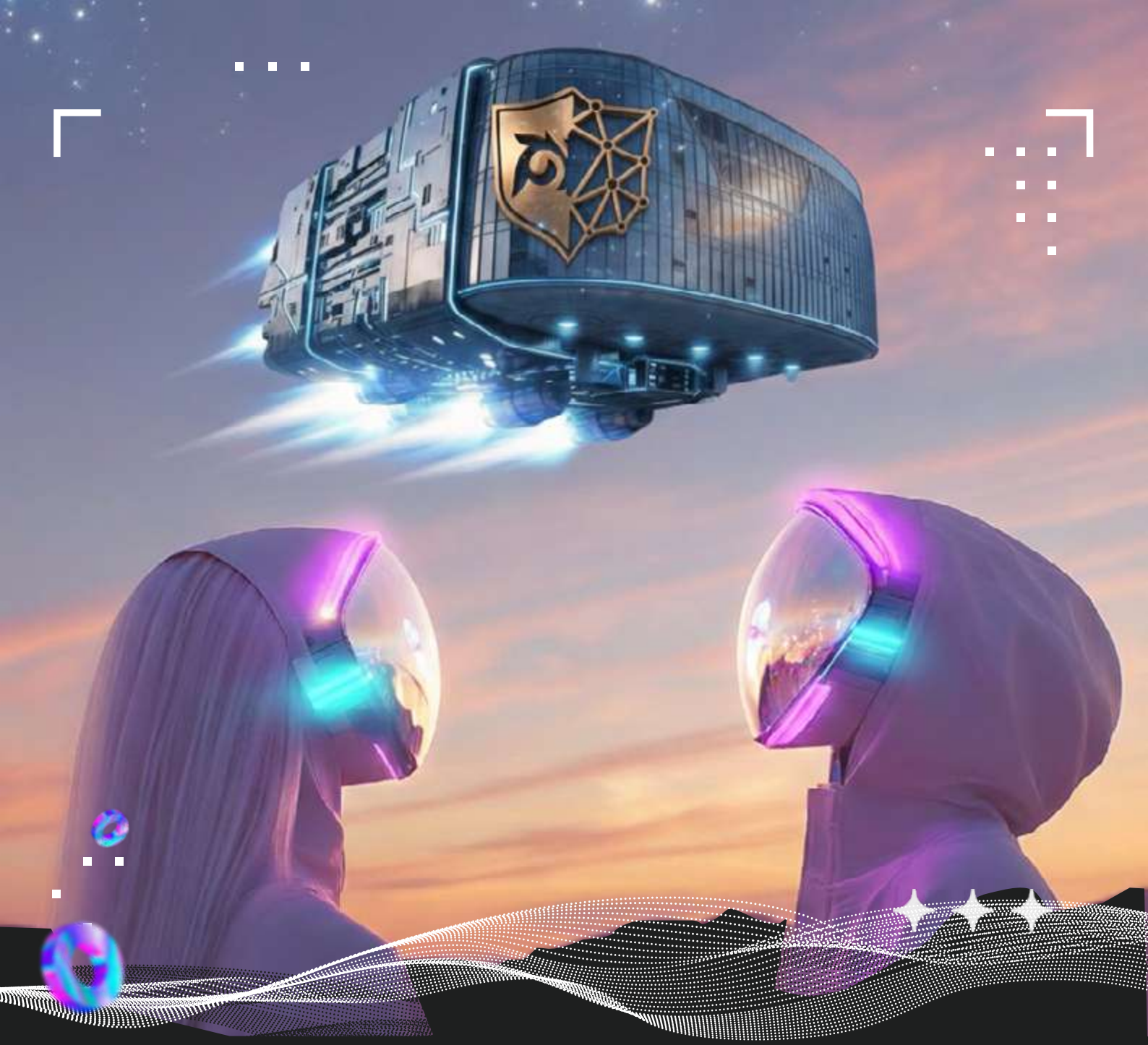


Кибердайджест

Киберкод 2025: вызовы цифровой эпохи

Акционерное общество «Государственная техническая служба» (АО «ГТС»)

Уважаемые читатели!

Пользуясь возможностью выхода в свет очередного выпуска Кибердайджеста, хотелось бы осветить некоторые актуальные проблемы обеспечения информационной безопасности, поделиться отдельными реальными кейсами, с которыми сталкивается АО «ГТС» в ходе обеспечения кибербезопасности страны.

Как вам известно, АО «ГТС» является ключевым звеном в обеспечении кибербезопасности Казахстана. Мы защищаем цифровое пространство страны, координируем действия государственных органов и организаций по противодействию киберугрозам.

Угрозы информационной безопасности с каждым днём становятся всё более сложными и изощрёнными, что требует от нас применения новых эффективных подходов. Однако благодаря этому мы становимся сильнее и мудрее: не только внедряем инструменты, позволяющие отражать атаки, но и, анализируя угрозы, принимаем упреждающие меры.

В последнее время довольно часто выявляются инциденты, сопряженные с утечкой персональных данных, несущие, в том числе, серьезные репутационные риски для бизнеса, что вызывает необходимость внедрения многоуровневых систем защиты, а также повышения ответственности организаций за сохранность персональных данных. Такого рода инциденты - напоминание о важности цифровой безопасности и внимательного отношения к своим данным в онлайн-пространстве.

В рамках компетенции, определенной Законом РК «Об информатизации», **АО «ГТС» проводит испытания объектов информатизации, информационно-коммуникационной платформы «электронного правительства» и платформенных программных продуктов.** Ввод в промышленную эксплуатацию объекта информатизации осуществляется при условии наличия протоколов с положительными результатами испытаний на соответствие требованиям информационной безопасности.

Дальнейшее развитие объектов информатизации осуществляется по усмотрению собственника или владельца. При этом, отсутствие контроля за изменениями после проведения испытаний может привести к серьезным негативным последствиям: появлению уязвимостей, утечке данных, несанкционированному доступу, сбоям в работе системы или ее компрометации.

Так, ранее публиковалась информация о массовой утечке данных пациентов медицинской системы Damumed, в результате которой медицинская информация сотен тысяч пациентов сети клиник Damumed попала в сеть. Инцидент был официально подтвержден постом соответствующего содержания на официальной странице Facebook медицинской компании.

Экстраординарность данной ситуации в немалой степени обусловлена тем фактом, что ранее мобильное приложение для пациентов Damumed получило отрицательный результат по итогам испытаний.

Известно, что в Казахстане многие государственные и банковские услуги предоставляются с применением биометрической идентификации. В ходе работы мы столкнулись с проблемами в реализации этого инструмента организациями, которые используют его для предоставления своих услуг.

Например, одна из телекоммуникационных компаний Казахстана ввела биометрическую идентификацию для регистрации SIM-карт. Казалось бы, применение технологии должно повышать безопасность. Но разработчиками была допущена ошибка: после успешного сканирования лица клиента результат кэшировался (сохранялся) на 15 минут.

То есть, в течение этого времени можно было зарегистрировать новый номер, используя данные другого пользователя. Злоумышленники нашли эту уязвимость, эксплуатировали ее, обходя биометрическую проверку, и регистрировали телефонные номера на чужие ИИН.

Этот случай демонстрирует, насколько важно учитывать все возможные риски при внедрении новых технологий: от создания стандартов защиты биометрических данных до работы с прецедентами, связанными с их утечкой.

Как уже упоминалось выше, технологии стремительно развиваются, спектр угроз информационной безопасности постоянно расширяется, что требует от нас своевременного реагирования и постоянной трансформации. Принимая во внимание складывающиеся реалии, мы запустили деятельность Центра исследования вредоносного кода - нашего форпоста в борьбе с новыми типами атак, где каждый инцидент становится уроком, а каждая угроза - возможностью для совершенствования.

Мы стремимся не просто реагировать на инциденты, но и прогнозировать их, разрабатывая меры, которые сделают нашу цифровую инфраструктуру неприступной.

С учетом выявляемых тенденций АО «ГТС» принимает организационно-практические меры, позволяющие соответствовать мировым стандартам и быть конкурентоспособным игроком, в том числе и на международной арене.

В частности, нами создан Центр компетенций, который в перспективе видится ядром инноваций и подготовки специалистов нового поколения, способных противостоять угрозам завтрашнего дня. Так, планируется получить для него статус авторизованного центра подготовки специалистов по программам ведущих мировых ИТ-производителей. Это позволит нам не только развивать внутренний потенциал, но и предлагать обучение на международном уровне, готовя кадры, способные решать самые сложные задачи в области обеспечения кибербезопасности.

АО «ГТС» активно развивает сотрудничество с зарубежными партнёрами, что позволяет нам своевременно получать актуальную информацию о новых угрозах и оперативно на них реагировать. Такое взаимодействие является одним из немаловажных элементов обеспечения надежной защиты наших цифровых ресурсов. Мы уверены, что совместная работа позволит значительно повысить уровень защиты наших цифровых активов и создать более безопасную цифровую среду для всех граждан.
Без ложной скромности можно отметить, что и казахстанские решения и услуги в сфере информационной безопасности вызывают значительный интерес на международной арене.

Мы готовы совместно развивать потенциал специалистов через программы обучения и киберучения в рамках нашего Центра компетенций, организуя тренинги и практические занятия для повышения уровня подготовки команд к современным киберугрозам. Наш опыт в области построения безопасных хранилищ больших данных и внедрения инструментов искусственного интеллекта может быть полезен для оптимизации бизнес-процессов и обеспечения высокой степени защиты данных.

Нельзя обойти вниманием такую стремительно развивающуюся область, как искусственный интеллект, который, с одной стороны, открывает перед нами невероятные возможности, трансформируя различные сферы нашей жизни. С другой - он становится серьезным инструментом в руках злоумышленников.

Надо признать, что скорость современных атак и экспоненциальный рост объёмов данных, которые необходимо анализировать, превышают возможности человеческого анализа. Постоянно эволюционирующие угрозы, такие как полиморфные вредоносные программы и целенаправленные фишинговые атаки, требуют более продвинутых и адаптивных решений. Именно поэтому использование искусственного интеллекта (ИИ) в обеспечении кибербезопасности перестало быть просто опцией и стало насущной необходимостью.

ИИ становится стратегической основой для перехода от реактивной к проактивной кибер-защите, обеспечивая устойчивость цифрового общества.

В этой связи, я полагаю, для всех представляет интерес практический опыт использования возможностей ИИ не только в информатизации, но и в вопросах информационной безопасности, включая защиту самих ИИ-моделей от атак злоумышленников.

В заключение хочу отметить, что поскольку мы живем в эпоху стремительной цифровой трансформации, одна из основных наших целей и задач - сделать так, чтобы эта трансформация была безопасной для каждого гражданина, каждой компании и каждого государственного органа.

С уважением,

Председатель Правления АО «ГТС»

А. Жүнісбек

Содержание

Исполнительное резюме

Исполнительное резюме содержит ключевые выводы и тенденции годового кибердайджеста. В нём обобщены результаты анализа киберинцидентов, ландшафта угроз, реальных атак, а также влияние ИИ на уровень киберрисков. Раздел предназначен для быстрого ознакомления с текущей киберобстановкой и приоритетами киберустойчивости по итогам 2025 года.

Ключевые тезисы

1. **Киберриски в 2025 году перешли в стратегическую плоскость**

   Киберинциденты напрямую влияют на устойчивость управления, непрерывность оказания услуг и доверие граждан и клиентов. Масштаб ущерба определяется не только атаками, но и готовностью организаций к обнаружению и восстановлению.

2. **Формальное соответствие требованиям больше не снижает риски**

   Усиление регулирования и ответственности за утечки данных повышает финансовые и репутационные потери при инцидентах. Комплаенс без инженерной реализации мер ИБ не обеспечивает защиту и не снижает вероятность штрафов и простоев.

3. **Основные потери связаны с утечками данных и шифровальщиками**

   Инциденты приводят к прямым финансовым убыткам, затратам на восстановление, юридическим последствиям и репутационному ущербу. Ключевыми факторами риска остаются скомпрометированные учётные записи, инсайдеры и слабый контроль резервного копирования.

4. **Искусственный интеллект усиливает как атаки, так и защиту**

   ИИ снижает порог входа для злоумышленников и повышает точность атак, одновременно становясь необходимым инструментом для автоматизации SOC, снижения операционных затрат и ускорения реагирования на инциденты.

5. **Критическая инфраструктура и АСУ ТП требуют проактивной защиты**

   Для КВОИКИ ключевыми являются сегментация IT/OT, непрерывный мониторинг и Threat Hunting. Отказ от реактивной модели снижает риск остановки процессов, аварий и системных последствий для экономики и безопасности

Ландшафт угроз в цифрах

Статистика демонстрирует доминирование фишинга, DDoS-атак, ботнет-активности и вредоносного ПО. При этом массовые атаки всё чаще используются как фон для целенаправленных операций. Ботнеты нового поколения, персонализированный фишинг указывают на системные проблемы кибергигиены и управления конечными устройствами.

Профиль угрозы: разборы инцидентов

Типовой сценарий успешных атак включает компрометацию учётных записей, закрепление с использованием легитимных инструментов и длительное скрытое присутствие. Масштаб ущерба от шифровальщиков и утечек данных обусловлен в первую очередь организационными пробелами: устаревшими системами, отсутствием мониторинга, слабым контролем резервного копирования и инсайдерскими рисками.

ИИ и кибербезопасность

ИИ стал фактором эскалации угроз, снизив порог входа для злоумышленников и повысив точность атак. Одновременно он превращается в обязательный элемент защиты. Классические SOC-модели исчерпали эффективность — без автоматизации, поведенческого анализа и оркестрации реагирования устойчивость становится недостижимой.

Обзор законодательства в сфере обеспечения информационной безопасности Казахстана

Усиление регулирования и ответственности за утечки данных повысило финансовые и репутационные риски. Практика показала, что формальный комплаенс без инженерной реализации мер ИБ не снижает угроз и не обеспечивает устойчивость. Дополнительным ограничивающим фактором стал дефицит квалифицированных кадров.

Коммерческие услуги ГТС и международное сотрудничество

Рост зрелости угроз усилил спрос на практико-ориентированные сервисы: мониторинг, реагирование, Threat Hunting и восстановление после инцидентов. Рынок смещается от разовых внедрений к долгосрочным моделям киберустойчивости и управляемых сервисов безопасности.

Киберустойчивость будущего: проактивная защита и риски критической инфраструктуры

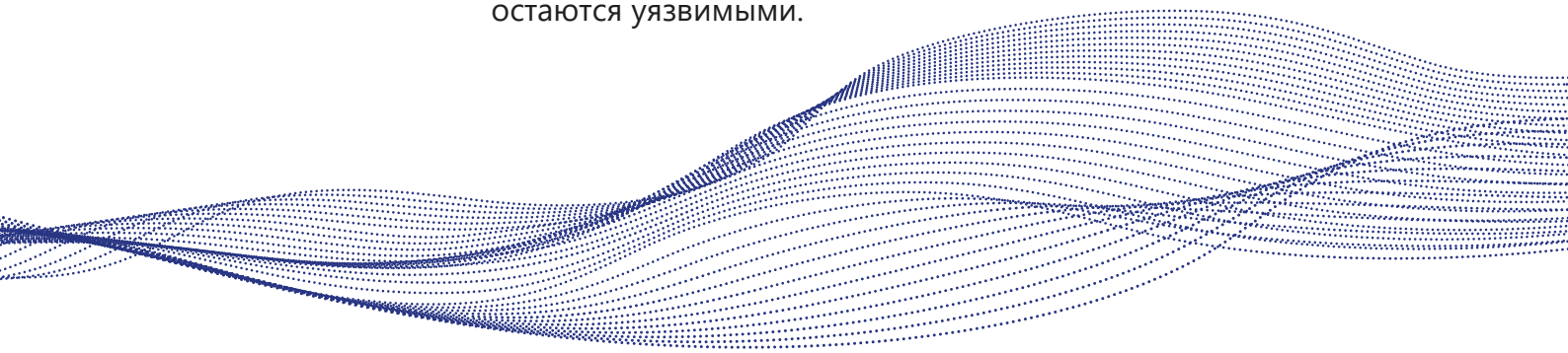
Координационная роль НКЦИБ и развитие отраслевых ОЦИБов становятся ключевыми элементами национальной киберустойчивости. В условиях роста APT-угроз и ИИ-атак приоритет смещается к прогнозированию, совместному обмену данными и превентивным мерам защиты.

АСУ ТП и критическая инфраструктура: защита, которая не может упасть

КВОИКИ и АСУ ТП остаются зоной повышенного риска из-за уязвимостей OT-сред, устаревших систем и ограниченных механизмов защиты. Классического мониторинга недостаточно — переход к Threat Hunting, сегментации IT/OT и непрерывному контролю является необходимым условием предотвращения системных сбоев и аварий.

Прогнозы кибербезопасности

2025 год подтвердил: кибербезопасность — это вопрос архитектуры, процессов и готовности команд. Организации, ограничивающиеся формальным соответствием требованиям, остаются уязвимыми.



Ключевые приоритеты:

- Управление идентификациями и привилегиями;
- Автоматизация SOC и применение ИИ;
- Защита от шифровальщиков и готовность к восстановлению;
- Предотвращение утечек и инсайдерских угроз;
- Безопасное внедрение ИИ;
- Переход от комплаенса к инженерной киберустойчивости.

Ландшафт угроз в цифрах

- Статистика инцидентов информационной безопасности
- Актуальные угрозы ИБ в РК
- Эпоха шифровальщиков: атаки на критические секторы
- Ландшафт угроз: анализ критических уязвимостей и векторы атак
- От реагирования к опережению: итоги года деятельности НКЦИБ

Статистика инцидентов информационной безопасности

ПО СОСТОЯНИЮ НА 2025 ГОД

В период с 1 января по 31 декабря 2025 года

Службой KZ-CERT зафиксировано и отработано свыше **61 067 угроз и инцидентов ИБ** в казахстанском сегменте Интернета.

58
Цепочки атак в ЦГО

Количество выявленных APT-атак

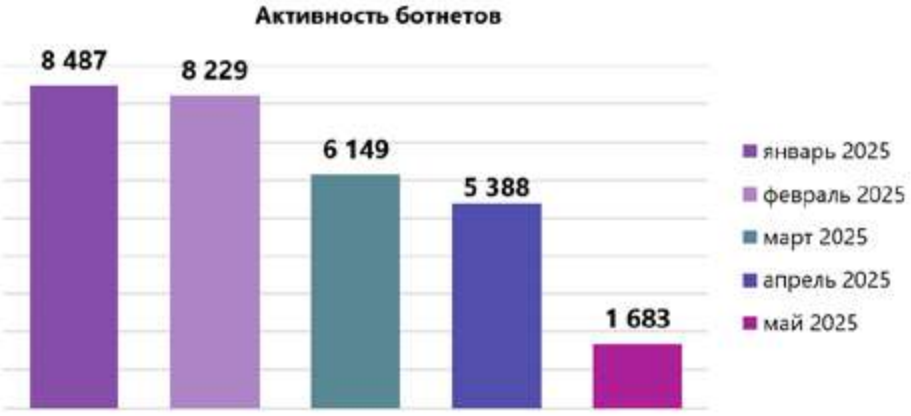
Актуальные угрозы ИБ в РК

Ботнет

В начале текущего года на оборудовании АО «ГТС» были зафиксированы массовые события, связанные с ботнетом Phorpiex – одной из наиболее устойчивых и активных киберугроз на сегодняшний день *(около 90% от общего количества зафиксированных ботнетов)*.

Ботнет

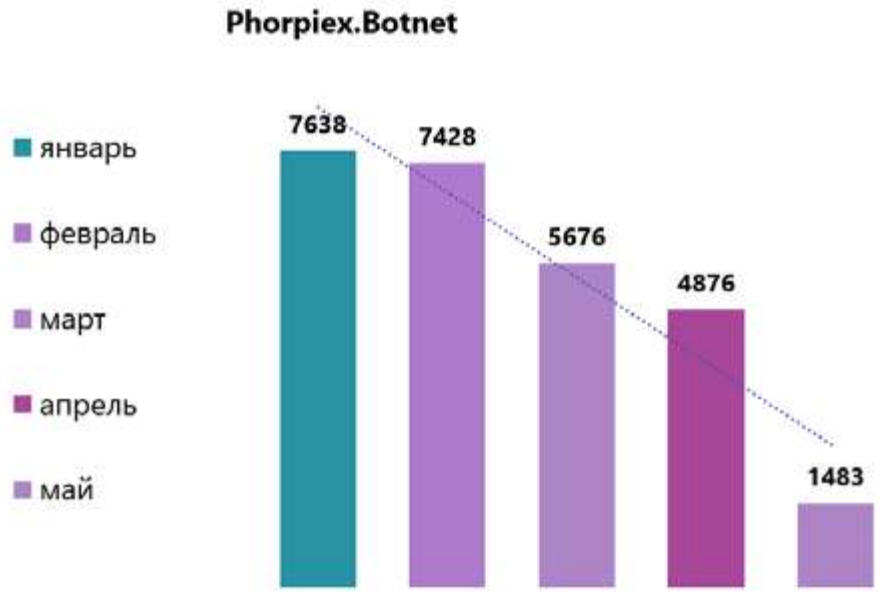
— это сеть заражённых устройств, которыми злоумышленник управляет удалённо для выполнения вредоносных действий.



Данное вредоносное ПО используется для кражи криптовалютных кошельков, рассылки спама, sextortion-атак и распространения программ-вымогателей.

По данным международных и внутренних источников, в деятельности ботнета были обозначены **более тысячи казахстанских IP-адресов,** что указывает на высокую степень его распространённости в национальном сегменте сети.

«Применение P2P-архитектуры позволяет ботнету Twizt функционировать без единого централизованного управляющего сервера»



В ряде организаций государственного сектора **зафиксировано обнаружение вредоносных файлов,** в частности «voldriver.exe», которые относятся к новой вариации ботнета Twizt. Эта модификация представляет собой серьёзную угрозу, поскольку использует **peer-to-peer (P2P) архитектуру.**

Применение P2P-архитектуры позволяет ботнету Twizt **функционировать без единого централизованного управляющего сервера.** Такая децентрализация делает угрозу исключительно стойкой и значительно затрудняет её обнаружение и нейтрализацию.

Сохраняющаяся активность ботнетов в целом обусловлена двумя ключевыми факторами:

- **Компрометация новых объектов информатизации**
- **Постоянное совершенствование** методов и алгоритмов управления заражёнными устройствами

Данная ситуация чётко указывает на **необходимость немедленного усиления мер защиты,** повышения уровня киберграмотности среди сотрудников государственных органов и внедрения дополнительных механизмов мониторинга и оперативного реагирования.

Для эффективного противодействия ботнет-угрозам, таким как Phorpiex и его модификация Twizt, критически важна реализация многоуровневого подхода к защите информационной инфраструктуры.

- **Комплексное обнаружение:**
  Обеспечение покрытия всех сетевых портов и протоколов средствами обнаружения и предотвращения атак (IDS/IPS).
- **Углублённый анализ:**
  Использование поведенческого анализа трафика для выявления аномалий, а также расширение возможностей сигнатурного детектирования за пределы стандартных правил.
- **Внедрение SIEM-систем:**
  Развёртывание систем управления информацией и событиями безопасности (SIEM) для централизованного сбора, анализа и корреляции данных о событиях.
- **Своевременные индикаторы:**
  Оперативное получение и внедрение **индикаторов компрометации (IoC)** от надёжных источников.
- **Сетевая гигиена:**
  Обеспечение сегментации сетей, ограничение маршрутизации для потенциально скомпрометированных узлов и **блокировка обращений к peer-to-peer-сетям,** активно используемым вредоносным ПО.

