM-системам *(Arkime и Splunk)*, которые использовались для мониторинга и анализа инцидентов. Вся информация о ходе учений передавалась через платформу MISP, что обеспечивало эффективную коммуникацию между участниками и организаторами. Техническую поддержку участников осуществляли через Telegram-боты, а результаты работы команд можно было наблюдать на онлайн-дашборде.

Процесс оценки выполнения заданий был очень строгим. Команды Red Team получали баллы за успешное выполнение рисков, причем баллы для каждой последующей командой, реализовавшей тот же риск, снижались. Например, первая команда, успешно реализовавшая риск, получала 100% от возможных баллов, а каждая последующая команда на 5% меньше. Аналогичная система оценки была применена и для Blue Team: баллы присуждались за успешное обнаружение инцидента и оперативную передачу информации.

Важно, что все отчеты оценивались на соответствие заранее установленным требованиям и публиковались в реальном времени на специализированном интернет-ресурсе НКЦИБ.

Кроме того, были определены конкретные риски для каждой из инфраструктур. Например, для «IT-компании» это могла быть утечка персональных данных клиентов, компрометация серверов Active Directory или внедрение в процесс разработки банковского процессинга. Для «Министерства образования» среди рисков были утечка конфиденциальных данных о студентах или компрометация серверов MSSQL. Важно отметить, что все эти риски требовали от команд высокой квалификации и готовности оперативно действовать в условиях, когда время на принятие решений было ограничено.

Учения прошли успешно и по итогам двух дней были определены победители. АО «Кселл» и ТОО «Digital Qalqan» продемонстрировали высокие результаты как в защите, так и в атаке. Также отличные результаты показали команды из ТОО «MSSP.GL» и ТОО «QazCloud», получившие высокие оценки за выполнение своих задач.

Отзывы участников также свидетельствовали о высокой эффективности учений, которые позволили не только повысить уровень киберзащиты, но и значительно улучшить понимание процесса реагирования на инциденты в реальных условиях.

Такие мероприятия становятся важным элементом для повышения квалификации специалистов в области информационной безопасности, а также помогают организациям лучше подготовиться к потенциальным угрозам, тестируя их способности противостоять современным угрозам информационной безопасности.

14. Заключение и выводы: основные итоги года

2024 год стал значимым этапом в развитии кибербезопасности, продемонстрировав как новые угрозы и вызовы, так и прогресс в создании современных методов защиты

Мировые и локальные события продемонстрировали, что угрозы информационной безопасности продолжают усложняться и расширяться, угрожая критической инфраструктуре, государственным учреждениям и бизнес-сектору.

Казахстан столкнулся с рядом серьезных инцидентов, которые выявили уязвимые места в защите цифровых систем, одновременно предоставив важный опыт и осознание значимости комплексного подхода к обеспечению информационной безопасности. Развитие кибергигиены и программ повышения осведомленности пользователей казахстанского сегмента Интернета продолжает играть ключевую роль в предотвращении угроз информационной безопасности, где человеческий фактор остается одним из самых значимых.

Международная арена в 2024 году вновь продемонстрировала, что киберпреступники не просто совершенствуют тактики атак, но и активно осваивают новые технологии, включая возможности искусственного интеллекта и эксплойты для уязвимостей автоматизированных систем управления, что подчеркивает необходимость постоянного мониторинга, развития адаптивных стратегий защиты и укрепления международного сотрудничества для сдерживания глобальных угроз.

Кроме того, немаловажным аспектом стало усиление **законодательного регулирования,** позволяющего создать условия для эффективной защиты данных и критически важных объектов информационно-коммуникационной инфраструктуры. Внедрение **передовых технологических решений,** таких как Bug Bounty программы, позволило не только выявить уязвимости в информационных системах, но и укрепить позиции организаций в борьбе с атаками нового поколения.

Однако ключевой вывод остается неизменным: **Кибербезопасность – это не разовая мера, а процесс, требующий постоянного контроля и внедрения инноваций.**

Только совместными усилиями государства, бизнеса, экспертного сообщества и граждан можно выстроить надежный щит против растущих цифровых угроз.

На пороге 2025 года мы видим не только новые вызовы, но и новые возможности.

Укрепление защиты информационной безопасности, развитие культуры безопасности и активное взаимодействие между всеми участниками цифровой экосистемы позволят создать более надежное и устойчивое цифровое будущее.

14. Заключение и выводы: основные итоги года

Ссылки на источники:

1. Концепция развития АО «Государственная техническая служба» на 2025-2027 годы
2. Лаборатория Касперского
3. Positive Technologies
4. Gartner
5. Shadowserver Foundation
6. Check Point Research
7. OpenAI
8. Microsoft
9. Juniper Networks
10. Apache
11. CVE-2024-36401: https://nvd.nist.gov/vuln/detail/CVE-2024-36401 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-36401
12. CVE-2024-21683: https://nvd.nist.gov/vuln/detail/CVE-2024-21683 https://www.monitorapp.com/2024-08-vulnerability-report-atlassian-confluence-remote-code-execution-cve-2024-21683/
13. CVE-2024-21762: https://www.rapid7.com/blog/post/2024/02/12/etr-critical-fortinet-fortios-cve-2024-21762-exploited/ https://nvd.nist.gov/vuln/detail/CVE-2024-21762
14. CVE-2024-24919: https://support.checkpoint.com/results/sk/sk182336
15. https://nvd.nist.gov/vuln/detail/CVE-2024-24919
16. CVE-2024-21378: https://www.netspi.com/blog/technical-blog/red-team-operations/microsoft-outlook-remote-code-execution-cve-2024-21378/ https://nvd.nist.gov/vuln/detail/CVE-2024-21378
17. https://global.ptsecurity.com/analytics
18. MITRE ATT&CK Framework: https://attack.mitre.org/
19. https://redcanary.com/blog/blog/lolbins-abuse/
20. https://www.kaspersky.com/blog/top-mitre-attack-techniques-2023-stats-and-protection-tips/51231/
21. https://blog.usecure.io/top-10-cybersecurity-threats
22. https://community.trustcloud.ai/article/cyber-security-tools-discover-the-top-18-must-know-tools-of-2024/
23. https://www.sisainfosec.com/blogs/top-10-cybersecurity-tools-you-should-be-aware-of-in-2024/
24. https://cybermagazine.com/top10/top-10-biggest-cyber-threats
25. Check Point - «2025 Cyber Security Predictions: The Rise of AI-Driven Attacks, Quantum Threats, and Social Media Exploitation.» https://blog.checkpoint.com/security/2025-cyber-security-predictions-the-rise-of-ai-driven-attacks-quantum-threats-and-social-media-exploitation/
26. Cloud Security by Google - «Cybersecurity Forecast 2025» (PDF) https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025
27. Forbes – «Six Cybersecurity Trends Heating Up in 2025» https://www.forbes.com/councils/forbestechcouncil/2024/11/22/six-cybersecurity-trends-heating-up-in-2025/
28. Fortinet - «Threat Predictions for 2025: Get Ready for Bigger, Bolder Attacks» (PDF) https://www.fortinet.com/blog/threat-research/threat-predictions-for-2025-get-ready-for-bigger-bolder-attacks
29. Kaspersky Security Bulletin – «Advanced Threat Predictions for 2025» https://securelist.com/ksb-apt-predictions-2025/114582/
30. Gartner-«Global Information Security Spending to Grow 15% in 2025» https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025
31. Palo Alto Networks - «2025 Predictions: How One Year Will Redefine the Cybersecurity Industry» https://www.paloaltonetworks.com/blog/2024/11/2025-predictions-redefine-the-cybersecurity-industry/
32. Trend Micro-«The Artificial Future: Trend Micro Security Predictions for 2025» https://www.trendmicro.com/vinfo/us/security/news/security-predictions/the-artificial-future-trend-micro-security-predictions-for-2025
33. Darktrace-«Preparing for 2025: Top AI and Cybersecurity Predictions» - https://darktrace.com/blog/ai-and-cybersecurity-predictions-for-2025
34. Splunk – «Ransomware & Extortionware in 2025: Stats & Trends» https://www.splunk.com/en_us/blog/learn/ransomware-trends.html
35. Palo Alto Networks - «The Convergence of Cybersecurity and AI: 7 Game-Changing Predictions for 2025» https://www.paloaltonetworks.com/why-paloaltonetworks/cyber-predictions
36. https://huntsmansecurity.com/blog/cyber-security-predictions-for-2025/
37. https://blog.checkpoint.com/security/2025-cyber-security-predictions-the-rise-of-ai-driven-attacks-quantum-threats-and-social-media-exploitation/
38. https://www.itweek.ru/security/article/detail.php?ID=231153
39. https://expertnw.com/ekspertnoe-mnenie/prognozy-ot-kiberdeda-na-2025-god/