Для эффективного противодействия... критически важна реализация многоуровневого подхода к защите информационной инфраструктуры.

Особое внимание следует уделить удалённым рабочим местам и рабочим станциям, с которых фиксируются массовые обращения, схожие с признаками заражения.

Эпоха шифровальщиков: Атаки на критические секторы

В первом квартале 2025 года зафиксирован ряд инцидентов, связанных с шифрованием данных в IT-инфраструктуре различных организаций. Анализ показал, что злоумышленники активно используют как **современные вирусы-шифровальщики** (например, Mimic), так и **встроенные средства шифрования** (например, BitLocker).

Обзор резонансных инцидентов

Финансовый сектор: взлом через RDP

В организации финансового сектора 12 января 2025 года были зашифрованы серверы с использованием **BitLocker** в результате взлома инфраструктуры. Дополнительно зафиксирован взлом интернет-ресурса с перенаправлением на сторонний сайт.

Вектор атаки и способствующие факторы:

- **Начальный доступ:**
  Осуществлён через **RDP-доступ** скомпрометированной учётной записи администратора.
- **Использование уязвимостей:**
  Получен доступ к админ-панели сайта, размещённого внутри корпоративной сети, который **не имел актуальных обновлений** и содержал открытую уязвимость в используемой CMS.
- **Усугубляющие факторы:**
  Недостаточный контроль ИБ, наличие устаревших операционных систем (Windows Server 2003/2012, Red Hat Linux 4), **отсутствие мониторинга на базе SIEM** и неструктурированная политика ИБ.

Местный исполнительный орган: компрометация через подрядчика

28 апреля 2025 года в инфраструктуре местного исполнительного органа были зашифрованы многочисленные **виртуальные машины,** включая критически важные сервисы (AD, DHCP, DNS). Вредоносное ПО парализовало работу систем, был получен файл с требованием выкупа. **Резервные копии отсутствовали либо были недоступны.**

Вектор атаки и способствующие факторы:

- **Начальный доступ:**

  Получен через **скомпрометированную учётную запись сотрудника организации,** осуществлявшей сопровождение (вектор удалённого доступа).

- **Использование уязвимостей:**

  Через удалённое подключение RDP проникли на сервер контроллера домена, произвели **очистку журналов событий,** а затем инициировали шифрование.

- **Усугубляющие факторы:**

  Использование **устаревшей и уязвимой версии CMS** на одном из интернет-ресурсов организации.

Сфера образования: политика и контроль

7 февраля 2025 года в организации сферы образования шифрование данных привело к нарушению штатной работы информационных систем.

Ключевые факторы, способствовавшие успеху атаки:

- **Отсутствие политики ИБ:**

  Не была сформирована и внедрена **структурированная политика** информационной безопасности.

- **Сетевая уязвимость:**

  Наличие открытых сетевых портов.

- **Недостаточный контроль:**

  Отсутствие регулярного аудита учётных записей пользователей и администраторов.

- **Проблемы с резервированием:**

  Некорректная организация хранения резервных копий, что существенно осложнило восстановление.

- **Низкая контролируемость трафика:**

  Не все задействованные IP-адреса были подключены к **централизованному шлюзу доступа к сети Интернет.**

«Успешная реализация атак стала возможной благодаря системным пробелам, включая отсутствие сформированной политики информационной безопасности, наличие устаревшего ПО и открытых сетевых портов, а также недостаточный контроль и мониторинг IT-инфраструктуры».

Комплексные выводы по шифровальщикам

Совокупность этих инцидентов наглядно демонстрирует, что к**лючевыми факторами успешности атак шифровальщиков** являются не только изощрённость самого вредоносного ПО, но и **системные пробелы в организации защиты:**

Устаревшие ОС и ПО с открытыми уязвимостями (CMS, RDP)

Слабый или скомпрометированный RDP-доступ администраторов

Отсутствие SIEM-мониторинга и структурированной политики ИБ

Проблемы с резервным копированием и доступом к резервным копиям

«Для предотвращения критически важно внедрение структурированной политики ИБ, регулярное обновление систем, закрытие избыточных сетевых портов и организация надёжного хранения резервных копий, подкреплённая централизованным мониторингом на базе SIEM»

В течение года мониторинг информационного пространства зафиксировал ряд критических уязвимостей, затронувших как инфраструктурные элементы, так и прикладное программное обеспечение.

Ландшафт угроз: Анализ критических уязвимостей и векторы атак

Детальный обзор угроз, обнаруженных в текущем периоде.

1. Сетевая инфраструктура и протоколы шифрования

Проблема устаревшего SSLv2

Масштабный анализ выявил **свыше 130 тыс. устройств** с активным протоколом SSLv2, преимущественно в инфраструктуре операторов связи. Ситуация усугубляется использованием веб-серверов GoAhead и отсутствием обновлений прошивок.

- **Вектор угрозы:**
  Инфраструктура уязвима к атакам классов DROWN, POODLE и CRIME. Это создаёт условия для расшифровки TLS-сессий и компрометации передаваемой информации.
- **Сопутствующие проблемы:**
  Обнаружены ресурсы с полным отсутствием TLS, просроченными или самоподписанными сертификатами, а также некорректным CN (Common Name).
- **Риск:**
  Перехват и расшифровка трафика, атаки «человек посередине» (MitM).

Открытые метрики Prometheus

В казахстанском сегменте Интернета обнаружен 341 сервер Prometheus с открытыми интерфейсами `/metrics` и `/debug` Часть экспортёров функционирует без аутентификации.

- **Риск:**
  Отказ в обслуживании (DoS), раскрытие внутренней архитектуры сети, несанкционированные манипуляции с мониторингом.
- **Рекомендация:**
  Закрытие публичного доступа, внедрение аутентификации и использование VPN для управления.

2. Безопасность веб-ресурсов и CMS

Массовые уязвимости Joomla

На 5022 интернет-ресурсах под управлением CMS Joomla выявлено **свыше 256 тыс. уязвимостей** (175 уникальных CVE).

- **Характер угроз:**
  XSS, SQL-инъекции и возможность выполнения произвольного кода.
- **Риск:**
  Полная компрометация ресурса, подмена контента, хищение баз данных пользователей.

Плагин W3 Total Cache
WordPress

Более 300 ресурсов в доменной зоне .kz используют устаревшую версию плагина W3 Total Cache, подверженную уязвимости **CVE-2024-12365.**

- **Суть:**
  Пользователи с низкими правами (подписчики) могут выполнять привилегированные действия.

Ошибки конфигурации
.git и IDOR

- **Публичная директория .git (CWE-527):**
  Позволяет злоумышленникам выкачать весь репозиторий проекта, включая историю изменений и жестко закодированные пароли/ключи.
- **IDOR (CWE-639):**
  Некорректная проверка прав доступа позволяет изменять параметры запросов и получать доступ к данным чужих аккаунтов.

3. Критические уязвимости корпоративного ПО
High/Critical

Для удобства анализа наиболее опасные уязвимости, выявленные в корпоративных системах, сведены в таблицу:

Система / ПО	CVE / Уязвимость	Суть угрозы и последствия
Microsoft SharePoint	CVE-2025-53770 (ToolShell)	**Критическая.** Удалённое выполнение кода через небезопасную десериализацию. Позволяет украсть MachineKey, подделать токены и атаковать OneDrive/ Exchange/Teams.
WSUS	CVE-2025-59287	**Критическая.** Удалённое выполнение кода с правами SYSTEM неаутентифицированным пользователем. Полный контроль над сервером обновлений.
Kerio Control	CVE-2024-52875	RCE через CRLF-инъекцию. Доступен публичный эксплойт. Риск полного захвата шлюза и проникновения во внутреннюю сеть.
Roundcube Webmail	CVE-2025-49113	Выполнение произвольного PHP-кода через специально сформированное email-сообщение. Угроза компрометации почтовых серверов.
Apache Superset	CVE-2023-27524	Использование дефолтного `SECRET_KEY`. Позволяет злоумышленнику сгенерировать токен админа и захватить управление базами данных.

4. Стратегия минимизации рисков

Для обеспечения устойчивости информационных ресурсов и минимизации рисков эксплуатации описанных уязвимостей необходимо придерживаться комплексного подхода:

- **Управление обновлениями:**
  Обеспечить регулярное обновление всех компонентов (CMS, плагины, FW, средства мониторинга) до актуальных версий.

- **Защита интерфейсов:**
  Отключить или ограничить доступ к отладочным панелям и административным интерфейсам. Использовать VPN и фильтрацию по IP для доступа к критическим сегментам.

- **Криптографическая защита:**
  Отказаться от SSLv2 и устаревших шифров, внедрить обязательный TLS.

- **Аудит и мониторинг:**
  Регулярно проводить тесты на проникновение, анализ конфигураций и сканирование уязвимостей.

- **Активная защита:**
  Внедрение Web Application Firewall (WAF) и систем логирования для своевременного обнаружения атак.

«Выявленный спектр угроз — от массового использования устаревших протоколов шифрования и уязвимых CMS до критических брешей в корпоративных платформах и открытых служебных директорий — указывает на системные пробелы в защите, делающие инфраструктуру уязвимой как для перехвата конфиденциальных данных, так и для полного захвата управления критически важными сервисами».

От реагирования к опережению: **итоги года деятельности НКЦИБ**

Сұлейменов Айдос Жұмагелдіұлы | Руководитель Штаба НКЦИБ

Уважаемые коллеги, партнёры, читатели!

2025 год стал для Казахстана временем серьёзной перегрузки и одновременно заметного взросления. Цифровая повестка в стране расширяется, инфраструктура усложняется, а вместе с ней растёт ответственность тех, кто стоит на рубеже кибербезопасности. В этих условиях Национальный координационный центр информационной безопасности не только сохранил устойчивость, но и продемонстрировал готовность работать на опережение, формируя новые стандарты реагирования и взаимодействия.

Цифровая повестка расширяется, инфраструктура усложняется, а вместе с ней растёт ответственность тех, кто стоит на рубеже кибербезопасности

В течение года зарегистрировано и обработано свыше 63 тысяч событий и инцидентов информационной безопасности. Через веб-платформу MISP направлено более 56 тысяч оповещений. Параллельно был организован устойчивый обмен с зарубежными партнёрами — направлены тысячи уведомлений по угрозам и инцидентам, получены сотни ответных сообщений. Такой масштаб взаимодействия отражает не только интенсивность атак, но и уровень доверия к центру как к национальной точке координации.

Для части инцидентов организовывались выезды мобильной группы с проведением разборов «на месте» и первичного анализа, включая сбор материалов для последующего расследования и выработки рекомендаций. Такой формат взаимодействия между НКЦИБ и организациями Республики Казахстан способствует укреплению доверия и повышению зрелости субъектов мониторинга.

Отдельного внимания заслуживает расследование 14 крупных кейсов высокого уровня критичности. Они включали утечки данных в государственных и коммерческих организациях, дипломатическом представительстве, сервисах для населения и корпоративных системах, эпизоды заражения вирусами-шифровальщиками в финансовых и образовательных учреждениях, а также попытки несанкционированного доступа к государственным ресурсам. По каждому инциденту проводился детальный технический анализ, выстраивалась цепочка атаки, формировались выводы и меры по недопущению повторения.

По каждому инциденту проводился детальный технический анализ и формировались меры по недопущению повторения

Развитие аналитической системы НКЦИБ позволило выявить и подробно изучить сложные сценарии вредоносной активности, включая несанкционированный доступ к инфраструктурам городских сервисных центров, центральных органов государственного управления и отдельных государственных организаций. Анализ артефактов, каналов проникновения и попыток закрепления злоумышленников переводит реагирование из плоскости точечного устранения последствий в область системной работы с угрозами.

Реагирование переходит от «тушения пожаров» к полноценному Threat Hunting

Значимый результат дал мониторинг казахстанского сегмента Интернета. Были выявлены уязвимости более чем на 15 тысячах IP-адресах — от открытых серверов мониторинга и межсетевых экранов до популярных систем управления сайтами и специализированных информационных систем. По результатам мониторинга проводилось информирование владельцев ресурсов и взаимодействие с операторами связи, что позволило снизить риск компрометации значимой части национальной инфраструктуры.

Мониторинг казахстанского сегмента Интернета позволяет снижать риски компрометации критически важной инфраструктуры

Помимо массовых проблем, выявлены уязвимости высокого уровня критичности на 13 информационных ресурсах различного профиля, включая образовательные платформы, сервисы открытых данных, специализированные порталы и мобильное приложение в сфере здравоохранения. Такой подход позволяет видеть картину шире отдельного инцидента и формировать понимание типовых ошибок и архитектурных рисков, характерных для целых отраслей.

Формируется понимание типовых ошибок и архитектурных рисков, характерных для целых отраслей

Методологическая и нормативная работа формирует фундамент долгосрочного развития. Подготовлены предложения по включению услуг мониторинга в нормативные акты, унификации требований к эксплуатации средств защиты и развитию современных подходов к обеспечению информационной безопасности.

Кибербезопасность – это не набор разрозненных мер, а системная функция управления

Отдельное внимание уделялось развитию технической инфраструктуры и технологий. В планы на 2026–2027 годы заложены масштабирование централизованной системы мониторинга, модернизация архитектуры и развитие аналитических инструментов, включая дашборды на основе матрицы MITRE ATT&CK.

Особое значение имеет человеческий капитал. Повышение квалификации сотрудников, участие в киберучениях, технических тренировках и международных соревнованиях подтверждают высокий уровень подготовки специалистов и применимость внутренних методик в условиях, приближённых к реальным атакам.

Люди и их компетенции остаются ключевым элементом устойчивости

Приоритеты на следующий период включают развитие сценариев реагирования, киберразведки, масштабирование мониторинга, внедрение технологий искусственного интеллекта и усиление превентивной работы. Сформированный фундамент позволяет уверенно смотреть вперёд и планомерно усиливать защищённость цифрового пространства страны.

Этот обзор подводит итог году напряжённой и во многом незаметной работы. Впереди — новые вызовы и более сложные сценарии, но 2025 год показал: система выстояла, стала взрослее и готова двигаться дальше.

Профиль угрозы: **разборы инцидентов**

Тени APT: новые атаки в 2025 году

Атака с 20+ техниками MITRE ATT&CK: уроки для защиты инфраструктуры

Ключевые уязвимости Казнета и зоны KZ — масштабные утечки 2025

Тени APT: новые атаки в 2025 году

С каждым годом стремление APT-группировок атаковать критически важные объекты информатизации страны растёт.

Ранее мы сообщали о нескольких группировках, проводящих операции кибершпионажа. В их инструментарии преобладают легитимные программные обеспечения и публичные, но малоизвестные эксплоиты.

Сегодня поговорим про группировку, отличающуюся от предыдущих своей оригинальностью и технологической продвинутостью.

В августе 2025 года в одном из государственных органов средствами защиты информации зафиксированы аномальные и подозрительные сетевые активности, впоследствии классифицированные как несанкционированное действие.

В результате проведенного исследования установлено, что целевая кибератака осуществлялась двумя хакерскими APT-группировками, по внутренней атрибуции «STA-2404» и «STA-2405», осуществляющими «кибершпионаж». При этом, заражение сервера злоумышленниками осуществлялось в несколько этапов.

На первом этапе осуществлялась разведка и первичное проникновение.

Злоумышленникам «STA-2404» удалось получить доступ к серверу через удаленный сервис «RDP» с использованием легитимной учетной записи привилегированного пользователя (T1078.002 - Valid Accounts: Domain Accounts).

После закрепления на первоначально скомпрометированном сервере, злоумышленники приступили к боковому перемещению по корпоративной сети. Используя техники «Pass-the-Hash» (T1550.002 - Use Alternate Authentication Material: Pass the Hash) и утилиту «PsExec» (T1021.002 - Remote Services: SMB/Windows Admin Shares), атакующие последовательно получили доступ к другим рабочим станциям.

В процессе перемещения проводился активный сбор учетных данных из памяти процессов (T1003 - OS Credential Dumping) и разведка структуры «Active Directory» для выявления высоко привилегированных учетных записей (T1087.002 - Account Discovery: Domain Account) и критически важных систем (T1018 - Remote System Discovery).

После реализации мер по первичному закреплению зафиксирована активность второй группировки «STA-2405», действовавшей более методично и с использованием иного набора инструментов.

На данном этапе с помощью выполнения команд были проанализированы активные процессы через утилиту и занятые сетевые порты (T1049 – System Network Connections Discovery), необходимые для автоматизации горизонтального перемещения внутри инфраструктуры.

Дополнительно посредством утилиты «fscan» выполнено сканирование текущего контура с охватом более 40 узлов сети (T1046 – Network Service Discovery).

Спустя несколько месяцев после первоначального проникновения, злоумышленники перешли к следующей фазе атаки.

На скомпрометированные системы были загружены легитимные инструменты администрирования (PsExec, PowerShell, T1105 – Ingress Tool Transfer), использовавшиеся для маскировки вредоносной активности под обычные административные задачи (T1036.004 - Masquerading: Masquerade Task or Service). Параллельно было развернуто троянское вредоносное ПО семейства «PlugX».

Данное вредоносное ПО представляет собой улучшенную и модифицированную версию базового варианта «PlugX».

Ключевой отличительной особенностью этой модификации является реализация **«P2P»-управления (peer-to-peer),** при которой зараженные узлы напрямую обмениваются командами и данными через зашифрованные каналы, формируя устойчивую «mesh»-сеть без необходимости постоянного подключения к центральному серверу контроля и управления (C2).

Такая архитектура значительно повышает отказоустойчивость вредоносной инфраструктуры и затрудняет её обнаружение.

Используемые туннельные модули, работающие через протоколы **«HTTPS» и «DNS»** (T1071.001 – Application Layer Protocol: Web Protocols (HTTPS), T1071.004 – Application Layer Protocol: DNS), позволяют **скрытно передавать большие объемы данных** (T1041 – Exfiltration Over C2 Channel, T1048 – Exfiltration Over Alternative Protocol) **с минимальным риском обнаружения** системами мониторинга сетевого трафика.

В результате проведенной кибератаки злоумышленниками получены доступы к нескольким объектам информатизации инфраструктуры и **эксфильтрованы несколько сотен служебных данных.**

Атака с 20+ техниками MITRE ATT&CK:

уроки для защиты инфраструктуры

Началом этого расследования инцидента стало обращение к АО «ГТС» от пострадавшей организации, столкнувшейся с последствиями атаки вируса-шифровальщика.

Задача состояла в том, чтобы выявить коренные причины проникновения и проанализировать последствия инцидента.

Сотрудники АО «ГТС» незамедлительно начали работу с предоставленными цифровыми образами. Анализу подверглись критически важные системы: рабочие станции, серверы, контроллеры домена, а также журналы средств мониторинга.

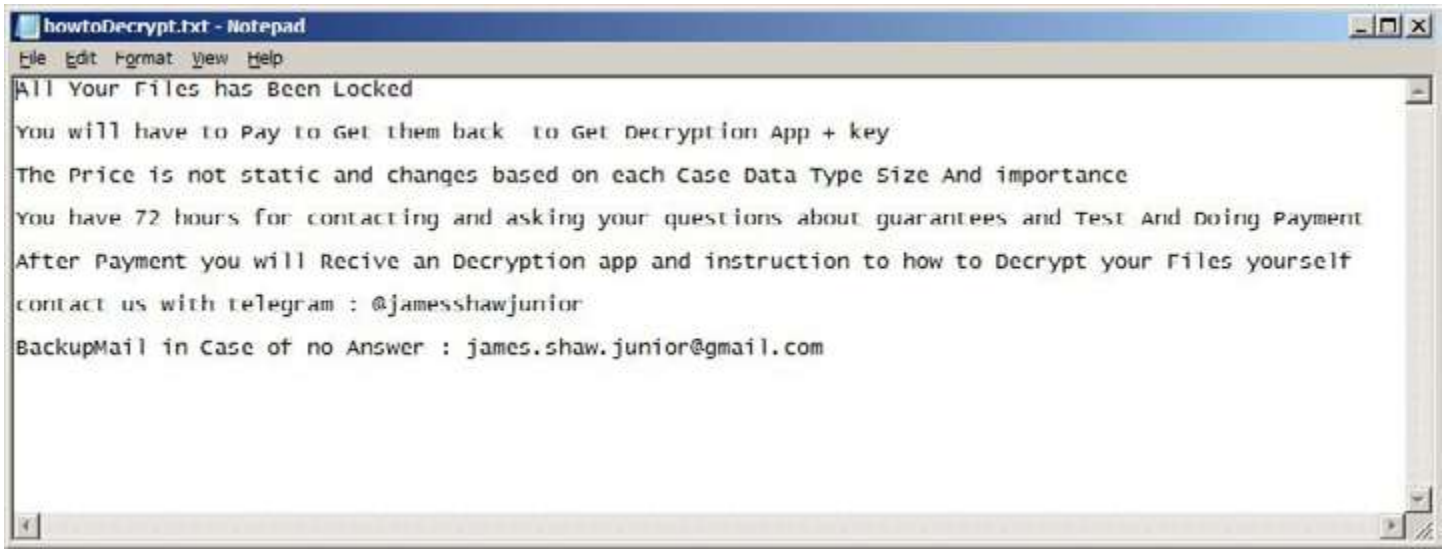
В результате анализа был собран обширный «портфель» вредоносных файлов, включая:

- Два экземпляра **MCVR100.dll**
- **Записка о выкупе (Nilson_Help.txt)**
- Исполняемые файлы **E.exe и Sphers.exe**
- Инструменты удаленного доступа **rdpwrap.dll и RDPWInst.exe**

Более того, в одном из обнаруженных файлов были выявлены идентификаторы киберпреступника — его Telegram-аккаунт и адрес электронной почты, которые ранее уже фигурировали в другом вредоносном контексте.

Все эти компоненты были переданы в специализированный центр анализа вредоносного ПО и загружены в изолированную исследовательскую инфраструктуру для дальнейшего детального изучения.

Рис.1. Записка о выкупе



По результатам анализа были установлены следующие факты:

- **E.exe**
  образец шифровальщика семейства Limbozar, расшифровка файлов без приватного ключа невозможна;
- **Nilson_Help.txt**
  записка о выкупе шифровальщика;
- **Файлы с расширениями вида *.Nilson**
  примеры данных, зашифрованных этим шифровальщиком;
- **Sphers.exe**
  инструмент для очистки свободного дискового пространства;
- **MCVR100.dll**
  текстовые отчёты о работе шифровальщика.

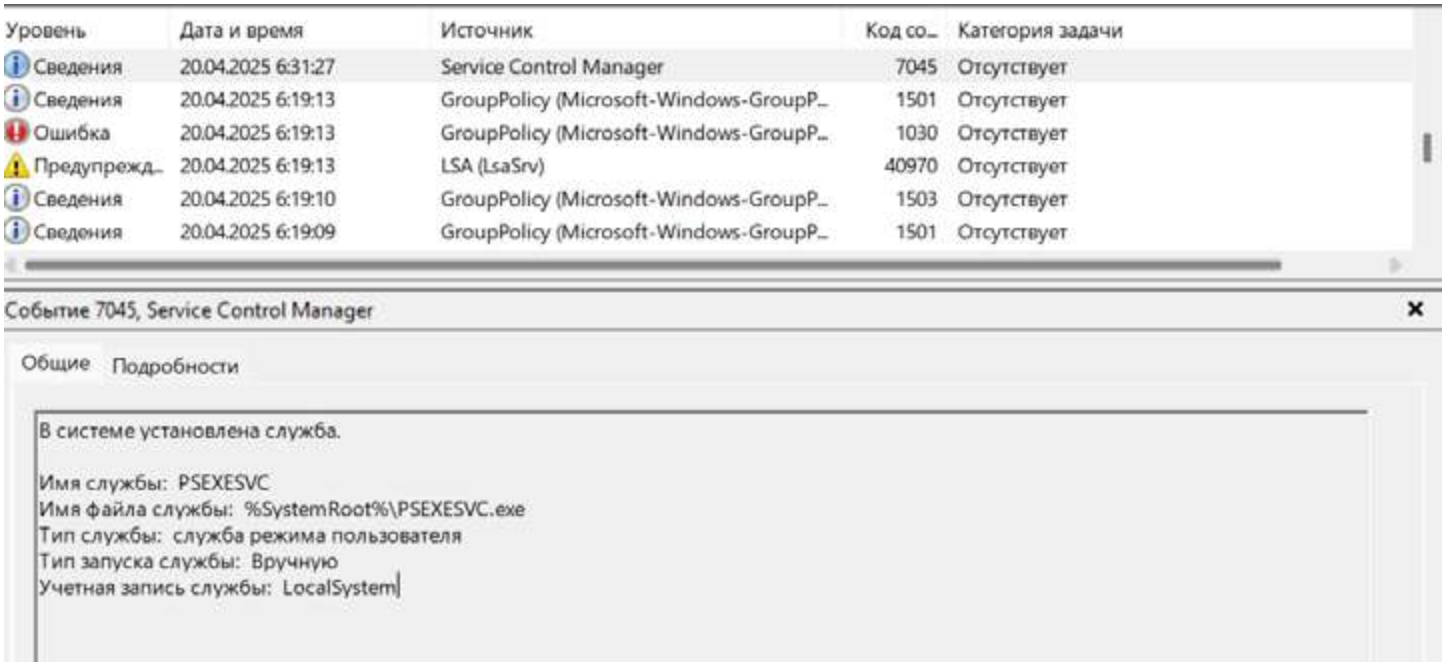
Дополнительно было установлено, что E.exe также соответствует шифровальщику, который добавляет к зашифрованным файлам специфическое расширение с идентификатором жертвы и использует собственную форму выкупного сообщения.

Анализ полученных данных показал, что активность злоумышленника началась с одной из рабочих станций инфраструктуры, где фиксировались запуски встроенных утилит, майнингового ПО и инструментов сетевого сканирования.

Обнаруженные встроенные утилиты Windows, которые злоумышленники часто используют для разведки или выполнения команд (living-off-the-land);

Таблица 1. Встроенные утилиты Windows использованные злоумышленником

Время (UTC+0)	Время (UTC+5)	Путь	Действие
2025-04-19 17:19:44	2025-04-19 22:19:44	C:\ranse\Prefetch\PSEXEC.EXE-60D1A2C5.pf	Запуск программы
2025-04-19 20:02:59	2025-04-20 01:02:59	C:\ranse\Prefetch\PSEXESVC.EXE-7F956DAF.pf	Запуск программы
2025-04-19 20:02:59	2025-04-20 01:02:59	C:\ranse\Prefetch\PSEXESVC.EXE-7F956DAF.pf	Запуск программы



Уровень	Дата и время	Источник	Код со...	Категория задачи
Сведения	20.04.2025 6:31:27	Service Control Manager	7045	Отсутствует
Сведения	20.04.2025 6:19:13	GroupPolicy (Microsoft-Windows-GroupP...	1501	Отсутствует
Ошибка	20.04.2025 6:19:13	GroupPolicy (Microsoft-Windows-GroupP...	1030	Отсутствует
Предупрежд...	20.04.2025 6:19:13	LSA (LsaSrv)	40970	Отсутствует
Сведения	20.04.2025 6:19:10	GroupPolicy (Microsoft-Windows-GroupP...	1503	Отсутствует
Сведения	20.04.2025 6:19:09	GroupPolicy (Microsoft-Windows-GroupP...	1501	Отсутствует

Обнаруженное майнинговое ПО

Peer2Profit.exe, iproyal_pawns

— это указывает на попытку монетизации ресурсов жертвы;

```
2025-04-15 00:12:05Z
  C:\ProgramData\Kaspersky Lab\IPRoyalPawns\iproyal_pawns.exe (1)
2025-04-15 00:11:46Z
  C:\ProgramData\Kaspersky Lab\1Peer2Profit\Peer2Profit.exe (1)
2025-04-15 00:07:12Z
  Microsoft.Getstarted_8wekyb3d8bbwe!App (14)
  Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App (13)
  Microsoft.WindowsMaps_8wekyb3d8bbwe!App (12)
  Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x (11)
  Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App (10)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (9)
  Microsoft.WindowsCalculator_8wekyb3d8bbwe!App (8)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (7)
```

Инструменты сетевой разведки — *Advanced IP Scanner, NetScan.exe* — применяются для:

Таблица 2. Использованные инструменты сетевой разведки

Время (UTC+0)	Время (UTC+5)	Путь	Действие
2025-04-19 22:17:16	2025-04-20 03:17:16	netscan.exe с рабочего стола (4)	Запуск netscan.exe с рабочего стола — утилита для сканирования сети
2025-04-19 01:04:59	2025-04-19 06:04:59	netscan.exe из Documents (1)	Запуск netscan.exe из папки Documents — повторное использование
2025-04-19 01:04:29	2025-04-19 06:04:29	Advanced_IP_Scanner_2.5.4594.1.exe (1)	Запуск установщика Advanced IP Scanner — вероятно, для сетевой разведки

Также из журналов событий установлено, что злоумышленник пытался загрузить и запустить ещё один шифровальщик chn.exe с удалённого ресурса, однако выполнение было заблокировано средствами защиты.

подробный анализ событий в таблице «Хронология действий злоумышленника»

Таблица 3. Хронология действий злоумышленника:

Время (UTC+0)	Время (UTC+5)	Действие злоумышленника
19.04.2025 23:45	20.04.2025 4:45	Запущен chn.exe с сетевого ресурса \\10.0.0.***\ vaeem\...
19.04.2025 23:43	20.04.2025 4:43	Запущен установщик systeminformer-3.0.7660-release-setup.exe с рабочего стола
19.04.2025 23:43	20.04.2025 4:43	Повторный запуск chn.exe с UNC-пути
19.04.2025 23:42	20.04.2025 4:42	Запуск интерфейса проводника Windows (explorer.exe)
19.04.2025 23:42	20.04.2025 4:42	Запущен dControl.exe из директории Defender. Control.2.1 на рабочем столе
19.04.2025 23:40	20.04.2025 4:40	Выполнен запуск powershell.exe
19.04.2025 23:36	20.04.2025 4:36	Запуск встроенных приложений: Calculator, Sticky Notes, Paint, Snipping Tool и др.

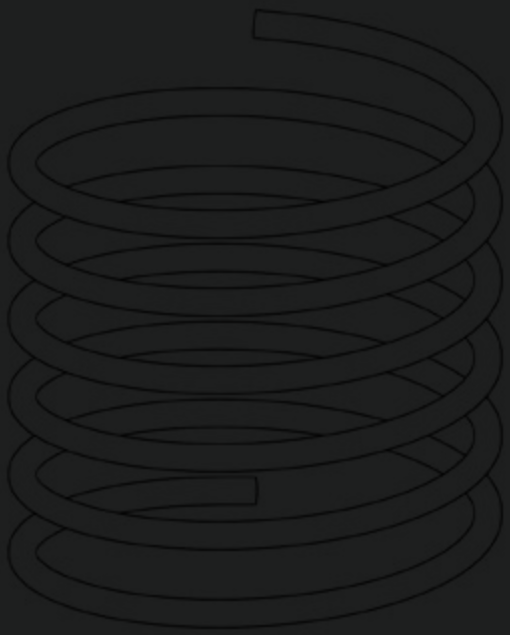
Таблица 4. Подробный анализ журнала событий касательно попытки запуска вируса шифровальщика

Дата и время	ID события	Детали
2025-04-20 04:40:24.839 +05:00	1116	Threat: Trojan:Win32/MammonRansom.YAN!MTB B¦ Severity: Severe B¦ Type: Trojan B¦ User: *OCAL\veeam B¦ Path: file:_\\10.0.0.***\vaaeem\chn.exe B¦ Proc: C:\Windows\explorer.exe
2025-04-20 04:41:42.260 +05:00	1116	Threat: Trojan:Win32/MammonRansom.YAN!MTB B¦ Severity: Severe B¦ Type: Trojan B¦ User: *_LOCAL\veeam B¦ Path: file:_\\10.0.0.***\vaaeem\chn.exe
2025-04-20 04:40:24.839 +05:00	1116	Threat: Trojan:Win32/MammonRansom.YAN!MTB B¦ Severity: Severe B¦ Type: Trojan B¦ User: *_LOCAL\veeam B¦ Path: file:_\\10.0.0.***\vaaeem\chn.exe B¦ Proc: C:\Windows\explorer.exe
2025-04-20 04:41:42.260 +05:00	1116	Threat: Trojan:Win32/MammonRansom.YAN!MTB B¦ Severity: Severe B¦ Type: Trojan B¦ User: *_LOCAL\veeam B¦ Path: file:_\\10.0.0.***\vaaeem\chn.exe

Финальная стадия анализа подтвердила **высокий уровень** подготовки злоумышленника и **комплексность** реализованной атаки.

Как был достигнут полный контроль

В ходе вторжения были **скомпрометированы несколько учетных записей**, которые стали плацдармом для дальнейших вредоносных действий. Используя эти скомпрометированные привилегии, атакующий последовательно развивал атаку, перемещаясь между рабочими станциями, серверами и, что критически важно, **контроллерами домена.**



Для развития атаки был задействован обширный набор инструментов и тактик:

- **Горизонтальное перемещение и исполнение:**
  Использовались инструменты удаленного выполнения команд, а также протокол SMB для быстрого распространения вредоносных компонентов по сети.
- **Закрепление и обход защиты:**
  Были запущены бэкдоры, изменены права доступа, а также задействованы механизмы обхода средств защиты (включая переопределение легитимных файлов Windows и отключение антивирусных служб).

На контроллерах домена злоумышленник действовал целенаправленно: устанавливал вредоносные службы, использовал легитимные системные компоненты для маскировки, **эскалировал привилегии и прочно закрепился** в ядре инфраструктуры.

Все эти действия отличались высокой степенью автоматизации, что позволило обеспечить охват как клиентских, так и критически важных серверных узлов доменной среды

Выводы и уроки для кибербезопасности

Обнаружено, что в процессе атаки было задействовано более 20 техник, описанных в матрице MITRE ATT&CK

Такая последовательность действий, включающая применение легитимных системных инструментов, автоматизацию и целенаправленное воздействие на контроллеры домена, позволила атакующему **добиться полного контроля** над инфраструктурой, успешно выполнить шифрование данных и максимально **скрыть следы своего присутствия**.

Это включает целенаправленную **очистку ключевых журналов** событий (Application, Security, Audit) в финальной фазе, что существенно затруднило восстановление полной картины инцидента.

Полученные результаты являются ярким свидетельством того, что текущие меры защиты требуют немедленного пересмотра.

Особое внимание необходимо уделить **усилению мониторинга привилегированных действий и внедрению более строгих механизмов контроля в доменной среде.**

Рекомендации

Обнаружено, что в процессе атаки было задействовано более 20 техник, описанных в матрице MITRE ATT&CK

По итогам всестороннего анализа, специалисты АО «ГТС» и подразделение KZ-CERT подготовили комплексные рекомендации. Эти меры направлены не только на устранение текущих последствий, но и на создание надежного барьера против повторных инцидентов.

Ключевые рекомендации включают:

- Усиление контроля за всеми привилегированными действиями.
- Корректировка настроек защиты на периметре и внутри сети.
- Повышение уровня журналирования для обеспечения полноты данных при будущих расследованиях.
- Улучшение процессов реагирования и мониторинга в масштабе всей инфраструктуры организации.

Ключевые уязвимости Казнета и зоны KZ: **масштабные утечки 2025**

В течение 2025 года утечки данных стали одной из наиболее актуальных и массовых угроз информационной безопасности в Казахстане. Были задокументированы многочисленные крупные инциденты, затронувшие как государственные структуры, так и частные компании.

Совокупный объём скомпрометированной информации исчислялся десятками миллионов строк, при этом в ряде случаев данные публиковались в открытом доступе либо распространялись через мессенджеры и специализированные форумы.

На этом фоне Национальная служба реагирования на компьютерные инциденты KZ-CERT в течение 2025 года вела активную разведку в казахстанском сегменте Интернета, выявляя и предупреждая критические уязвимости.

Ниже представлена сводка ключевых обнаружений и угроз.

Отрасль	Количество записей	Характер компрометации	Риски и особенности
Здравоохранение	~16 млн записей	Предположительно из крупной ИС. Массив фигурировал в продаже с декабря 2024 года	Длительный характер компрометации, риск многократной перепродажи
Электронная коммерция и Цифровые сервисы	~4,5 млн записей	Компрометация интернет-ресурса. Данные связаны с телекоммуникациями, образованием и контактными сервисами	Включение сведений о гражданах Республики Казахстан, создание национальных рисков
Экстренная медицинская помощь	~800 тыс. записей	Утечка базы данных ИС экстренной помощи. Злоумышленники демонстрировали выборки по 10 тыс. записей	Наличие полномасштабного доступа к данным станций скорой помощи
Средства массовой информации	>5,3 млн записей	Данные с 2016 по 2025 год: служебная информация и персональные данные пользователей	Значительный объём потенциального ущерба из-за длительности накопления
Финансовые услуги	228 682 строки	Файл с персональными данными, включая частично замаскированные номера банковских карт, ФИО и телефоны	Высокий риск реализации финансового мошенничества и таргетированных фишинговых атак
Строительная отрасль	~294 762 записи	Компрометация контактных и идентифицирующих данных жителей и организаций Казахстана	Утечка специфических региональных данных
Транспортная отрасль	Несанкционированный перенос служебных документов	Анализ системных артефактов указал на возможную причастность сотрудников. Документ опубликован в Telegram	Риск целенаправленной инсайдерской утечки

Прорыв периметра:
межсетевые экраны и VPN

1. Уязвимость Kerio Control
CVE-2024-52875

Дата обнаружения: 14 января 2025 года.

Находка: с помощью OSINT-разведки (поисковая система Shodan) было идентифицировано 120 межсетевых экранов Kerio Control в Казнете, которые оказались уязвимы.

Опасность: уязвимость (CVSS 8.8) позволяет удаленному злоумышленнику выполнить произвольный код с root-привилегиями через отправку специального HTTP-запроса. Это равносильно полному захвату сетевого периметра организации.

2. Атака на Cisco VPN
ArcaneDoor

Дата обнаружения: сентябрь 2025 года (после раскрытия Cisco).

Находка: KZ-CERT выявила 185 потенциально уязвимых устройств Cisco с активным Web-VPN в Казнете, включая 18 клиентов ЕШДИ.

Опасность: устройства подвержены цепочке из двух уязвимостей нулевого дня (CVE-2025-20333 и CVE-2025-20362). Эти уязвимости были активно эксплуатированы известной APT-группировкой (UAT4356/STORM-1849) в рамках кампании ArcaneDoor для установки постоянного доступа и внедрения буткитов (RayInitiator и LINE VIPER).

Слабые звенья веб-ресурсов:
CMS и почтовые сервисы

3. Массовое заражение WordPress:
плагины и вредоносные кампании

- **W3 Total Cache**
  CVE-2024-12365

  21 января 2025 года обнаружены 323 интернет-ресурса на CMS WordPress, использующих уязвимый плагин. Уязвимость позволяет аутентифицированным злоумышленникам (даже с правами подписчика) выполнять несанкционированные действия, что может привести к раскрытию информации и запросу данных из внутренних сервисов (например, метаданных облачных приложений).

- **WP3.XYZ**
  Атака на администраторов

  23 января 2025 года выявлен скомпрометированный ресурс, атакованный вредоносной кампанией wp3[.]xyz. Целью атаки является создание учетных записей администраторов, установка вредоносных плагинов и кража данных.

4. Критический провал в Roundcube Webmail
CVE-2025-49113

Находка: обнаружено 1**49 веб-интерфейсов Roundcube Webmail**, среди которых 5 клиентов ЕШДИ, потенциально подверженных критической RCE-уязвимости.

Опасность: уязвимость **существовала более десяти лет** во всех актуальных версиях. Она связана с логической ошибкой, позволяющей передать сериализованные данные, которые десериализуются PHP на сервере, приводя к **выполнению произвольного кода** с правами веб-процесса.

5. Уязвимости в Joomla и SharePoint

- **Joomla**
  Массовая проблема

  Обнаружены 5 022 уязвимых интернет-ресурса на базе CMS Joomla с 256 093 уязвимостями, имеющих 175 уникальных идентификаторов. Этот масштаб указывает на хроническое отставание в обновлении популярной системы.

- **Microsoft SharePoint**
  CVE-2025-53770 / ToolShell

  Выявлено 7 IP-адресов, потенциально уязвимых к критической RCE-уязвимости (CVSS 9.8). Атака не требует аутентификации и затрагивает локальные версии SharePoint Server, что делает ее крайне опасной для корпоративных систем.

Неожиданная цель:
промышленность и энергетика

6. Уязвимость систем ATG
Automated Tank Gauges

Находка: в ходе OSINT-мониторинга обнаружено 15 IP-адресов, использующих открытый порт 10001 для систем измерения уровня топлива в баке (ATG).

Опасность: ATG используются на заправках и топливных складах для мониторинга резервуаров. Открытый доступ к таким системам может позволить злоумышленникам не только получить чувствительную информацию о запасах топлива, но и потенциально вмешаться в их работу.

Анализ TLS/SSL-безопасности

хромающая криптография

KZ-CERT проанализировала более **180 000 интернет-ресурсов** в зоне KZ для оценки качества шифрования (SSL/TLS-конфигурации). **Результаты выявили многочисленные проблемы с безопасностью**, которые подрывают доверие к защищенным соединениям:

Категория проблемы	Описание и риск
Отсутствие TLS	ИР не поддерживает защищенное соединение HTTPS. (шифрование TLS не применяется вовсе)
Истекший сертификат	SSL/TLS-сертификат интернет-ресурса просрочен, срок его действия закончился
Несовпадение имени	Сертификат не соответствует домену: имя хоста не совпадает с именем, на которое выдан сертификат
Самоподписанный сертификат	Сертификат не подписан доверенным центром сертификации (CA), а является самоподписанным
Комбинированные проблемы	Сочетание вышеупомянутых уязвимостей на одном интернет-ресурсе (например, самоподписанный сертификат, чей срок уже истек, и др.)
Валидный сертификат	Корректный SSL/TLS-сертификат без обнаруженных проблем (действующий, соответствующий домену, подписан доверенным УЦ, срок действия более 30 дней)

Широкое распространение устаревших или некорректно настроенных сертификатов и методов шифрования представляет собой **системный риск для всего казахстанского сегмента Интернета.**

Устаревший щит:
тревожная статистика WordPress в Казнете

KZ-CERT провела масштабный аудит более **180 000 интернет-ресурсов** в доменной зоне .kz, сосредоточив внимание на популярной системе управления контентом WordPress. Результаты вызывают серьезную обеспокоенность, поскольку значительная часть ресурсов использует устаревшее ПО.

Масштаб: идентифицировано свыше 19 000 ресурсов на базе WordPress.
Опасный архаизм: из 13 869 ресурсов, для которых удалось определить версию, 5117 используют устаревшие версии.

Гонка за обновлениями:
почему старый WordPress — это риск

По состоянию на октябрь 2025 года, единственной актуальной и активно поддерживаемой версией является WordPress 6.8.x.

KZ-CERT выявила множество ресурсов, работающих на семействах версий:
- **WordPress 4.x** (например, 4.7–4.9)
- **WordPress 5.x** (5.0–5.9)
- **Ранние 6.x** (6.0–6.7)

Ключевые риски:

- **Отсутствие полной защиты:** хотя для некоторых старых версий (4.7–4.9 и 5.0–5.9) до 30 сентября 2025 года выпускались финальные обновления безопасности, они не получают новые функции и остаются на устаревшей программной базе.
- **Полное прекращение поддержки:** для самых старых версий (4.1–4.6) обновления безопасности не выпускаются с июля 2025 года, что делает их крайне уязвимыми.
- **Технологическое отставание:** версии ниже 6.8 не включают дополнительные механизмы защиты, реализованные в актуальной версии 6.8.3, и не в полной мере поддерживают современное программное окружение (например, актуальные версии PHP).

Использование устаревших версий, даже если для них еще выходят редкие патчи, ставит ресурсы под постоянную угрозу из-за отсутствия комплексной защиты.

Критическая брешь в FortiWeb: обход аутентификации

В ходе мониторинга открытых источников (OSINT-инструменты Shodan, ZoomEye) KZ-CERT обнаружила критическую угрозу, нацеленную на системы сетевой защиты:

- **Находка:** выявлено 148 IP-адресов, потенциально подверженных уязвимости Fortinet FortiWeb (CVE-2025-64446).
- **Масштаб угрозы:** уязвимость имеет критический рейтинг CVSS 9.8 из 10.
- **Механизм атаки:** уязвимость связана с обходом аутентификации и трассировкой пути (path traversal) в продукте FortiWeb.
- **Последствия:** успешная эксплуатация позволяет неавторизованному удаленному злоумышленнику выполнить административные команды и создать учетные записи с правами администратора.

Эта уязвимость предоставляет злоумышленникам полный контроль над защитным веб-приложением, что делает ее одной из самых опасных на обнаруженных в этот период.

KZ-CERT настоятельно рекомендует владельцам интернет-ресурсов и сетевого оборудования **незамедлительно проверить** свои системы на наличие указанных уязвимостей, применить соответствующие патчи и настроить корректное шифрование.

Создание Сети обмена интернет-трафиком:

шаг к устойчивому и автономному Казнету

В условиях динамичной международной обстановки вопросы устойчивости и независимости национальной интернет-инфраструктуры становятся особенно актуальными. Казахстан продолжает развивать собственные цифровые сервисы и укрепление внутренней сетевой архитектуры – важный элемент повышения уровня информационной безопасности и технологического суверенитета.

Одним из факторов, подчёркивающих необходимость модернизации, является существующее распределение международных каналов связи. Значительная часть трафика традиционно проходит через соседние государства, что потенциально приводит к технологическим рискам и влияет на доступность интернет-ресурсов. Ранее фиксировались случаи, когда обмен данными между казахстанскими операторами связи проходил через зарубежные маршруты, что увеличивало задержки и создавало дополнительные точки возможной нестабильности.

Роль Точки обмена интернет-трафиком (ТОИТ) в укреплении устойчивости национального сегмента Интернета

Для повышения автономности и отказоустойчивости Казнета были созданы государственные ТОИТ. Эти площадки позволяют операторам связи обмениваться трафиком внутри страны, сокращая зависимость от внешней инфраструктуры и улучшая скорость доставки данных.

В 2025 году узлы ТОИТ функционируют в 18 городах страны: Астана, Алматы, Актобе, Атырау, Актау, Караганда, Кызылорда, Павлодар, Семей, Уральск, Шымкент, Кокшетау, Костанай, Петропавловск, Усть-Каменогорск, Тараз, Талдыкорган и Жезказган. К ТОИТ подключен 31 оператор связи, суммарный объём передаваемого трафика превышает 300 Гбит/с. На площадках ТОИТ размещены DNS-серверы KZ-Root совместно с KazNIC, а также K-Root сервер от RIPE в Астане, что существенно повышает устойчивость национальной доменной зоны.

Создание ТОИТ заметно улучшило связанность и доступность локальных интернет-ресурсов, позволило перераспределить нагрузку и повысило устойчивость сервисов, работающих для пользователей внутри страны.

Роль ТОИТ в укреплении устойчивости национального сегмента Интернета

Несмотря на широкое покрытие ТОИТ, их узлы пока не соединены между собой собственной магистральной сетью. Междугородний обмен осуществляется через инфраструктуру междугородных операторов связи, что сохраняет определённую зависимость от их каналов.

Поэтому следующим логичным шагом является создание **Сети обмена интернет-трафиком (СОИТ)** — единой транспортной инфраструктуры, которая обеспечит прямую связанность между региональными ТОИТ и повысит автономность национального сегмента Интернета.

Что даст внедрение СОИТ?

Создание СОИТ станет качественным скачком в развитии национальной сетевой архитектуры. В числе ключевых преимуществ:

- **Повышенная автономность Казнета**

Даже при перебоях на международных каналах внутренние ресурсы продолжат работать в штатном режиме.

- **Надёжность и доступность госуслуг**

Сервисы электронного правительства и государственные информационные системы будут доступны через региональные узлы, расположенные в экосистеме Казнета.

- **Снижение зависимости от операторских магистралей**

Обмен трафиком будет происходить по собственной выделенной инфраструктуре.

- **Оптимизация маршрутов**

Меньше промежуточных звеньев — ниже задержки и выше скорость доступа.

- **Укрепление цифрового суверенитета**

СОИТ станет ключевым элементом национальной модели безопасности и устойчивости цифровой среды.

Инфраструктурные аспекты создания СОИТ и роль АО «ГТС»

Для работы СОИТ необходимы собственные магистральные каналы, связывающие региональные точки. На данный момент АО «ГТС» не располагает всей необходимой магистральной инфраструктурой, поэтому рассматривается модель партнёрства с операторами связи, которые уже имеют разветвлённые межрегиональные линии.

Такой подход широко используется в международной практике: государственные и частные организации совместно создают критически важную сетевую инфраструктуру, распределяя ресурсы и компетенции и ускоряя запуск проектов.

АО «ГТС» готово к проработке различных моделей взаимодействия с операторами связи на взаимовыгодных условиях. Операторы, заинтересованные в развитии национальной цифровой экосистемы, могут стать ключевыми участниками проекта, что позволит:

- Использовать имеющуюся магистральную инфраструктуру;
- Сократить сроки запуска СОИТ;
- Оптимизировать финансовые и технические затраты;
- Повысить устойчивость внутренней сетевой архитектуры Казахстана.

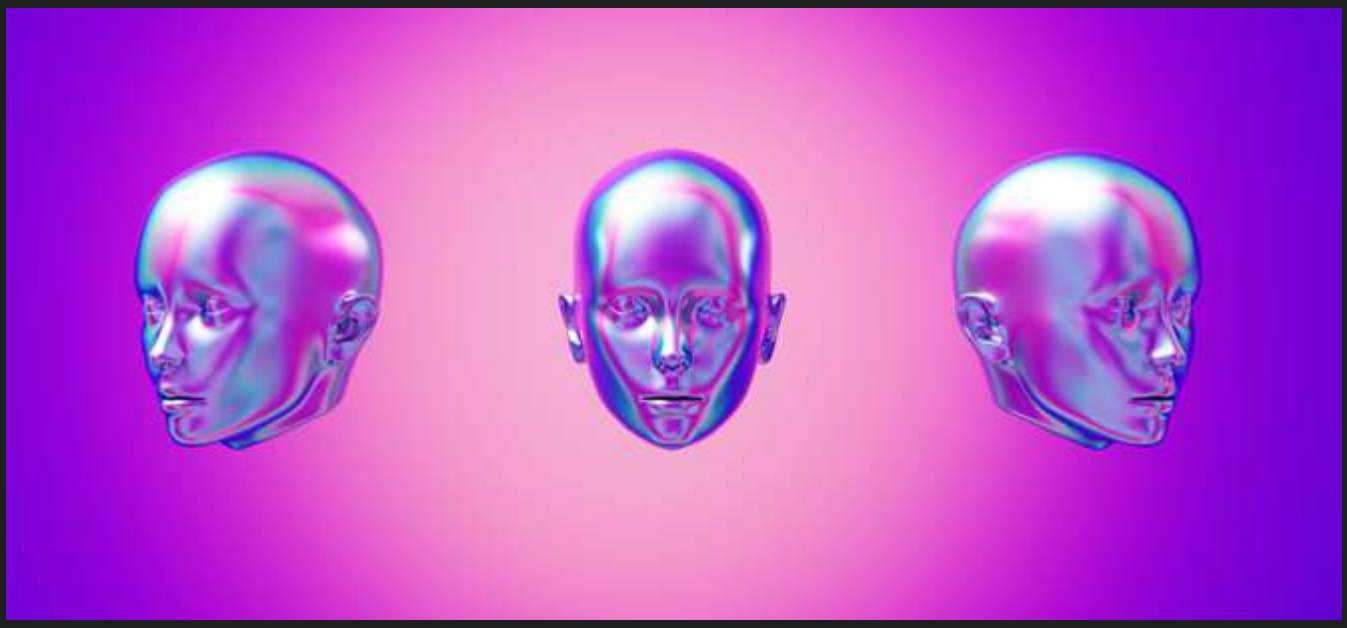
Таким образом, СОИТ предполагает партнёрскую модель, где АО «ГТС» выполняет роль координатора и интегратора, а операторы связи — инфраструктурных партнёров. Такой формат ускоряет реализацию проекта и повышает его эффективность.

Заключение

Развитие системы ТОИТ и создание СОИТ — это не просто модернизация сетевой инфраструктуры. Это стратегический шаг к формированию надёжного, независимого и устойчивого цифрового пространства Казахстана.

СОИТ повысит готовность национальной инфраструктуры к внешним вызовам, улучшит качество внутренних интернет-услуг, обеспечит стабильность государственных сервисов и укрепит информационную безопасность страны.

ИИ и кибербезопасность



- ИИ как главный инструмент вирусописателей
- «Оружие ИИ»: Как нейронки используются для атак
- «Броня ИИ»: Как использовать ИИ для защиты
- ИИ-капканы и анти-ИИ-щиты: куда эволюционирует искусственный нападающий
- Как мы создаём интеллектуальную систему, облегчающую рутину SOC-аналитикам
- Практика внедрения ИИ в процессы SOC
- Оптимизация поддержки в support.sts.kz

ИИ как главный инструмент вирусописателей

За последние годы киберпреступность прошла точку невозврата. Если раньше ИИ обсуждался как теоретическая угроза, то теперь он стал рабочим инструментом атак.

Одно из главных изменений - снижение порога входа. Вам больше не нужно быть экспертом, чтобы создавать сложное вредоносное ПО. Достаточно уметь правильно формулировать запросы к нейросети.

---

1. Феномен «Zero-Knowledge Threat Actor»

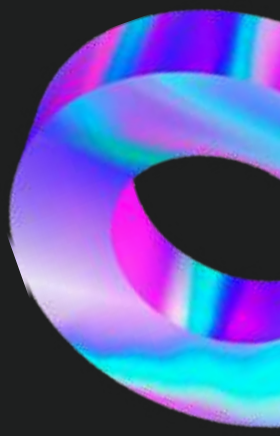
Злоумышленник с нулевыми знаниями

Одним из опасных последствий внедрения ИИ является появление «Zero-Knowledge Threat Actor». Это злоумышленники, не обладающие навыками программирования, которые используют ИИ для написания вредоносного кода.

Исследователи Cato CTRL доказали, что человек без опыта может заставить ChatGPT, Copilot или DeepSeek написать полноценно функционирующий инфостилер (вирус для кражи паролей), используя технику «сюжетной инженерии». Вместо прямого запроса «напиши вирус», атакующий создает выдуманный сценарий, где ИИ играет роль детектива или персонажа игры, для которого написание такого кода является частью сюжета, а не нарушением закона.

2. Dark LLM

На смену попыткам обмануть легальные модели пришли специализированные инструменты для преступников, названные как Dark LLMs:



WormGPT и FraudGPT:
Первые массовые модели, обученные на данных о малвари и фишинге. Они позиционируются как «ChatGPT без ограничений» и позволяют генерировать идеальные фишинговые письма и вредоносные скрипты без этических фильтров.

Xanthorox:
Более продвинутый инструмент 2025 года, способный писать сложный системный код на C++ для обхода современных антивирусов, включая создание драйверов и работу с памятью.

Мимикрия:
Часто под видом «уникальных хакерских нейросетей» продаются просто «обертки» (wrappers) для GPT-4 или Claude, к которым прикручены автоматические джейлбрейки.

---

3. Невидимая угроза

ИИ позволил создать малварь, которая меняет саму себя во время работы, делая традиционные антивирусы бесполезными.

BlackMamba и MalGEN:
Концепции вредоносного ПО, которое не несет в себе вредоносного кода. При запуске программа обращается к API (например, OpenAI), просит сгенерировать код атаки (например, кейлоггер) и исполняет его прямо в памяти.

PROMPTFLUX:
Вредоносное ПО, которое использует ИИ для полной перезаписи своего кода каждый час. Оно создает бесконечный цикл мутаций, где каждая новая версия программы уникальна и не похожа на предыдущую, но выполняет ту же задачу.

4. Новый вектор атак: Hallucination Squatting

Злоумышленники используют склонность ИИ выдумывать факты. Модели часто предлагают разработчикам использовать несуществующие библиотеки кода. Хакеры находят эти повторяющиеся галлюцинации, создают реальные вредоносные пакеты с такими именами и загружают их в репозитории (например, npm или PyPI). Жертва, доверяя совету ИИ, сама устанавливает вирус.

Заключение

Интеграция ИИ в инструментарий киберпреступников - не просто эволюция, а революция, меняющая правила игры.

Последние годы показали, что порог входа в киберпреступность практически исчез, а возможности автоматизации достигли уровня, позволяющего создавать уникальное ВПО в промышленных масштабах.

Появление Dark LLM, техник джейлбрейка, автономного полиморфизма и атак на цепочки поставок через галлюцинации требует от защитников перехода от реактивной защиты к проактивному управлению рисками ИИ.

«Оружие ИИ»:
как нейронки используются для атак

В 2025 году кибербезопасность находится в состоянии «гонки вооружений», где искусственный интеллект (ИИ) стал мощнейшим инструментом в руках злоумышленников. Нейронные сети, особенно большие языковые модели (LLM) и генеративно-состязательные сети (GAN), позволяют создавать автоматизированные, адаптивные и труднообнаружимые атаки.

1. Трансформация социальной инженерии

Использование LLM позволило преступникам перейти от массовых рассылок к созданию гиперреалистичного контента.

- **Гиперреалистичный фишинг:**

  LLM сканируют цифровой след жертвы для создания персонализированных сообщений без грамматических ошибок. CTR (кликабельность) таких писем достигает 54% против 12% у текстов, написанных людьми.

- **Атаки Business Email Compromise** (BEC-атаки):

  Модели имитируют корпоративный стиль и тон голоса руководителей для кражи средств или данных.

- **Дипфейки:**

  В 2025 году число инцидентов с аудио- и видеоподменами выросло на 500%. Технологии используются для обхода биометрии и мошенничества с имитацией руководства (CEO Fraud).

2. Автономное и адаптивное вредоносное ПО

Наиболее опасным трендом стала интеграция нейросетей непосредственно в тело вируса для обеспечения его автономности.

- **Концепция Just-in-Time AI** (JIT-AI):

  Вредоносное ПО использует API нейросетей (например, Gemini или Hugging Face) для генерации кода прямо в процессе атаки.

- **Самообучающийся код:**
  - **PROMPTFLUX:**

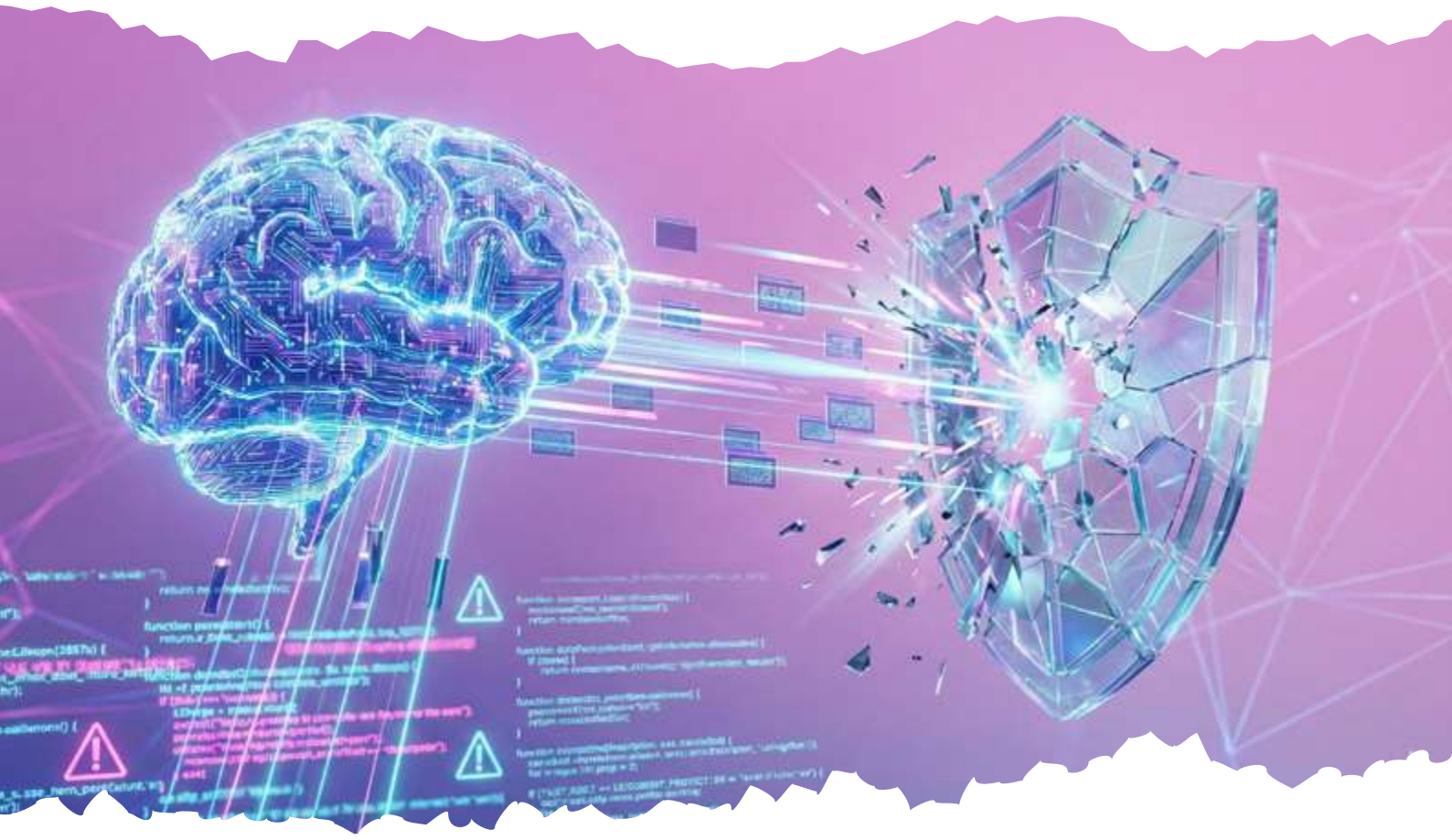
    Дроппер, который переписывает свой исходный код в процессе исполнения, чтобы оставаться скрытым.

  - **PROMPTLOCK:**

    Программа-вымогатель, которая на лету решает, какие файлы шифровать, исходя из анализа среды.

- **Автоматизация эксплуатации:**

  ИИ-боты сканируют сети и разрабатывают векторы атаки с хирургической точностью.



3. Атаки против систем машинного обучения
Adversarial ML

Поскольку защита сама полагается на ИИ, злоумышленники начали атаковать непосредственно модели безопасности.

- **Состязательные примеры** (Evasion):
  В код или текст добавляются незаметные для человека «шумы», заставляющие нейросеть-детектор классифицировать вредоносный файл как безопасный.
- **Отравление данных** (Data Poisoning):
  Внедрение ложных данных на этапе обучения модели защиты для создания «бэкдоров» или снижения её общей точности.

---

4. Интеллектуальные DDoS-атаки

ИИ изменил характер распределенных атак, сделав их адаптивными и многовекторными.

- **Эмуляция поведения:**
  Ботнеты имитируют действия человека для обхода CAPTCHA и фильтров.
- **Динамическое распределение:**
  Нейросети меняют характер трафика в режиме реального времени, подстраиваясь под контрмеры. Пример — зафиксированная 18-дневная кампания против Cloudflare в начале 2025 года.
- **Демократизация угроз:**
  Появление сервисов «DDoS-as-a-Service» с ИИ-интерфейсами позволяет даже неопытным хакерам проводить сложные атаки.

2025 год закрепил переход киберпреступности к модели «преступление как услуга» (Crime-as-a-Service), существенно снизив порог входа для злоумышленников. Ключевым фактором выживания систем безопасности становится не только развитие защитных нейросетей, но и глубокое понимание уязвимостей самих ИИ-моделей.

«Броня ИИ»:
как использовать ИИ для защиты

В 2025 году кибербезопасность окончательно перешла к формату **«противостояния ИИ против ИИ».** Традиционные сигнатурные методы стали неэффективными против атак, проводимых на «машинной скорости». Искусственный интеллект превратился из вспомогательного инструмента в центральную архитектурную основу прогностической безопасности.

1. Агентный ИИ (Agentic AI): автономный защитник

Агентный ИИ — это продвинутая система, способная принимать независимые решения и адаптироваться к новым угрозам с минимальным участием человека.

- **Трансформация SOC:**

  Аналитик перестает быть исполнителем и становится архитектором и аудитором системы.

- **Ключевые возможности:**

  Мониторинг миллионов точек данных в реальном времени, самостоятельная оценка угроз и выбор сценариев реагирования.

- **Мгновенная реакция:**

  При обнаружении аномалии (например, входа из необычной геолокации) агент может самостоятельно изолировать учетную запись и запустить анализ, сокращая время реагирования (MTTR) с часов до секунд.

2. Обнаружение угроз «нулевого дня» Zero-Day

ИИ выявляет неизвестные угрозы через поведенческий анализ, строя динамический базовый уровень «Нормы».

- **Неконтролируемое обучение:**
  Эффективно против полиморфного ПО и атак типа «living off the land».
- **Глубокое обучение** (RNN):
  Выявляет сложные временные зависимости в системных событиях.

Например, обнаружение эксплойта LANDFALL (CVE-2025-21042), нацеленного на устройства Samsung с применением критической уязвимости «нулевого дня» в библиотеке обработки изображений, стало возможным не по сигнатуре файла, а через выявление аномальных цепочек процессов (высокое выделение памяти и необычные сетевые вызовы).

---

3. LLM в системах оркестрации (SOAR)

Большие языковые модели (LLM) автоматизируют когнитивно-емкие задачи в центрах безопасности.

- **Создание сценариев** (Playbooks):
  Аналитик может запрашивать создание сложных цепочек защиты на естественном языке.
- **Контекстуальное обогащение:**
  LLM объединяет данные SIEM и Threat Intelligence, предоставляя готовую сводку рисков по подозрительным IP-адресам или пользователям.
- **Автоматизация отчетности:**
  Модели мгновенно генерируют отчеты об инцидентах, соответствующие стандартам NIST или ISO 27001.

4. Проактивная охота за угрозами
Threat Hunting

ИИ трансформирует поиск скрытых угроз в высокоскоростной процесс корреляции данных.

- **Malware-free атаки:**

  Согласно отчету CrowdStrike за 2025 год, 81% вторжений происходят без использования вредоносного ПО (через легитимные инструменты системы). ИИ выявляет такие атаки, анализируя необычные последовательности команд (например, в PowerShell).

- **Динамическая приоритизация уязвимостей:**

  ИИ присваивает Risk-score уязвимостям, учитывая их активность в даркнете и уникальную архитектуру сети организации, а не только техническую серьезность CVSS.

---

5. Защита от состязательного ИИ
Adversarial AI

Сами модели ИИ становятся поверхностью атаки, что требует внедрения механизмов защиты.

Тип атаки	Описание	Механизм защиты (2025)
Состязательные искажения	Внесение изменений в данные для обхода детектора	Состязательное обучение (Adversarial training)
Отравление данных	Внедрение ложных данных в обучающий набор	Проверка целостности данных и обработка аномалий
Jailbreaking LLMs	Попытки обойти политики безопасности модели	Усиление охранных периметров (guardrails)

Будущее кибербезопасности зависит от способности построить устойчивую архитектуру, где ИИ является центральным звеном проактивной защиты.

ИИ-капканы и анти ИИ-щиты:

куда эволюционирует искусственный нападающий

В 2025 году технологии искусственного интеллекта (ИИ), особенно большие языковые модели (LLM), стали критическим активом как для организаций, так и для киберпреступников. ИИ спровоцировал «кибергонку вооружений», где наступательные возможности развиваются быстрее традиционных механизмов защиты.

Современные инструменты демократизировали доступ к сложным атакам, снизив порог входа для злоумышленников.

1. ИИ-капканы:

эволюция искусственного нападающего

Главные отличия «искусственного нападающего» — контекстуальная осведомленность, адаптивность и скорость.

1.1. Генеративный ускоритель социальной инженерии

ИИ превратил социальную инженерию в высокомасштабируемый конвейер.

- **Гиперперсонализированный фишинг и BEC:**

  Злоумышленники используют ИИ для автоматического сбора данных (OSINT) и генерации сообщений, имитирующих индивидуальный стиль речи (style mimicry) руководителей. Успешность таких атак в 2025 году выросла на 45%.

- **Дипфейк-мошенничество:**

  Голосовые дипфейки (vishing) позволяют клонировать голос в реальном времени для обхода аутентификации. В видеоконференциях синтетические изображения используются для отдачи ложных финансовых распоряжений. В 70% случаев жертвы не могут распознать подделку при первом контакте.

1.2. Адаптивное вредоносное ПО

- **Полиморфизм и уклонение:**

  ИИ генерирует код с уникальными сигнатурами, делая классические антивирусы бесполезными. Вредоносное ПО может самомодифицироваться при обнаружении или имитировать нормальные системные процессы (например, медленное шифрование под видом бэкапа).

- **Автономная разведка:**

  ИИ-агенты самостоятельно исследуют сеть, выявляют ценные активы и выбирают оптимальный путь для бокового перемещения (lateral movement). «Время прорыва» (breakout time) сократилось до менее чем 60 минут.

2. Демократизация преступности

и новые угрозы

- **Crime-as-a-Service:**

  Появление вредоносных моделей вроде WormGPT и FraudGPT позволяет даже неопытным хакерам генерировать эксплойты и фишинговый контент.

- **Атаки на сами ИИ-системы:**

  - **Враждебные атаки** (Adversarial attacks):

    Использование инъекций запроса (prompt injection) для раскрытия данных. В системах компьютерного зрения минимальный «шум» заставляет модель неверно классифицировать объекты (например, дорожные знаки).

  - **Заражение данных** (Data poisoning):

    Внедрение «бэкдоров» в обучающие наборы данных, которые срабатывают только при специфическом триггере.

- **Теневой ИИ** (Shadow AI):

  Сотрудники, использующие публичные LLM для работы, создают риски утечки конфиденциального кода и финансовых отчетов.

3. Анти ИИ-щиты:

асимметричный ответ защитников

Защита переходит от реактивных мер к проактивной автоматизации.

3.1. ИИ в обнаружении и реагировании

- **Автоматизация SOC** (XDR/SOAR):

  ИИ агрегирует данные из облаков, сетей и конечных точек, отсеивая ложные срабатывания. Системы SOAR могут автоматически изолировать сегменты сети или сбрасывать учетные данные за секунды. Внедрение таких решений сократило время реагирования на 40%.

- **Предиктивное управление:**

  ИИ прогнозирует вероятность эксплуатации уязвимостей, позволяя приоритизировать патчинг. Также используются ИИ-агенты для непрерывной имитации атак (BAS).

3.2. Стратегические подходы

- **Zero Trust Architecture** (ZTA):

  Отказ от доверия внутреннему периметру. Микросегментация сети запирает вредоносную LLM в узком сегменте, не давая ей распространяться.

- **Identity-first security:**

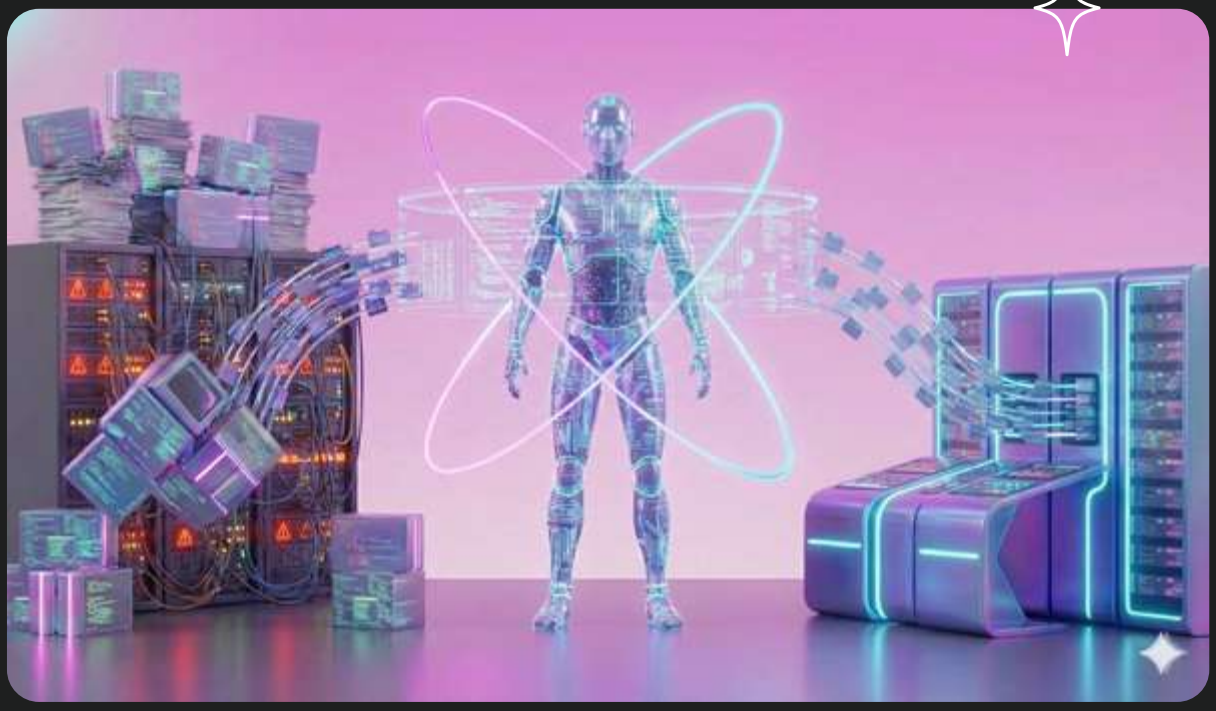
  Использование адаптивной MFA, которая требует дополнительной проверки при малейших отклонениях в поведенческом профиле пользователя.

3.3. Защита моделей (MLeC)

Организации внедряют фреймворки типа MITRE ATLAS для защиты от prompt injection и мониторинга смещения (drift detection) точности моделей. Для повышения устойчивости применяется обучение моделей на специально сгенерированных враждебных примерах (adversarial training).

В 2025 году кибербезопасность окончательно перешла в фазу, определяемую скоростью ИИ. Победа зависит от сочетания технологического превосходства (автоматизация XDR/SOAR) и жесткого управленческого контроля (AI Governance). Будущее за «автономным пентестингом» и созданием экосистем доверенных данных.

Как мы создаём интеллектуальную систему, облегчающую рутину **SOC-аналитикам**



Работа SOC-аналитиков — одна из самых насыщенных и ответственных в компании. Ежедневно специалисты просматривают тысячи событий, логов, уведомлений и аномалий, поступающих в реальном времени. В условиях высокого темпа и постоянного информационного шума нагрузка становится критичной: требуется одновременно следить за инцидентами, анализировать происходящее и при этом формировать отчёты, которые должны быть точными, структурированными и основанными на данных. Подготовка таких материалов — отдельная трудоёмкая задача: нужны агрегации, выборки, анализ пиков, интерпретация динамики и проверка на непротиворечивость.

Чтобы снять часть этой нагрузки, мы начали разработку интеллектуального ассистента — системы, которая **понимает запросы SOC-аналитиков в произвольной форме и мгновенно формирует ответ на основе данных из обогащённых логов SIEM-систем.** Это не просто чат-интерфейс поверх базы данных. Это полноценный аналитический модуль, который умеет интерпретировать смысл запроса, находить нужные данные, рассчитывать агрегаты и представлять результат в виде готовой аналитики.

*«Это не просто чат-интерфейс поверх базы данных. Это полноценный аналитический модуль, который **умеет интерпретировать смысл запроса,** находить нужные данные, рассчитывать агрегаты и представлять результат в виде готовой аналитики»*

Главная идея проста: позволить аналитику работать в формате «спросил — получил». Пользователь формулирует вопрос обычным языком: «Покажи пики событий за последние два часа», «Какие атаки были за последний час?», «Сделай сводку» — и получает точный, структурированный и подтверждённый данными ответ. **Время на подготовку материала сокращается с нескольких часов до нескольких минут.**

В основе системы — LLM, работающая исключительно с внутренними источниками. Модель не придумывает факты: она опирается на реальные данные SIEM, историю диалога и подтверждённые события. Это критически важно для безопасности, где недостоверность недопустима. Несмотря на небольшие вычислительные ресурсы, система способна анализировать контекст, интерпретировать сложные вопросы и формировать отчёты, включающие цифры, пики нагрузки, динамику и любые виды агрегаций.

*«Время на подготовку материала сокращается **с нескольких часов до нескольких минут...** инструмент экономит не просто время — он **сокращает когнитивную нагрузку** и помогает аналитикам сосредоточиться на принятии решений»*

На следующем этапе проект станет ещё мощнее. Мы планируем расширять функциональность, чтобы система не только извлекала данные и формировала отчёты, но и помогала принимать решения: предлагать варианты реакции на инцидент, выявлять нетипичное поведение, рекомендовать приоритеты обработки.

По мере развития ассистент станет частью повседневной работы SOC-команды — таким же привычным инструментом, как SIEM, но значительно более гибким и интеллектуальным. Это шаг к тому, чтобы аналитики работали быстрее, точнее и увереннее, а компания получала выгоду от более эффективного и современного подхода к информационной безопасности.

Практика внедрения ИИ в процессы SOC

1. Операционный тупик: почему классическая модель SOC больше не работает

Мы подошли к точке, где традиционный подход к мониторингу безопасности (ручной разбор логов SIEM) стал физически невозможен. Ситуация в отрасли характеризуется не просто нагрузкой, а полноценным кризисом видимости.

Кризис масштаба
Крупные инфраструктуры генерируют свыше 10 000 алертов ежедневно. Даже укомплектованные команды SOC (а таких единицы) физически не способны качественно обработать этот поток — 66% команд признают, что не справляются.

Паралич аналитиков
Главная проблема — катастрофическое соотношение сигнала к шуму. До 83% всех оповещений — это «пустышки» (False Positives). При этом на разбор каждого такого «ложного вызова» аналитик тратит в среднем более 10 минут. В итоге высококвалифицированные специалисты занимаются механическим закрытием тикетов, пропуская реальные атаки.

Слепые зоны
Чтобы хоть как-то снизить нагрузку, SOC начинают «отключать датчики». Тревожная статистика: 34% центров мониторинга уже отказались от инспекции SSL/TLS-трафика, просто потому что у них нет ресурсов на его расшифровку и анализ. Это открывает злоумышленникам прямой туннель в защищаемый периметр.

Вывод:
Дальнейшее масштабирование штата линейных аналитиков (L1) экономически бессмысленно. Единственный выход — смена парадигмы с сигнатурного анализа на поведенческий (UEBA) и автоматизированный.

2. Эволюция инструментов: Три волны ИИ

Внедрение ИИ в SOC — это не разовая закупка «волшебной коробки», а поэтапный процесс. На рынке сейчас четко прослеживаются три технологические волны.

Волна 1:
UEBA (Отсекаем шум)

Вместо того, чтобы писать тысячи правил корреляции («если 5 ошибок входа, то алерт»), мы внедряем поведенческий анализ (UEBA). Система сама строит профиль нормы для каждого юзера и узла.

Как это работает:
если администратор, который обычно работает из Астаны в рабочее время, вдруг в 3 ночи подключается к базе данных с незнакомого IP — это аномалия.

Результат:
Мы перестаем реагировать на каждое событие отдельно. Система сама склеивает сотни логов в один инцидент. Реальный кейс Golomt Bank показал снижение «шума» на 60% и ускорение расследований на 40%.

Волна 2:
NLP в киберразведке (Читаем быстрее)

До 80% данных об угрозах (Threat Intelligence) приходят в виде текстов: отчетов вендоров, статей, бюллетеней. Человек не успевает их читать и переводить в правила защиты.

Решение:
NLP-модели (обработка естественного языка) автоматически «вычитывают» эти отчеты. Они вытаскивают не только IP-адреса (которые живут пару часов), но и TTPs (тактики и техники) злоумышленников.

Эффект:
SOC переходит от реактивной блокировки к проактивному поиску угроз, сокращая время реакции с недель до минут.

Волна 3:
GenAI и Агенты (Меняем процесс)

Самый свежий тренд, меняющий саму суть работы аналитика.

1. Co-pilot (Помощник):
работает как «второй пилот». Аналитик пишет запрос на удобном ему языке («покажи все входы админов мимо VPN»), а ИИ сам переводит это в сложный код запроса к SIEM (KQL/SPL). Также отлично справляется с рутиной — пишет отчеты по инцидентам.

2. Agentic AI (Автономный сотрудник):
это уже замена первой линии (L1). В отличие от старых скриптов (плейбуков SOAR), которые ломаются при любой нестандартной ситуации, ИИ-агенты умеют «рассуждать». Они помнят контекст («этот сервер всегда бэкапится по ночам, это не атака») и сами принимают решение закрыть инцидент.

3. Экономика внедрения: Цифры и KPI

Для обоснования инвестиций перед руководством стоит опираться на изменение ключевых метрик. ИИ не просто «улучшает» работу, он меняет её структуру.

Сейчас в ручном режиме мы видим лишь верхушку айсберга (~33% алертов), остальное игнорируется. ИИ обеспечивает **100% первичную обработку** каждого сигнала.

Время на принятие решения (инцидент или ложное срабатывание) падает с 40 минут **до 3-10 минут.**

Компании с развитым ИИ в безопасности теряют на утечках данных в среднем на **$2.2 млн меньше,** чем те, кто работает по старинке.

Сравнение эффективности:

Показатель	Традиционный SOC	SOC с ИИ
Обработка алертов	~33% *(остальное в drop)*	**100%** *(авто-триаж)*
Ложные срабатывания (*на ручном разборе)*	До 83% потока	Снижение на **60-70%**
Время вердикта *(MTTC)*	30-40 мин	3-11 мин
Эскалация на человека	Весь поток	**-95%** *(только сложные)*

4. Люди и Риски: «Холодный душ»

Не стоит питать иллюзий: ИИ — это не автопилот, который можно включить и уйти.

Главные риски:

Эффект «Черного ящика»
Нейросеть может принять верное решение, но не сможет объяснить почему. Для юридически значимых действий (блокировка, суд) всегда нужна валидация человеком.

Атаки на сам ИИ
Хакеры уже учатся обманывать модели. Классический пример — «отравление данных» (Data Poisoning), когда злоумышленник специально «скармливает» системе мусорный трафик, чтобы приучить её считать атаку нормой.

Разочарование
Опросы SANS 2024 показывают, что удовлетворенность от внедрения GenAI пока низкая (оценка 1.8 из 5). Причина проста: люди пытаются использовать «сырые» модели без обучения контексту.

Кадровая стратегия:

Мы не найдем на рынке готовых специалистов по защите ИИ — их просто нет.

Единственный путь — это внутренний апгрейд. Нужно брать опытных аналитиков L3 (которые знают специфику наших сетей) и дообучать их работе с данными и ML.

ИИ не заменит экспертов.

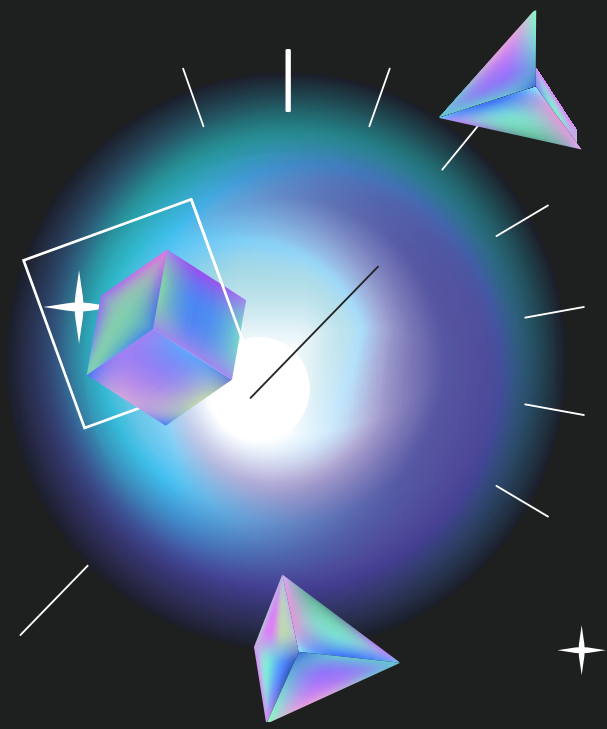
Он убьет рутинные должности «клик-операторов» (L1), но создаст острую потребность в «архитекторах детектирования» и «тренерах нейросетей».

Оптимизация поддержки в support.sts.kz

Когда речь идёт о консультациях на основе нормативно-правовых документов, ключевым становится не только полнота базы знаний, но и скорость нахождения точного ответа. Пользователи обращаются с десятками вопросов: от трактовки пунктов регламентов до практических ситуаций, связанных с применением норм. Вручную отсматривать документы, искать нужные формулировки, сверять версии – длительный и сложный процесс.

Чтобы сократить это время и повысить качество консультаций, в процессе разработки находится чат-бот в **support.sts.kz** — интеллектуальная система, которая поможет отвечать пользователям на основе уже существующей базы нормативно-правовых документов и накопленных ранее вопросов и ответов.

*«Это позволяет **сравнивать тексты не по ключевым словам, а по смысловой близости**... такой подход даёт возможность находить подходящие материалы даже тогда, когда формулировка вопроса отличается от терминологии документа»*



Система разрабатывается на основе векторного поиска. Каждый документ – статья, пункт, разъяснение или ответ – преобразуется в векторное представление. Это позволяет **сравнивать тексты не по ключевым словам, а по смысловой близости.** Алгоритм вычисляет косинусное сходство между вектором пользовательского запроса и векторами документов базы, ранжируя результаты по степени соответствия. Такой подход даёт возможность находить подходящие материалы даже тогда, когда формулировка вопроса отличается от терминологии документа.

*«Пользователь получает не просто пересказ нормативного текста, а **структурированное и контекстное объяснение**, основанное на проверенных источниках»*

После отбора релевантных фрагментов система передаёт их LLM-модели, которая формирует финальный ответ. При этом модель опирается исключительно на предоставленные документы, что исключает домыслы и повышает точность.

За счёт векторного поиска система бужет работать быстро даже при большой базе. Вместо того, чтобы обращаться к документам напрямую, она сначала ищет смысловое совпадение, а уже потом передаёт соответствующие источники модели. Такая многоступенчатая схема обеспечивает скорость, точность и масштабируемость.

Преимущество решения проявляется сразу:

- Сокращается время на обработку обращений
- Пользователи получают корректные и обоснованные ответы
- Сотрудники поддержки избавляются от рутины
- Повышается единообразие формулировок и толкований норм
- Исключаются ошибки, связанные с неверным трактованием текста

В итоге support.sts.kz превращается в универсальный инструмент, который делает работу с нормативно-правовой базой проще, быстрее и понятнее. Он соединит мощность векторного поиска, точность юридических источников и гибкость современных LLM-моделей, создавая экосистему, где знания становятся по-настоящему доступными.

*Такой подход не просто ускоряет ответы – он формирует **единый стандарт обработки обращений,** повышает качество сервиса и создаёт **фундамент для дальнейшей автоматизации процессов.***

DevSecOps:

значимость и роль SAST

1. Что такое SAST и почему это выгодно

SAST (Static Application Security Testing) — статический анализ исходного кода и связанных артефактов до запуска приложения. Он переносит безопасность в начало SDLC (shift-left), когда исправления быстрее и дешевле.

- **Ловит дефекты до релиза:** меньше инцидентов, штрафов и внеплановых «пожарных» патчей.
- **Делает политику безопасности измеримой:** правила и критерии допуска фиксируются и исполняются автоматически.
- **Перераспределяет ответственность:** безопасность становится обязанностью владельцев сервисов, а не «аудитом в конце».

2. Роль SAST в DevSecOps-конвейере

- **IDE/локально:** быстрый фидбек разработчику, пока контекст свежий.
- **Pull request:** анализ как часть ревью, комментарии прямо в diff, единый процесс подавлений/исключений.
- **CI/CD:** quality gate (warn → block поэтапно), запрет на вливание небезопасных изменений.
- **Периодические full-scan:** контроль техдолга и выявление уязвимостей вне активных PR.

3. Что именно помогает обнаруживать

- Инъекции (SQL/NoSQL/command), небезопасная обработка входных данных, XSS.
- Ошибки авторизации/аутентификации, некорректные проверки прав доступа.
- Утечки секретов, небезопасная криптография и неправильное использование security API.
- Небезопасная сериализация, path traversal и другие типовые классы CWE/OWASP.

4. SAST и IaC: связка кода и инфраструктуры

Метрика	Что показывает
PR pass rate	Доля pull request без критических/высоких находок
MTTR critical	Скорость устранения критичных дефектов
Age of vulns	«Возраст» уязвимостей и динамика снижения бэклога
False positives	Качество правил и нагрузку на команды
Coverage	Покрытие репозиториев/языков/пакетов правил и долю кода под контролем

5. SAST + IaC: единый контроль кода и инфраструктуры

- Сканируйте не только приложение, но и IaC (Terraform/Helm/K8s YAML/Dockerfile) и pipeline-скрипты.
- Ищите «связанные риски»: ошибка в коде + небезопасная конфигурация (ingress/egress, права, секреты, TLS).
- Фиксируйте invariants политиками-as-code: минимальные права, запрет привилегированных контейнеров, корректные параметры логирования и т.д.

6. Критическое условие эффективности: актуальные правила и управляемый процесс

- Регулярно обновляйте движок и rulepacks; иначе новые классы уязвимостей будут пропускаться.
- Внедряйте triage и SLA: кто разбирает находки, сроки, критерии «ложно/истинно».
- Исключения — только управляемые и ограниченные по времени (time-box) с компенсирующими мерами.

Итог

SAST — базовый «механизм безопасности по умолчанию» в DevSecOps. Он снижает стоимость исправлений, повышает предсказуемость релизов и даёт руководству измеримые показатели зрелости разработки.

Обзор законодательства РК в сфере обеспечения информационной безопасности Казахстана

Обзор нормативной правовой базы информационной безопасности Казахстана:

как изменился ландшафт информационной безопасности Казахстана к концу 2025 года

Устойчивость к внешним и внутренним угрозам информационной безопасности как национальный приоритет

В условиях ускоренной информатизации и постоянно растущего ландшафта рисков и угроз информационной безопасности (ИБ) обеспечение ИБ стало приоритетной задачей государства.

Казахстан последовательно выстраивает системную архитектуру обеспечения ИБ для **защиты электронных информационных ресурсов, информационных систем** и, в особенности, критически важных объектов информационно-коммуникационной инфраструктуры (КВОИКИ).

Последние годы (2024–2025) стали периодом **интенсивной актуализации требований по обеспечению ИБ:** приняты стратегические документы и законы, направленные на укрепление устойчивости КВОИКИ, введены новые понятия и усилены меры реагирования на инциденты ИБ.

Данный обзор охватывает действующие нормативные правовые акты в сфере обеспечения ИБ по состоянию на конец 2025 года, анализируя ключевые векторы регулирования, новейшие законодательные инициативы, и сопоставляя казахстанский опыт с международными подходами.

Фундамент регулирования: ключевые законы и стратегии

1. Закон РК «Об информатизации»: введение института исследователей ИБ

Закон задает правила требования ИБ для госорганов и бизнеса. Поправки последних лет внесли в него критически важные обновления, синхронизировав казахстанское право с мировыми трендами:

- **Новый понятийный аппарат:**
  Закреплены термины «угроза ИБ», «уязвимость» и «оперативный центр информационной безопасности» (SOC).
- **Институционализация SOC:**
  Собственникам и владельцам объектов информатизации «электронного правительства» и КВОИКИ предоставлено право выбора — создавать собственный SOC или отдавать эту функцию на аутсорсинг профессиональным SOC.
- **Программа взаимодействия с исследователями ИБ (Bug Bounty)**
  Введена программа Bug Bounty, порядок функционирования которой определяет уполномоченный орган в сфере обеспечения ИБ, заводя исследователей ИБ в правовое поле.

С 18 сентября 2025 года Министерство цифрового развития, инноваций и аэрокосмической промышленности РК (МЦРИАП РК) было реорганизовано и преобразовано в Министерство искусственного интеллекта и цифрового развития РК (МИИЦР РК).

Угроза информационной безопасности

совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности

Уязвимость

недостаток объекта информатизации, использование которого может привести к нарушению целостности и (или) конфиденциальности, и (или) доступности объекта информатизации

Оперативный центр информационной безопасности (SOC)

юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации

2. Защита персональных данных: вектор на ответственность

Закон Республики Казахстан «О персональных данных и их защите», регулирующий сбор, обработку и защиту персональных данных (ПД) граждан, за последние годы был существенно усилен.

Закон обязывает собственников и операторов баз ПД получать согласие субъектов ПД на обработку их данных, обеспечивать конфиденциальность и целостность ПД, а также определяет права субъектов (граждан) на доступ к своим ПД и требования по их защите.

Изменение	Суть	Цель
Новое понятие	Введено понятие **«нарушение безопасности персональных данных»** (незаконное распространение, изменение, уничтожение, несанкционированный доступ)	Четкое определение инцидента
Обязательное уведомление	Собственники/операторы баз ПД обязаны **уведомить уполномоченный орган в течение ОДНОГО рабочего дня** с момента обнаружения безопасности ПД	Ускорение реагирования и снижение ущерба
Запрет на бумажные копии	**Запрет на сбор и хранение бумажных копий** удостоверений личности при наличии интеграции с государственными базами данных	Снижение рисков утечек и избыточного сбора данных

Стратегический вектор 2023–2029

Концепция цифровой трансформации, развития отрасли ИКТ и кибербезопасности на 2023–2029 годы (Постановление Правительства РК № 269 от 28 марта 2023 года) определяет стратегические цели. Документ фиксирует не только планы, но и конкретные метрики текущего состояния:

- **Осведомленность:**
  77,4% населения осведомлены об угрозах в области кибербезопасности.

- **Инфраструктура:**
  Функционируют 3 профильных общественных организации и 8 аккредитованных испытательных лабораторий, занимающихся испытаниями на соответствие требованиям ИБ и форензикой (расследованием инцидентов ИБ).

- **Критические объекты:**
  Определен перечень из 495 стратегических объектов с критической инфраструктурой.

- **Казнет:**
  В пространстве казахстанского сегмента Интернета зарегистрировано более 160 тысяч доменных имен .KZ и ҚАЗ, аккредитовано 12 компаний, которые занимаются регистрацией доменных имен.

- **Импортозамещение:**
  Разработаны первые отечественные средства антивирусной защиты.

- **Кадры и рынок:**
  Сформирован рынок квалифицированных услуг ИБ, увеличено количество грантов для студентов.

За период реализации Концепции были достигнуты определенные результаты в сфере обеспечения ИБ, в частности, создан рынок квалифицированных услуг ИБ, увеличены образовательные гранты по данной специальности, повышена культура ИБ, обеспечивается круглосуточный мониторинг событий ИБ объектов информатизации государственных органов и мониторинг обеспечения ИБ объектов информатизации «электронного правительства».

Актуализация законодательства
ключевые изменения 2024–2025 гг.

Период 2024–2025 годов ознаменовался оперативным обновлением законодательства в ответ на новые внешние и внутренние вызовы и угрозы ИБ с учетом лучшей мировой практики.

Закон о внесении поправок в законодательные акты по вопросам ИБ

Настоящим Законом внесен ряд существенных изменений и дополнений в некоторые законодательные акты Республики Казахстан, комплексно усилив правовую базу законодательства в сфере обеспечения ИБ:

- **Цифровые активы:**
  Введены положения о приостановлении лицензии майнинговым компаниям за несоблюдение требований ИБ.

- **Госконтроль:**
  Защита персональных данных включена в перечень сфер государственного контроля за деятельностью бизнеса. Это интегрирует требования ИБ во все секторы экономики.

Усиление ответственности и уведомлений

- **Цифровые активы:**
  Приказ МЦРИАП от августа 2024 года № 481/НҚ утвердил **Правила уведомления субъектов** о нарушении безопасности их данных. Уведомление теперь осуществляется через кабинет пользователя на веб-портале «электронного правительства» или SMS. Оператор инфраструктуры «электронного правительства» рассылает уведомления на основании данных регулятора.

- **Госконтроль:**
  С 10 января 2025 года КоАП (ст. 79) штрафы за незаконный сбор или утечку данных выросли в три раза. Для крупного бизнеса ценник за инцидент теперь варьируется от 600 до 2000 МРП, в зависимости от тяжести последствий. Это прямой финансовый **стимул инвестировать в кибергигиену.**

Первые шаги в регулировании искусственного интеллекта

17 ноября 2025 года Президент подписал второй в мире **Закон РК «Об искусственном интеллекте».**

- **Искусственный интеллект (ИИ) — это объект информатизации.** Он признан инструментом для достижения задач человека.

- **Принцип ответственности:**
  Закреплены принципы **ответственности и подконтрольности,** обязывая собственников и владельцев управлять рисками, обеспечивать безопасность и надежность систем ИИ.

- **Национальная платформа ИИ:**
  Введены законодательные **основы для создания национальной платформы ИИ,** где будут разрабатываться и обучаться модели ИИ (в том числе в безопасных «песочницах»).

В работе также находится Цифровой кодекс и отраслевой Закон «О кибербезопасности», которые должны в будущем объединить разрозненные нормы **в единую экосистему.**

Ключевые векторы госрегулирования ИБ в Казахстане

К концу 2025 года нормативная правовая база Республики Казахстан в сфере обеспечения ИБ сформировалась в разветвленную и целостную систему.

В данном обзоре рассматриваются ключевые векторы государственного контроля, иерархия нормативных правовых актов и специфика требований к КВОИКИ.

1. Единые требования

Базовым элементом регулирования остаются Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности (утверждены Постановлением Правительства РК № 832 от 20.12.2016, актуализированы в 2024 году).

Данный документ носит обязательный характер для государственных органов, государственных юридических лиц, субъектов квазигосударственного сектора, собственников и владельцев КВОИКИ. **Единые требования регламентируют необходимый перечень технических и организационных защитных мер, включая:**

- криптографическую защиту;
- разграничение прав доступа;
- антивирусную защиту;
- межсетевое экранирование;
- резервное копирование;
- защиту от утечек информации;
- управление инцидентами;
- обучение персонала;
- физическую безопасность.

Исключения из правил:

С целью исключения дублирования отраслевого регулирования, нормы Единых требований не распространяются на интернет-ресурсы и информационные системы Национального банка, а также на информационные системы в защищенном исполнении, отнесенные к государственным секретам, а также на сети телекоммуникаций специального назначения.

2. Мониторинг соответствия и лицензирование

Контроль за исполнением требований осуществляется через механизмы мониторинга и испытаний, регламентируемые следующими документами (актуализированы в 2025 году):

- **Правила мониторинга ИБ объектов «электронного правительства» и КВОИКИ**
  Приказ МОАП РК № 52/НҚ

- **Методики и правила проведения испытаний на соответствие требованиям ИБ**
  Приказ МЦРОАП РК № 111/НҚ

Криптографическая защита

Деятельность, связанная с разработкой и реализацией средств криптографической защиты информации (СКЗИ), находится под особым контролем государства. Согласно Постановлению Правительства РК № 589 (от 27.07.2015), данная сфера подлежит обязательному лицензированию Комитетом национальной безопасности (КНБ) РК.

---

3. Национальная система стандартизации

В вопросах стандартизации законодательство Казахстана демонстрирует гибкий подход, сочетающий добровольность применения с нормативной обязательностью в конкретных случаях.

Согласно Закону РК «О стандартизации», применение национальных стандартов носит в основном добровольный (рекомендательный) характер. Однако требования национального стандарта становятся обязательными при наличии прямой ссылки на него в законодательных актах.

Практика применения:

В тексте Единых требований содержатся ссылки на 22 стандарта, что делает их соблюдение обязательным на всех этапах жизненного цикла информационных систем. При этом организации вправе применять международные стандарты напрямую (при уведомлении Казстандарта).

Значительная часть базы гармонизирована с международными нормами ISO/IEC:

- **СТ РК ISO/IEC 27002-2023**
  руководство по внедрению средств управления ИБ

- **СТ РК ISO/IEC 27005-2022**
  требования к управлению рисками ИБ

4. Защита КВОИКИ

Закон РК «Об информатизации» вводит понятие **КВОИКИ.** Критерии отнесения объектов к данной категории закреплены приказом МЦРОАП № 221/НҚ от 30 июня 2023 года.

К КВОИКИ относятся системы, сбой которых влечет не только экономические потери, но и риски техногенных катастроф, угрозы обороне и жизнедеятельности населения.

В перечень входят объекты, нарушение функционирования которых может привести к чрезвычайным ситуациям, ущербу обороноспособности или экономике.

Отраслевой охват включает:

- Топливно-энергетический комплекс (тепло-, электро-, газоснабжение)
- Банковскую сферу и транспорт
- Здравоохранение и водоснабжение
- Правоохранительную деятельность и «электронное правительство»

Требования к SOC

Собственники и владельцы КВОИКИ обязаны создать и обеспечить функционирование SOC.

Законодательство предоставляет собственникам и владельцам КВОИКИ выбор модели обеспечения безопасности: создание собственного SOC или привлечение лицензированных внешних поставщиков услуг SOC.

Законодатель предусматривает две модели реализации:

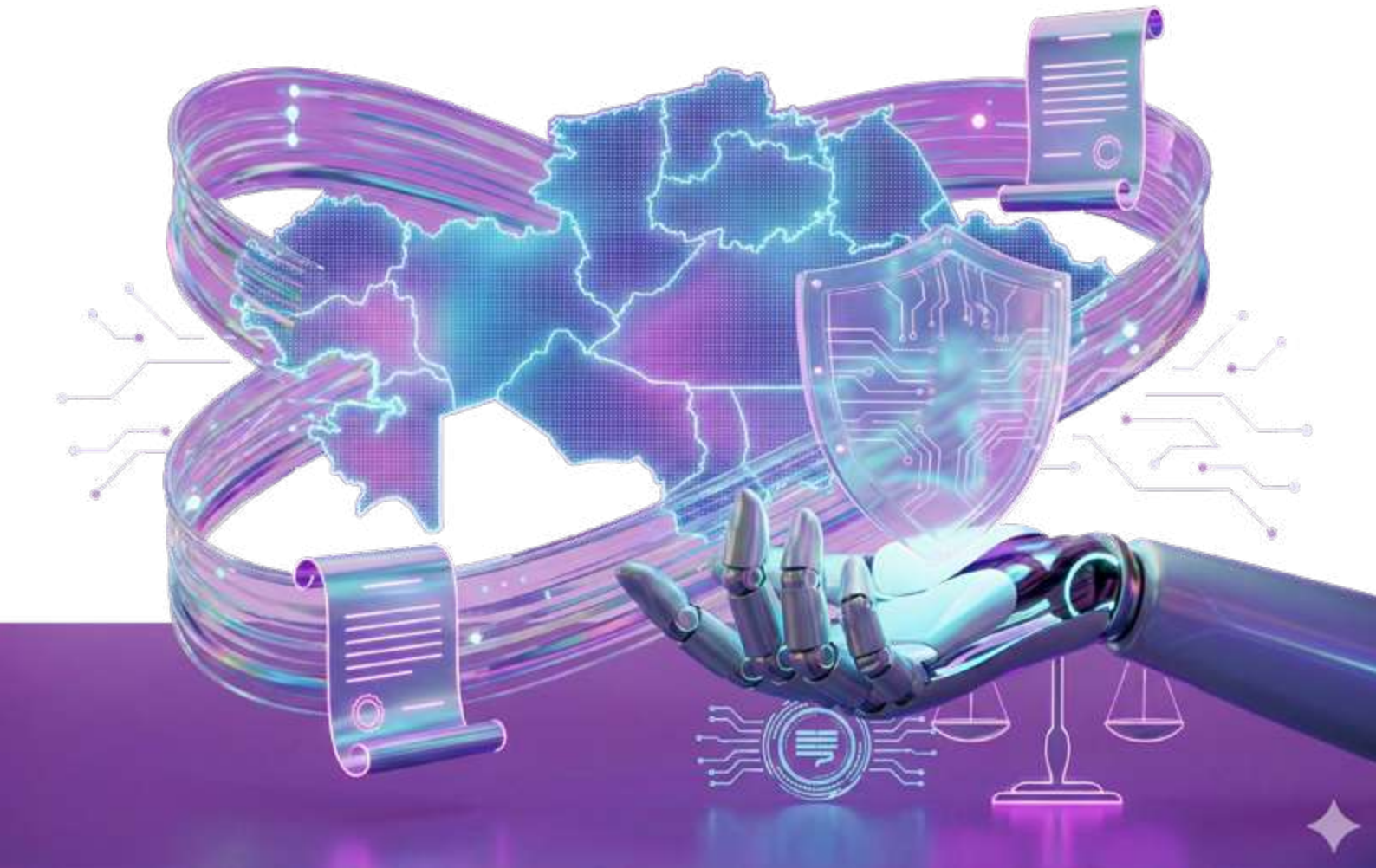
1. Создание собственного SOC.
2. Приобретение услуг SOC у третьих лиц (аутсорсинг) в рамках гражданско-правовых отношений.

В этом аспекте опыт Казахстана сопоставим с международной практикой, в частности с законодательством РФ о безопасности критической информационной инфраструктуры (КИИ), действующим с 2018 года и также предусматривающим ведение реестров и категорирование объектов.

Заключение:
в ногу со временем

К концу 2025 года нормативная правовая база Республики Казахстан в сфере обеспечения ИБ года представляет собой разветвленную систему актов – от законов и государственных концепций до детальных правил и стандартов.

За сравнительно короткий период Казахстан совершил заметный рывок в развитии законодательства в сфере обеспечения ИБ, создав основу для защиты как государственных информационных ресурсов, так и интересов граждан в цифровой среде.



Коммерческие услуги ГТС
и международное сотрудничество

- Новый вектор выхода на международный рынок кибербезопасности: международное техническое сотрудничество АО «ГТС»
- Профессиональная защита от DDoS-атак

Новый вектор выхода на международный рынок кибербезопасности:

Международное техническое сотрудничество АО «ГТС»

В феврале текущего года АО «ГТС» получило право оказывать коммерческую услугу «Международное техническое сотрудничество». Этот шаг стал важной вехой в расширении деятельности Общества за пределы Казахстана, открывая новые возможности для участия в зарубежных проектах и выстраивания устойчивых партнёрств с международными вендорами и технологическими компаниями.

Международное техническое сотрудничество позволяет АО «ГТС» реализовывать совместные проекты с зарубежными компаниями, формировать консорциумы с казахстанскими организациями для выхода на внешние рынки, а также продвигать как собственные, так и партнёрские решения в области кибербезопасности, аналитики данных и цифровой инфраструктуры.

Уже сформирован перечень услуг, готовых к практическому продвижению и реализации, включая сотрудничество с ведущими казахстанскими технологическими компаниями — MSSP Global, DataTeam и tLAB.

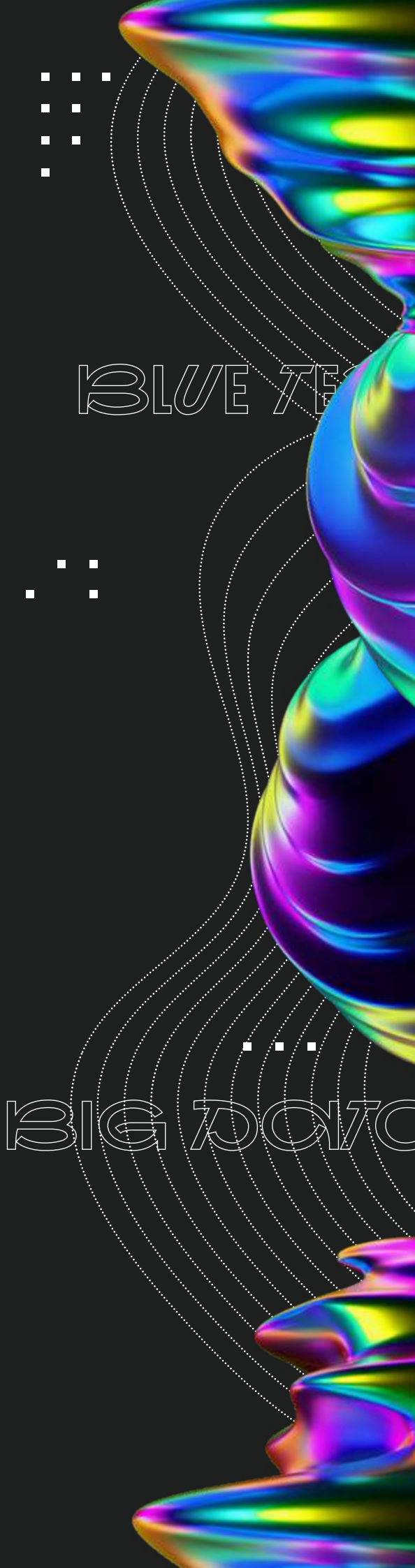
RED TEAM

Одной из ключевых услуг является **Red Team.** Она направлена на имитацию действий киберпреступников для выявления уязвимостей и оценки уровня защищённости информационных систем. В рамках услуги проводятся имитация кибератак, поиск уязвимостей в ИТ-инфраструктуре, тестирование сервисов электронного правительства и оценка состояния информационной безопасности устройств, подключённых к сети Интернет.

Дополняет её услуга **Blue Team,** обеспечивающая комплексную защиту ИТ-инфраструктуры и реагирование на инциденты информационной безопасности. Сервис включает защиту ИТ-инфраструктуры, анализ потенциально вредоносных файлов, актуализацию информации о киберугрозах и уязвимостях, а также подготовку детализированных отчётов с атрибуцией инцидентов к конкретным APT-группировкам.

Особое внимание уделяется построению **кибербезопасной национальной инфраструктуры.** Совместно с ТОО «DataTeam» (бывший KazAI) АО «ГТС» предлагает комплексные решения по защите цифрового суверенитета государств. Услуга включает консультации по построению цифровой границы, разработку и внедрение национальной инфраструктуры кибербезопасности, проведение аналитических исследований, формирование заключений и архитектурного видения проектов, обучение специалистов работе с внедряемыми системами и продуктами, разработку систем анализа сетевого трафика для выявления инцидентов, построение систем автоматического сканирования сети Интернет и обеспечение постоянной технической поддержки.

В области аналитики больших данных АО «ГТС» предлагает услугу **Big Data и Machine Learning,** также реализуемую совместно с ТОО «DataTeam». Она направлена на внедрение современных решений для работы с большими объёмами данных, включая разработку защищённых хранилищ, интеграцию данных (включая потоковые), анализ и структурирование информации, а также разработку и внедрение решений на базе технологий машинного обучения.



Для защиты от современных и сложных киберугроз, включая атаки нулевого дня и APT, предлагается продукт класса **Anti-APT Sandbox,** разработанный совместно с tLAB. Он обеспечивает обнаружение скрытых атак, анализ поведения на уровне дерева действий, отражающего цепочку вредоносной активности, и возможность подключения к различным источникам файлов в инфраструктуре заказчика.

Еще одной важной инициативой является **Cyberguard DLP,** реализуемая совместно с MSSP Global. Решение применяется в GovSOC для мониторинга рабочих станций в центральных государственных органах, обеспечивает проактивную защиту от утечек данных, анализ поведения сотрудников и документов на предмет наличия конфиденциальной информации, раннее предотвращение нарушений целостности данных, а также выявление мошеннических схем и сотрудников, нарушающих регламенты и безопасность организации.

Развитие направления международного технического сотрудничества позволяет АО «ГТС» масштабировать национальные компетенции в области кибербезопасности, выступать технологическим партнёром для зарубежных государств и организаций, формировать устойчивые международные консорциумы и продвигать казахстанские решения и экспертизу на глобальном рынке.

Сегодня АО «ГТС» позиционирует себя как экспертный и технологический партнёр, готовый к реализации сложных международных проектов в области информационной безопасности, аналитики данных и цифровой инфраструктуры.

Услуги оказываются по запросу:
info@sts.kz

Профессиональная защита от DDoS-атак

АО «ГТС» предоставляет услугу защиты интернет-ресурсов от DDoS-атак, обеспечивая стабильную работу информационных систем даже в условиях киберугроз. Решение подходит как для небольших проектов, так и для крупных предприятий, и доступно по модели ежемесячной подписки.

Основные преимущества услуги:

Гибкость и масштабируемость:
Поддержка неограниченного количества IP-адресов и возможность расширения защиты по мере роста инфраструктуры.

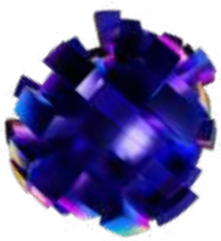
Региональная защита:
Оборудование развернуто в 18 городах и интегрировано с магистральными сетями ведущих операторов, что позволяет блокировать атаки на региональном уровне.

Локализация и конфиденциальность:
Анализ трафика осуществляется внутри страны, что соответствует требованиям Казнета и повышает безопасность данных.

Многоуровневая защита (L3-L4):
Защита на сетевом и транспортном уровнях от атак с использованием протоколов TCP, UDP, ICMP и malformed-пакетов.

Простая интеграция:
Подключение не требует изменений в сетевой топологии и передачи SSL-сертификатов, достаточно указать IP-адрес.

Интеллектуальная фильтрация трафика:
Система анализирует входящий трафик в реальном времени, блокируя только подозрительные запросы.



Автоматическая передача логов:
Информация о попытках атак передается клиенту для анализа.

Экономия ресурсов:
Нет необходимости в закупке дорогого оборудования; защита справляется с атаками мощностью до 500 Гбит/с.

Как работает система:

Моделирование нормального поведения сети:
Создается базовая модель на основе стандартных правил TCP/IP.

Анализ трафика:
Сравнение текущей сетевой активности с ожидаемым поведением.

Обнаружение аномалий:
Фиксирование любых отклонений как потенциальной угрозы.

Блокировка атак:
Автоматическая фильтрация и блокировка вредоносных пакетов.

Такая архитектура позволяет поддерживать стабильность и доступность ресурсов, обеспечивая защиту от атак разного масштаба.

Процесс технического решения по защите от DDoS-атак

- Создание модели нормального поведения в сети
- Анализ сетевого трафика для мониторинга активности
- При аномальном поведении сети фиксируется потенциальная атака
- Автоматическая блокировка трафика при фиксации атаки
- Сохранение стабильности при изменениях объема трафика

Современные подходы к обучению **кибербезопасности**

Практико-ориентированное обучение, командная работа и моделирование реальных киберугроз – ключевые элементы подготовки современных специалистов по кибербезопасности. О том, как эти принципы внедряются в образовательный процесс и приносят результат на международном уровне, рассказал в интервью архитектор кибербезопасности KZ-CERT Нурбек Тулендинов, преподаватель Astana Polytechnic College. В сентябре 2025 года его студенты стали победителями финала II Международного открытого турнира GO CTF TATARSTAN 2025.

— Вы совмещаете преподавательскую деятельность с практической работой. Почему это важно для специалиста в сфере кибербезопасности?

— Преподавательская деятельность помогает постоянно находиться в профессиональном тонусе. Взаимодействие со студентами, объяснение сложных тем и ответы на их вопросы позволяют систематизировать собственные знания и глубже осмысливать материал. Кроме того, образовательный процесс всегда двусторонний: обучая других, ты продолжаешь учиться сам.

— В чём именно проявляется этот «обратный эффект» от работы со студентами?

— Современные студенты, особенно представители поколения Z, задают нестандартные вопросы и искренне интересуются актуальными технологиями и практиками. Это мотивирует постоянно обновлять знания, осваивать новые подходы и следить за развитием отрасли. В результате преподавание становится не только передачей опыта, но и важным инструментом профессионального развития.

— Когда вы только начали преподавать, что вам было особенно интересно узнать о студентах?

— Мне было важно понять, как сами студенты воспринимают информационную безопасность: считают ли они её сложной и узкоспециализированной сферой или видят в ней перспективное и интересное направление для будущей карьеры. Это помогло выстроить образовательный процесс более осознанно.

— Как живое общение со студентами повлияло на формат обучения?

— Наблюдение за реакцией студентов и живое общение позволили сделать занятия более понятными и практико-ориентированными. Я смог адаптировать содержание курсов под уровень подготовки обучающихся и сформировать у них устойчивый интерес к вопросам кибербезопасности.

— На что вы делаете основной акцент в процессе обучения будущих специалистов?

— В первую очередь я стараюсь передавать именно те знания и навыки, которые будут востребованы в реальной профессиональной деятельности. Моя цель - не просто изложить теорию, а показать, как она применяется на практике. Поэтому значительная часть занятий посвящена разбору реальных кейсов, лабораторным работам и моделированию типовых рабочих задач.

— Вы часто говорите об индивидуальном подходе. В чём он заключается?

— Я оцениваю не только конечный результат, но и сам процесс решения задачи. Студент должен объяснить ход своих рассуждений, аргументировать принятые решения и показать глубину понимания материала. По сути, это формат мини-собеседования, который позволяет лучше понять уровень подготовки обучающегося. Такой формат развивает аналитическое мышление, навыки самопрезентации и профессионального рассуждения. Кроме того, индивидуальная работа позволяет своевременно выявлять пробелы в знаниях и при необходимости корректировать учебный процесс.

— Используете ли вы командные или соревновательные форматы обучения?

— Да, я делю студентов на 3–4 мини-группы и организую между ними соревновательные задания. Это делает занятия более динамичными и повышает интерес к предмету. Команды предлагают собственные решения, обсуждают их и аргументируют, почему их подход наиболее эффективен.

— Какую роль такие мини-соревнования играют в подготовке специалистов?

— Они развивают навыки командной работы, критического мышления и умение отстаивать свою позицию. Это важные качества для будущих специалистов по информационной безопасности, которые в реальной работе постоянно взаимодействуют с коллегами и заказчиками.

— Насколько важны игровые и интерактивные элементы в обучении зумеров?

— Они играют большую роль. Профессиональные игры, командные задания и имитация реальных рабочих ситуаций повышают вовлечённость студентов и делают процесс обучения более живым. Такой формат помогает лучше усваивать материал и развивает аналитическое мышление.

— Расскажите о внеаудиторной работе со студентами.

— В колледже ежегодно проводится CTF-соревнование, в котором участвуют все студенты. Это эффективный инструмент, позволяющий проверить знания и навыки в условиях, максимально приближённых к реальным задачам специалистов по кибербезопасности.

— Что дают студентам CTF-соревнования помимо соревновательного элемента?

— Они развивают аналитическое мышление, умение работать в команде и решать нестандартные задачи. Для студентов это не просто конкурс, а полноценный образовательный формат, который помогает глубже понять специфику профессии.

— В колледже также работает CTF-клуб. Какую роль он играет?

— CTF-клуб объединяет студентов и выпускников, обеспечивая преемственность между разными поколениями обучающихся. Это способствует формированию профессионального сообщества, где участники регулярно встречаются, решают практические задачи и обмениваются опытом.

— Как вы в целом понимаете инновации в преподавании кибербезопасности?

— Для меня инновации — это не столько новые методики, сколько правильная организация учебного процесса. Настоящая инновация заключается в том, чтобы давать студентам именно те задачи и подходы, с которыми они столкнутся в реальной работе.

— Какой подход вы считаете наиболее эффективным?

— Максимальное приближение обучения к реальным условиям: анализ практических кейсов, командная работа, обсуждение решений и аргументация выбранных подходов. Это помогает студентам заранее понимать требования профессии и значительно снижает разрыв между обучением и реальной работой.

Кибербезопасность глазами зумеров:

новые подходы и ожидания

На волне трендов о разнице в поколениях мы решили провести небольшой опрос среди 100 студентов, изучающих информационную безопасность. Цель опроса – понять, как новое поколение специалистов в кибербезопасности воспринимает эту область, какие подходы считает наиболее эффективными и что ожидает от профессии в будущем.

Кибербезопасность для представителей поколения Z – это не просто защита сетей и данных от внешних угроз. Для современных студентов и молодых специалистов это целый комплекс мер, направленных на обеспечение безопасности в быстро меняющейся цифровой среде. Их подход к этому направлению более целостный и глубокий: это постоянное обучение, адаптация к новым киберугрозам и стратегическая оборона.

На начальных этапах обучения многие студенты воспринимают кибербезопасность как что-то вроде цифрового «экшена»: они ожидают, что смогут сразу учиться взламывать системы, создавать защитные механизмы и разрабатывать код. На самом деле первые курсы направлены на создание базовых навыков - обучение программированию, понимание основ сетей и алгоритмов. Введение в кибербезопасность происходит на общих занятиях по информационным технологиям, где объясняются базовые угрозы и методы защиты.

Однако к концу учебы представление о кибербезопасности значительно расширяется. Обучение включает реальные проекты, симуляции и лабораторные работы, моделирующие современные угрозы и контрмеры. Особое внимание уделяется таким важным аспектам, как работа с цифровыми доказательствами, оценка уязвимостей и сетевые технологии. Студенты приобретают реальные навыки, востребованные на рынке труда, и начинают понимать, **что настоящая работа в кибербезопасности требует не только технических умений, но и критического мышления, навыков решения проблем и способности работать в команде.**

Современные студенты рассматривают кибербезопасность как непрерывное испытание, которое предоставляет возможности для профессионального роста и хорошего заработка. Молодые специалисты заинтересованы в постоянной борьбе с новыми угрозами и в создании инновационных решений, адаптируясь к динамичной среде киберугроз.

Ожидается, что в будущем кибербезопасность будет все больше полагаться на автоматизацию и искусственный интеллект (ИИ) для выявления и предотвращения угроз. Важным шагом в этом направлении станет развитие квантовых вычислений, которые могут поставить под угрозу существующие криптографические методы, что потребует разработки новых алгоритмов шифрования. Поколение Z видит перспективу в кибербезопасности как одной из ключевых отраслей будущего, где технические новшества будут идти рука об руку с грамотным управлением данными и конфиденциальностью.

Спрос на узкоспециализированные роли в сфере кибербезопасности будет только расти: инженеры по безопасности, специалисты по обнаружению угроз (Threat Hunters), ответственные за инциденты и тестировщики на проникновение. Важно, что работодатели ценят не только технические, но и «мягкие» навыки. Например, способность грамотно доносить технические детали до заинтересованных сторон, стратегически мыслить и понимать бизнес-процессы становится неотъемлемой частью работы.

Плюсы и минусы кибербезопасного образования

Плюсы: учебные программы, охватывающие разнообразные темы - от судебной экспертизы и реагирования на инциденты до этичного взлома, дают широкие знания. Практическое обучение через лабораторные занятия и симуляции заполняет пробел между теорией и практикой, а высокий спрос на специалистов по кибербезопасности улучшает шансы на трудоустройство.

Минусы: недостаток единых стандартов в образовательных программах затрудняет выбор оптимального курса. Некоторые программы делают акцент на конкретных инструментах вместо глубокого понимания концепций безопасности, а также недостаточно развивают навыки коммуникации и стратегического мышления.

Исходя из вышеперечисленного, подведем следующие основные тезисы:

Востребованность и хорошие перспективы дохода

Молодые специалисты в сфере информационной безопасности (ИБ) ожидают, что рынок труда будет обширным и высокооплачиваемым, учитывая высокий спрос на специалистов и рост числа угроз.

Целостный подход и постоянное развитие

Поколение Z видит кибербезопасность как комплексный процесс, который требует постоянного обучения, адаптации к новым угрозам и применения стратегических мер для обеспечения безопасности.

Автоматизация и искусственный интеллект

В будущем кибербезопасность будет все больше полагаться на автоматизированные системы и ИИ для обнаружения и предотвращения угроз. Развитие квантовых вычислений также потребует пересмотра криптографических методов.

Фокус на узкоспециализированные роли

Ожидается рост спроса на такие позиции, как инженеры по безопасности, специалисты по обнаружению угроз, ответственные за инциденты и тестировщики на проникновение.

Недостатки образовательных программ

Молодые специалисты отмечают недостаток едины стандартов в обучении и считают важным усилить подготовку в области реальных кейсов, а также развивать навыки коммуникации и стратегического мышления.

Ожидание реальных сценариев

Студенты хотели бы видеть больше практических кейсов и возможность работы с инцидентами в реальной жизни, а также стажировки и практику, организованные в сотрудничестве с бизнесом.

Современные студенты хотели бы видеть больше реальных сценариев в процессе обучения: кейс-стадии и случаи управления инцидентами. Также важно улучшить подготовку в области мягких навыков, обучая студентов координации, взаимодействию и согласованию целей безопасности с бизнес-задачами.

Таким образом, кибербезопасность для поколения Z - это не просто защита от вирусов и кибератак, а целая экосистема, требующая всестороннего подхода и постоянного развития.

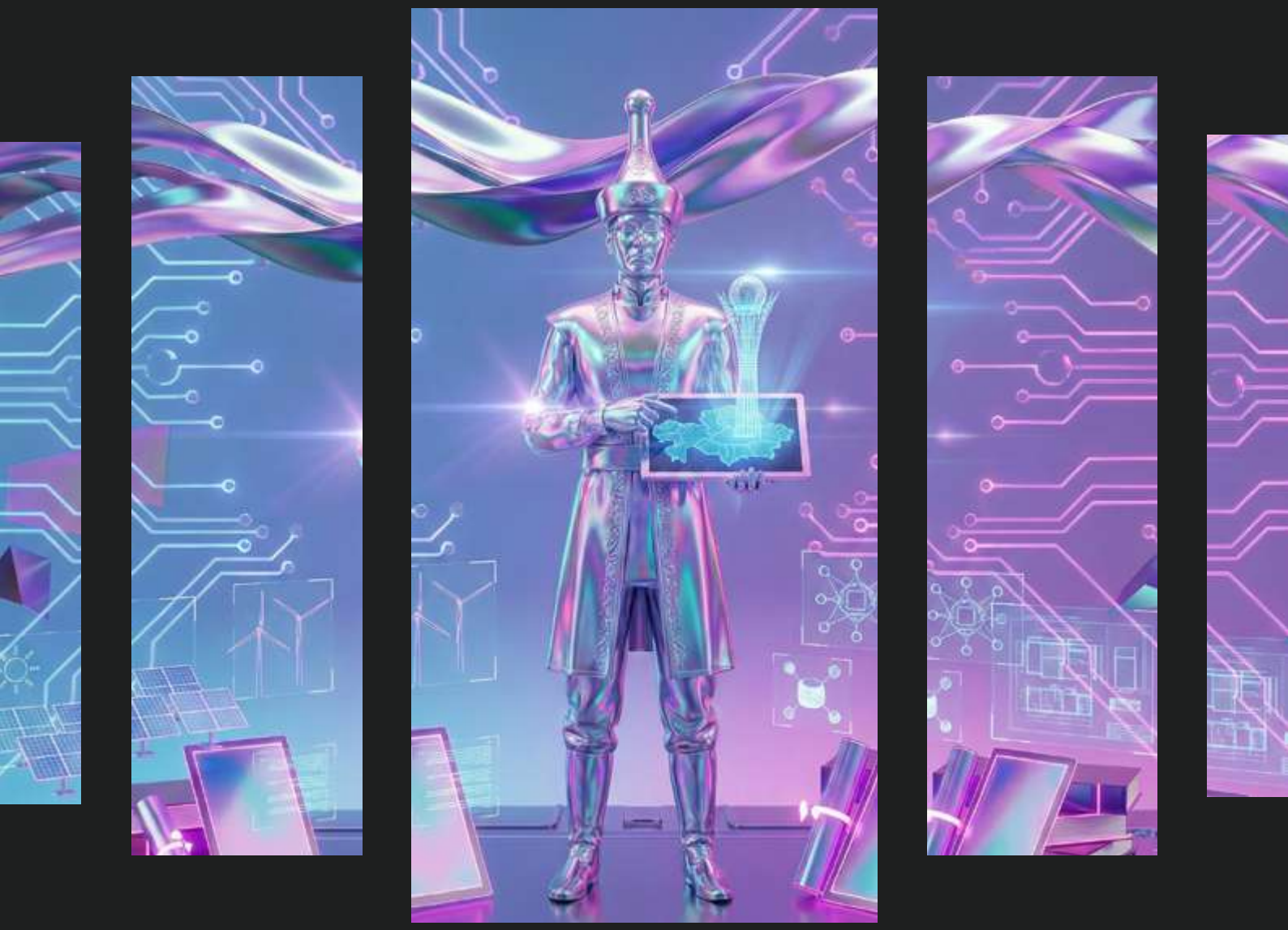
Киберустойчивость будущего:

проактивная защита и риски критической инфраструктуры

Threat Hunting 2.0: как мы перестаем ждать атаки и выходим на охоту

Риск-прогноз для КВОИКИ: приоритетные направления защиты

Чек-лист зрелости ИБ



Threat Hunting 2.0: как мы перестаем ждать атаки и выходим на охоту

Threat Hunting – далее TH

Threat Hunting – это проактивный процесс поиска скрытых атак и компрометаций в инфраструктуре. Мониторинг SOC строится вокруг алертов, а Threat Hunting *(далее – TH)* нацелен на поиск невидимых или слабо заметных признаков активности злоумышленников. TH в АО «ГТС» занимаются работники направления поиска угроз в составе Центра исследования вредоносного кода.

Современные APT группировки, с целью обхода средств защиты информации часто используют различные техники, где применяются легитимные пути и/или доверенное, но уязвимое ПО. Таким образом, детектирование «продвинутых» угроз возможно только с помощью TH.

У TH есть свои особенности, которые определяют его ценность и эффективность. Отличие TH от SOC-мониторинга:

SOC-аналитик

реагирует на алерты (SIEM/EDR/NDR)

Threat Hunter

исследует инфраструктуру без привязки к сработкам, опираясь на гипотезы, TTP злоумышленников и аномалии. Итог охоты – новые правила корреляции, индикаторы компрометации (IoC) и сценарии, которые затем можно автоматизировать и передать в SOC для того, чтобы в будущем SOC детектировал поведение сложной угрозы самостоятельно

Основная особенность ТН – постановка и проверка гипотез, к примеру:

1

«Если в инфраструктуре есть злоумышленник, использующий CobaltStrike, он, вероятно, будет применять named pipe для коммуникации. Проверим аномальные именованные каналы в системе».

2

«APT-группировки, работающие в регионе, используют легитимные админ-инструменты (Living off the Land). Проверим, кто запускал rundll32.exe с нестандартными параметрами».

Рис. 1. Схема запуска подозрительного процесса

В данном случае (рис. 1), родителем легитимного rundll32.exe является WMI Provider host (Wmiprvse.exe).

Однако, цепочка является подозрительной, так как стартовые параметры rundll32.exe содержат отсылку к подозрительной динамической библиотеке C:\ProgramData\malware.dll.

Таким образом, можно предположить, что злоумышленники, воспользовавшись удаленным WMI запустили вредоносную динамическую библиотеку на рабочей станции.

ТН в данном случае, посредством EDR, скачает данный файл с конечной точки и передаст на исследование работникам направления исследования вредоносного кода.

Рис. 2. Зловредная активность, обнаруженная Quantum EDR

На рис. 2 обнаруженная активность злоумышленников с помощью Quantum EDR в инфраструктуре одного из государственных органов Республики Казахстан.

На скриншоте видно, что родительским процессом, создавшим файл art.jse в C:\Users\public, является легитимный Microsoft Word (winword.exe). Данная активность была обнаружена по аномальной активности процесса winword.exe.

На первой стадии вредоносные документы содержали макрос, выполняющийся при открытии файла. Макрос сохранял свою копию в виде шаблона .dotm в папку автозагрузки приложения Microsoft Word (Application. StartupPath).

Шаблон получал уникальное имя (на основе времени и переменной docid) и сохранялся вместе с макросом, обеспечивая скрытое и автоматическое выполнение кода при каждом запуске Microsoft Word, так реализуется механизм закрепления (persistence) в системе.

То есть при открытии любого документа пользователем будет подгружаться вредоносный макрос. Данная цепочка не детектируется антивирусными средствами, так как Microsoft Word в списке доверенного ПО.

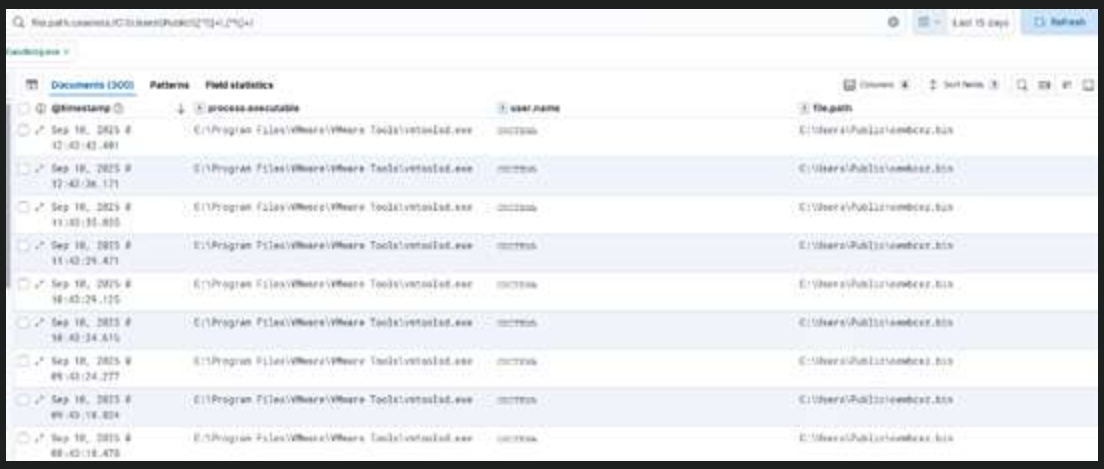


Рис. 3. Создание файла зараженным процессом vmtoolsd.exe.

DLL Side-Loading

- это метод атаки, при котором злоумышленник помещает вредоносную DLL в место, откуда доверенное приложение Windows по ошибке загружает её вместо легитимной библиотеки.

На рис. 3 посредством Quantum EDR обнаружено создание файла oewbcxz.bin легитимным, но зараженным процессом vmtoolsd.exe от имени системы.

ТН первоначально был снят дамп памяти процесса, в строках которого был обнаружен ряд динамических библиотек, подмененных злоумышленниками для закрепления на зараженном устройстве.

Злоумышленники, осознавая, что команда кибербезопасности не может заблокировать работу легитимного процесса vmtoolsd.exe, использовали DLL Side-Loading.

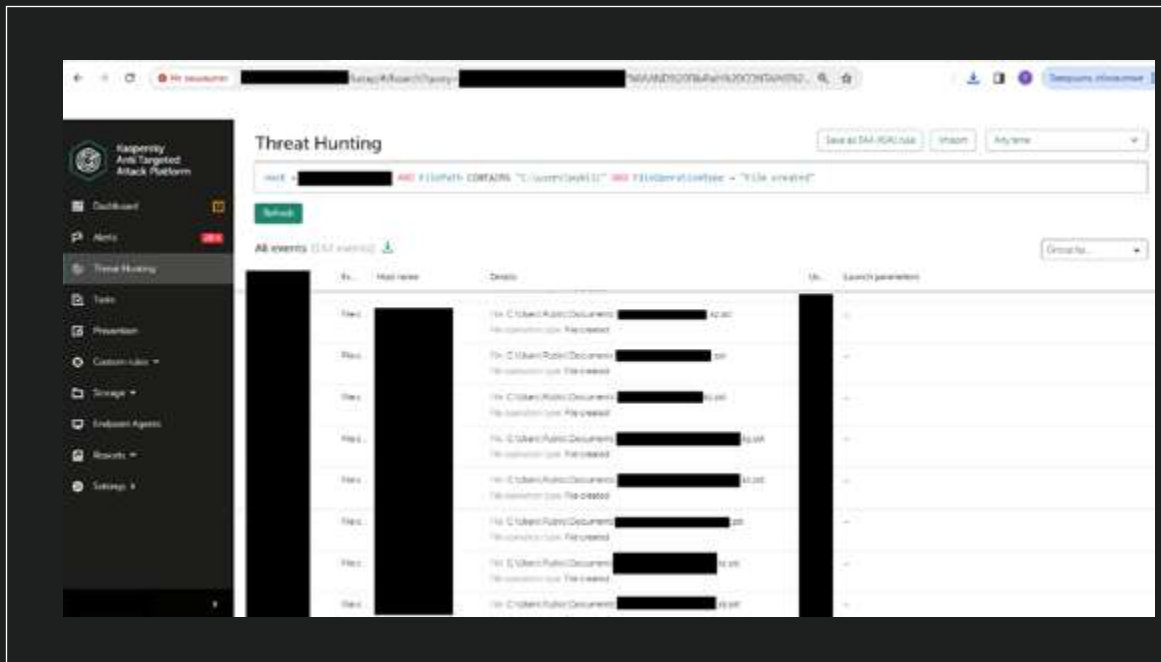


Рис. 3. Создание файла зараженным процессом vmtoolsd.exe.

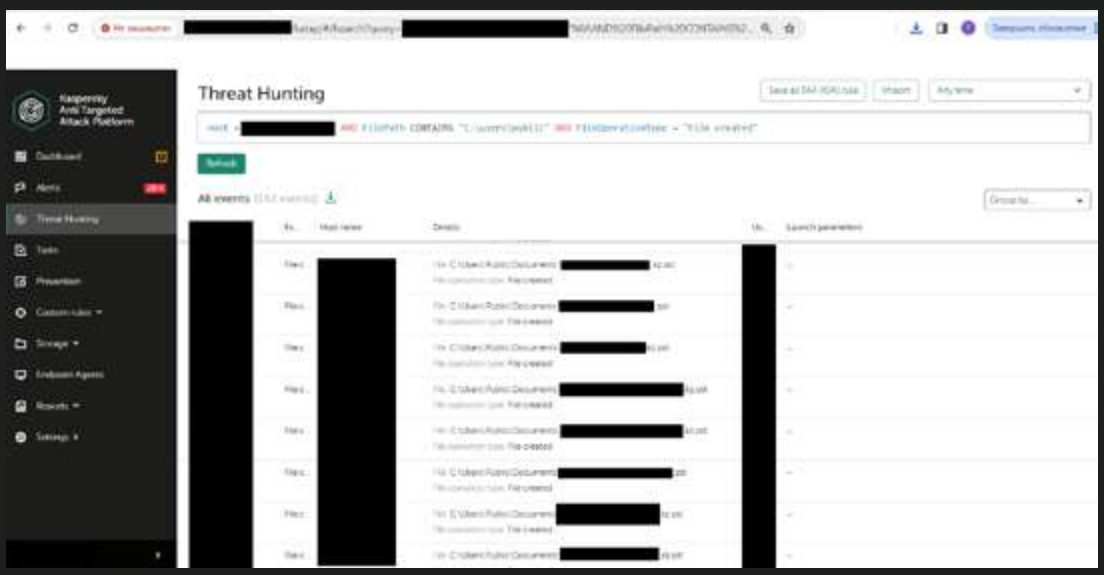


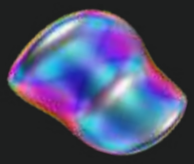
Рис. 5 архивация украденных писем

На рис. 4 и 5 видно, как злоумышленники на зараженном почтовом сервере, используя PlugX бэкдор googleup.exe, tmdbglog.dll и легитимную службу экспорта писем MSExchangeReplicationService, экспортировали архив писем .pst с различных почтовых адресов зараженного Microsoft Exchange в папку C:\Users\Public\Documents*.

После нелегитимного экспорта писем злоумышленники, используя легитимный rar.exe (архиватор WinRAR для командной строки), заархивировали украденные данные и впоследствии эксфильтровали их посредством бэкдора.

Вышеуказанная активность злоумышленников обнаружена работниками центра исследования вредоносного кода, для поиска которой использовались инструменты класса EDR/XDR, SIEM, NDR, NGFW, MailGateway, IDS/IPS систем.

Основополагающим фактором для выявления аномальной активности является высокая компетенция работников и собственные детектирующие правила, которые формировались на основании активностей злоумышленников в различных организация и государственных органах Республики Казахстан.



TH часто завязан на матрице MITRE ATT&CK. Выбирается техника (например, T1059 – Command and Scripting Interpreter), строится гипотеза, как злоумышленники могли её применить, проверяются артефакты (логи PowerShell, командные строки, процессы).

MITRE ATT&CK становится навигационной картой для построения систематических сценариев Threat Hunting.

Эффективность TH определяется качеством телеметрии.

Ключевые источники: EDR/AV (процессы, команды, загрузки модулей), windows Event Logs / Sysmon (создание служб, сетевые соединения, модификация реестра, создание исполняемых файлов в несвойственных директориях), SIEM, IDS/IPS.

Стоит отметить, что TH поиска могут использовать любые доступные источники в зависимости от инфраструктуры и вида атаки (средства защиты информации, журналы регистрации событий ОС, ППО, веб приложений, межсетевых экранов и т.д.).

Результат работы TH:

1. Обнаружение ранее незамеченной активности.
2. Создание новых правил и плейбуков для SOC.
3. Обогащение Threat Intelligence (собственные IoC, TTP).
4. Повышение уровня готовности к APT.

TH лучше всего осуществлять с TTP злоумышленников, а не с IOC, использовать базовые линии нормального поведения для выявления аномалий, делать ретроспективный анализ логов, интегрировать охоту с Threat Intelligence (APT-группы региона, новые инструменты, zero-day).

Для специалиста по Threat Hunting критически важно непрерывно отслеживать актуальный ландшафт угроз

Изучать отчёты ведущих мировых лабораторий, совершенствовать знания посредством постоянного обучения и обмена опытом с профильными специалистами. Документировать процесс в Hunting Journal и/или IRP (что искали, что нашли, какие правила добавили).

Проактивный поиск угроз

— это работа на опережение: методика предполагает целенаправленный поиск скрытой вредоносной активности в инфраструктуре, не дожидаясь явных сигналов о вторжении.

Вместо того, чтобы ждать срабатывания автоматических средств защиты, специалисты выдвигают и проверяют гипотезы о возможных угрозах, чтобы обнаружить сложные атаки и компрометации, которые могли ускользнуть от стандартных решений безопасности.

Риск-прогноз для КВОИКИ: приоритетные направления защиты

В условиях роста цифровой зависимости и повышения требований к обеспечению технологической устойчивости особое значение приобретает надёжность критически важных объектов информационно-коммуникационной инфраструктуры.

На этих площадках сходится ответственность за бесперебойность процессов, общественную безопасность и стабильность ключевых отраслей экономики. Соответственно, уровень тревожности в отношении их защищённости закономерно сохраняется повышенным.

КВОИКИ

критически важные объекты информационно-коммуникационной инфраструктуры

107

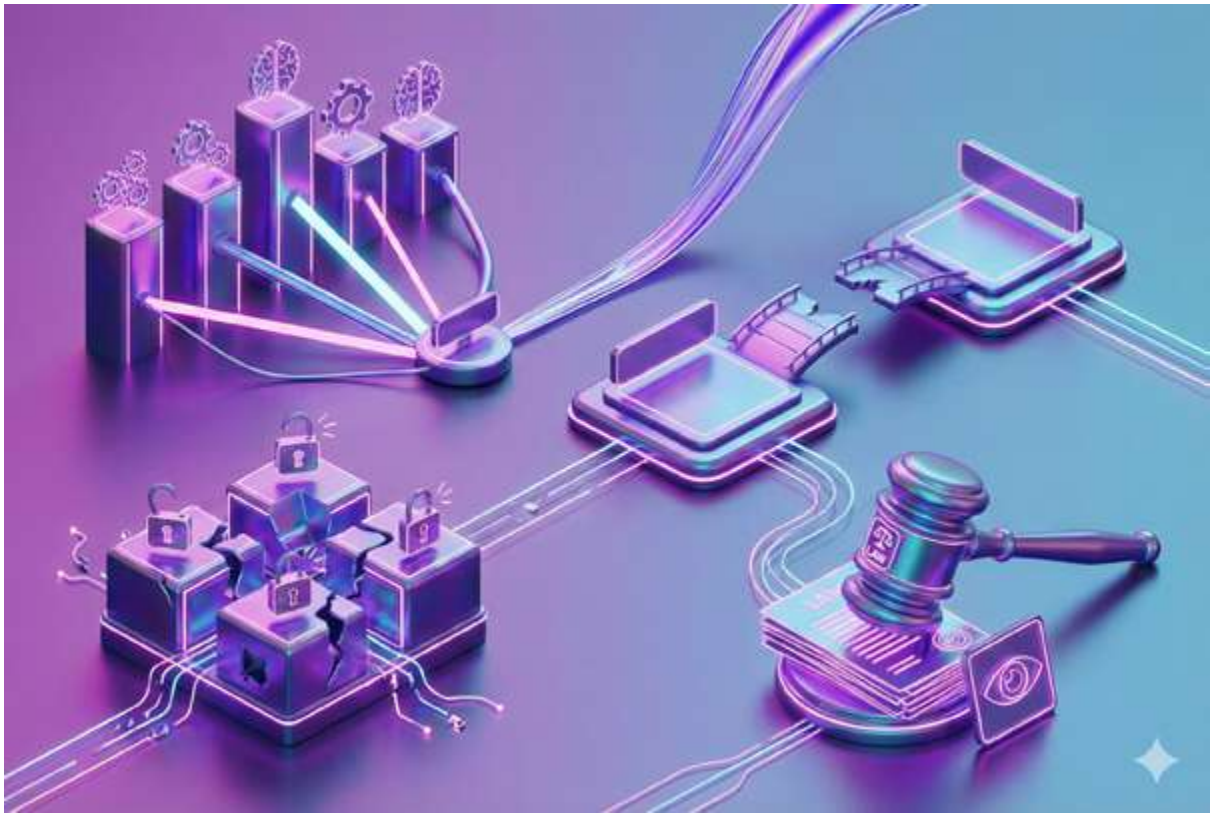
Текущая картина рисков

Проведённые профильные учения и аналитика отрасли демонстрируют неоднородность зрелости систем информационной безопасности среди операторов КВОИКИ. Наблюдаются значимые различия в готовности команд к выявлению и сдерживанию современных киберугроз.

Это формирует серию уязвимостей:

- **Различный уровень компетенций ОЦИБ,** что напрямую влияет на скорость и качество реагирования;
- **Инфраструктурные и конфигурационные уязвимости,** сохраняющиеся из-за нерегулярного или формального тестирования;
- **Операционные разрывы в ответственности,** когда меры ИБ распределены между внутренними командами и подрядными организациями;
- **Усиление регуляторного давления,** создающее дополнительные требования к аудитам, мониторингу и отчётности.

В совокупности эти факторы формируют зону повышенной тревожности, требующую системного подхода.



Где требуется усиление подготовки

Анализ тенденций указывает на несколько направлений, где повышенная концентрация усилий является наиболее актуальной:

1. **Укрепление ОЦИБ**

   Ключевой задачей становится повышение зрелости процессов, регулярность Red/Blue-учений и формирование единого корпоративного подхода к реагированию.

2. **Непрерывный аудит уязвимостей**

   Ожидается рост требований к глубине и периодичности контроля: от регулярных пентестов до автоматизированного мониторинга конфигураций и исходного кода.

3. **Развитие кадровых компетенций**

   Подготовка специалистов, усиление аналитических функций и закрепление ответственных за устойчивость ИБ внутри каждого объекта становятся критически важными элементами.

4. **Повышение управленческой ответственности**

   На первый план выходят механизмы отчётности, контроль выполнения мероприятий по устранению нарушений и соблюдение регуляторных требований в установленные сроки.

5. **Готовность к кризисным сценариям**

   Особое внимание должно уделяться отработке сценариев масштабных инцидентов, процессам эскалации и взаимодействию с государственными центрами реагирования.

Вывод

Сектор КВОИКИ остаётся в зоне особого внимания как регуляторов, так и самих операторов инфраструктуры. При этом уровень рисков не уменьшается, а смещается в сторону более сложных и системных угроз. Усиление готовности — от тестирования и аналитики до кадровой устойчивости и управленческого контроля — становится ключевым условием поддержания национальной цифровой стабильности.

Комплексная работа в обозначенных направлениях позволит снизить неопределённость, укрепить технологическую надёжность и обеспечить устойчивость критически важных объектов в долгосрочной перспективе.

Чек-лист зрелости ИБ

1. Логирование и аудит

- Определить перечень систем и приложений, с которых должны собираться логи безопасности.
- Включить расширенное логирование ключевых событий (аутентификация, изменения прав, системные ошибки, действия администраторов).
- Настроить централизованный сбор логов (syslog, агенты, шина логов, SIEM).
- Установить регламенты ротации и безопасного хранения логов.
- Проводить регулярную проверку полноты и целостности логов.
- Выполнять регулярный анализ логов (еженедельно/ежемесячно).

2. SIEM / SOC-готовность

- Определить приоритетные источники для интеграции с SIEM (AD, серверы, FW, DLP, EDR, базы данных).
- Настроить оповещения по критическим событиям (подбор пароля, изменения в AD, отключение защиты, сетевые аномалии).
- Разработать базовый набор корреляционных правил.
- Определить порядок эскалации инцидентов и каналы реагирования (почта, мессенджеры, тикет-система).
- Обеспечить круглосуточный мониторинг (внутренний SOC или аутсорсинг).
- Подготовить playbook’и реагирования на типовые инциденты.

3. IAM — управление учетными записями и правами

- Обеспечить централизованное управление учетными записями (AD/LDAP).
- Применять принцип минимально необходимых привилегий.
- Настроить многофакторную аутентификацию для критически важных систем.
- Проводить регулярный пересмотр прав сотрудников и администраторов.
- Автоматизировать отключение доступа при увольнении сотрудников.
- Использовать ролевую модель доступа (RBAC).
- Вести журналирование действий привилегированных пользователей.

4. Инвентаризация ИТ-активов

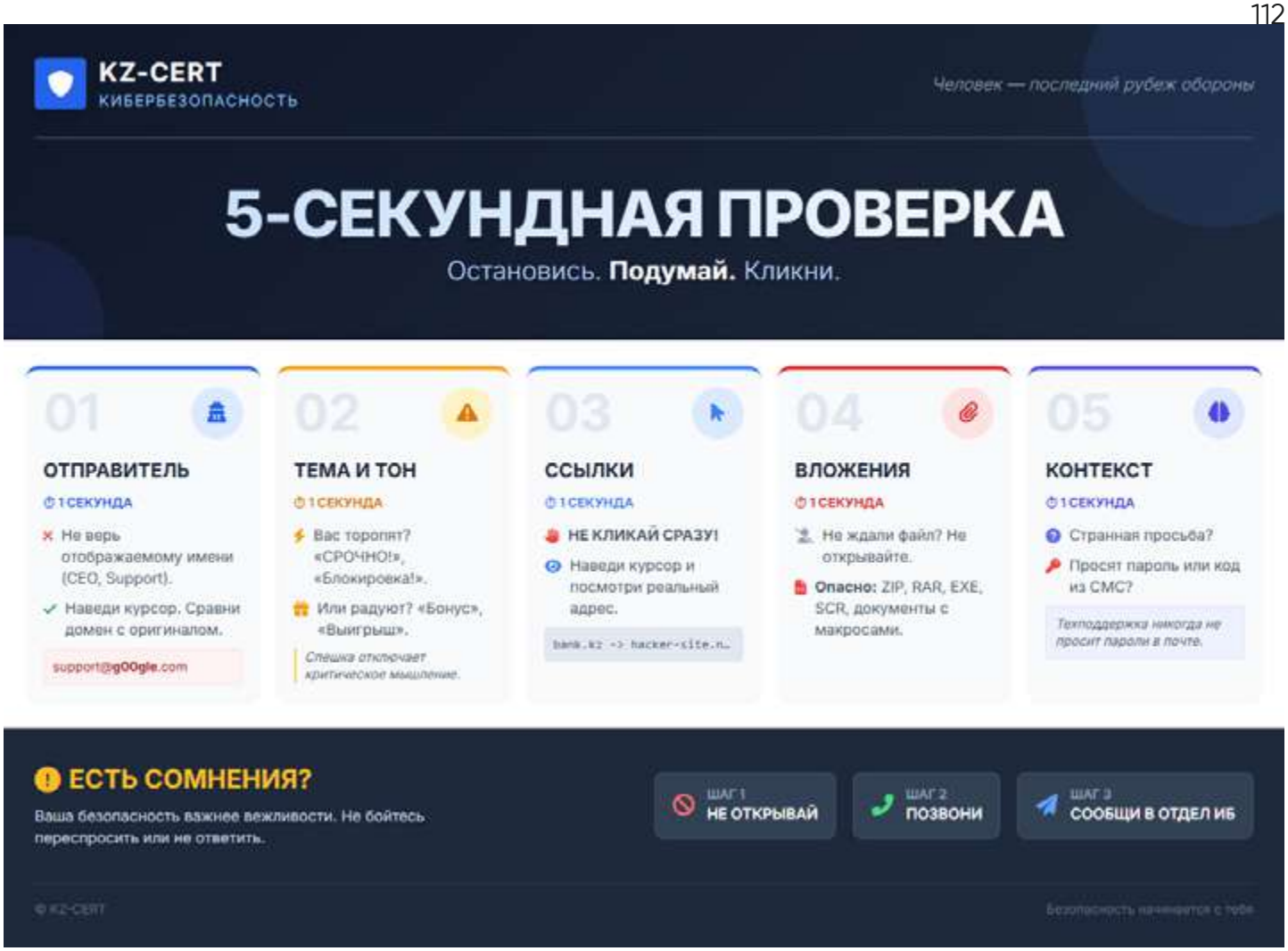
- Создать и поддерживать актуальный реестр серверов, рабочих станций, сетевых устройств, виртуальных машин, ПО и сервисов.
- Назначить владельцев каждого актива.
- Определить критичность активов для бизнеса
- Внедрить автоматизированные средства инвентаризации.
- Обновлять данные инвентаризации не реже одного раза в месяц.
- Учитывать активы при оценке рисков и формировании требований ИБ.

5. Антифрод-контроль

- Настроить мониторинг аномальной активности пользователей или клиентов.
- Разработать правила выявления подозрительных операций.
- Интегрировать антифрод-систему с SIEM, логированием и IAM.
- Определить процесс расследования подозрительных операций.
- Настроить защиту от автоматизированных атак (боты, брутфорс).
- Проводить периодическую оценку качества антифрод-правил и уровня ложных срабатываний.

6. Каналы реагирования на инциденты

- Определить ответственных за реагирование на ИБ-инциденты.
- Создать выделенный канал для экстренных ИБ-сообщений (почта, чат, hotline).
- Установить SLA на обработку, классификацию и устранение инцидентов
- Обеспечить документирование всех инцидентов и ведение истории.
- Проводить регулярные тренировки по реагированию.
- Организовать взаимодействие с государственными CERT/CSIRT при необходимости.



Telegram-бот

KZ_CERT_chat_bot

Круглосуточный call-центр

1400

incident@cert.gov.kz

info@sts.kz

Контакты:

STS.KZ

team@cert.gov.kz

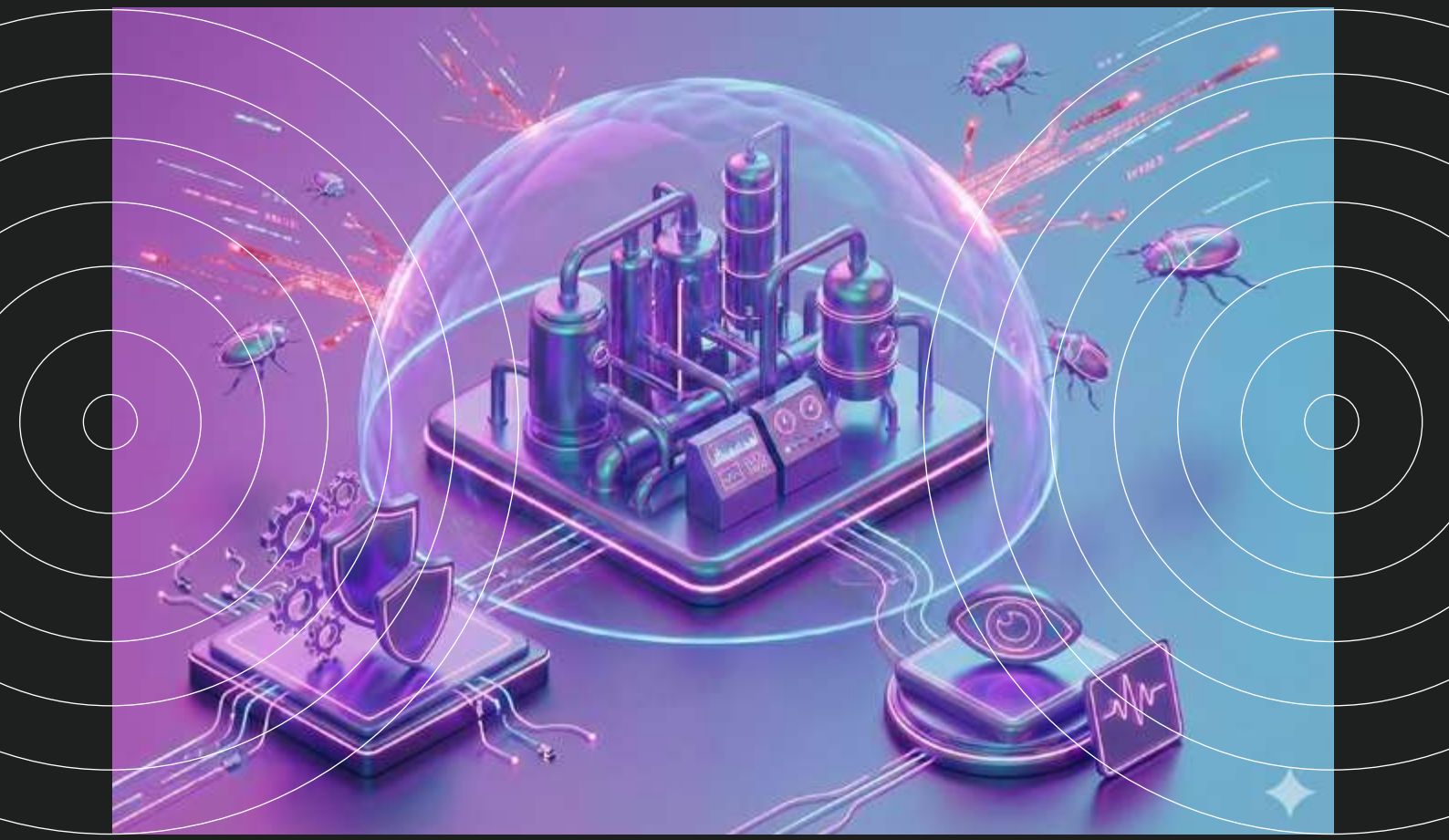
Сообщить об инциденте ИБ

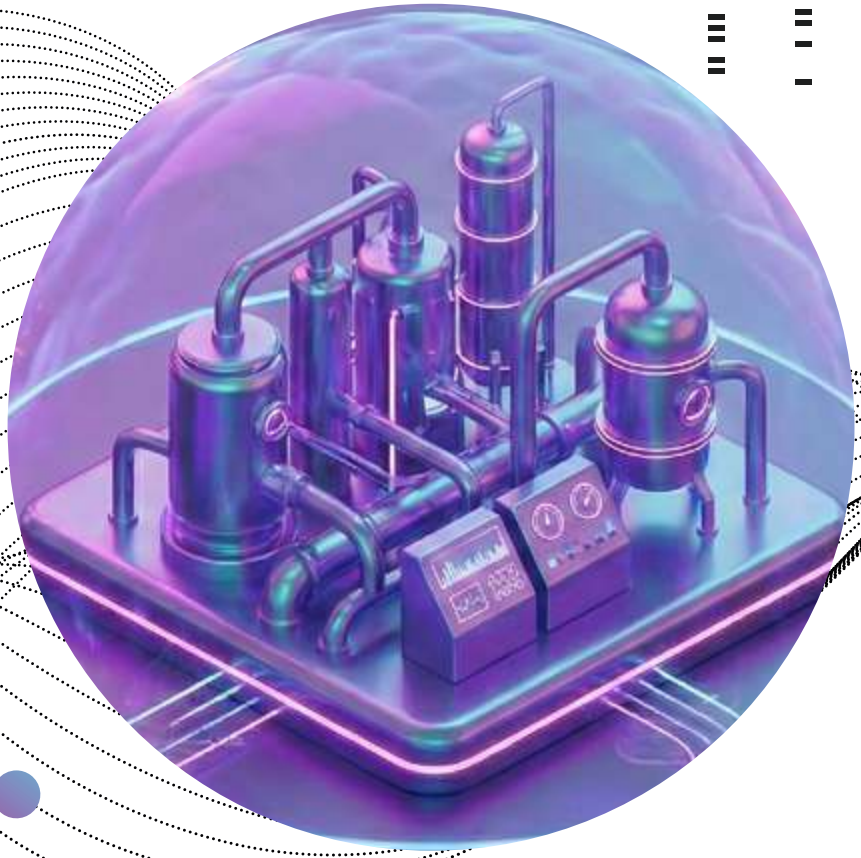
cert.gov.kz

АСУ ТП и критическая инфраструктура:

защита, которая не может упасть

- АСУ ТП и критическая инфраструктура: защита, которая не может упасть
- Уязвимости гигантов: двойной удар по безопасности АСУ ТП
- Атаки, которые идут в глубину





АСУ ТП и критическая инфраструктура:

защита, которая не может упасть

АСУ ТП играют ключевую роль в бесперебойной работе объектов критической инфраструктуры Казахстана – от энергетики и нефтегаза до транспорта, ЖКХ и медицины. При этом их сложность и взаимосвязанность делают такие системы привлекательной мишенью для киберпреступников: при росте зависимости от автоматизации увеличивается и риск эксплуатации уязвимостей.

По оценкам экспертов, в оборудовании ведущих мировых производителей (Siemens, Schneider Electric, Rockwell, ABB и др.) за последние месяцы были обнаружены десятки новых критических уязвимостей. Злоумышленники, получив доступ через эти дыры, могут остановить промышленные процессы, вызвать сбои в энергоснабжении и нарушить работу городских инфраструктур.

АСУ ТП

автоматизированные системы управления технологическими процессами

Основные выявленные уязвимости

В числе наиболее серьёзных уязвимостей – как уязвимости удалённого исполнения кода (RCE), так и обхода аутентификации и слияния прав.

Так, Siemens зафиксировал критическую уязвимость CVE-2025-40804 (CVSS 9.3) в системе SIMATIC Virtualization as a Service: злоумышленник может получить или изменить конфиденциальные данные без авторизации. Ранее в первом квартале 2025 года была выявлена уязвимость CVE-2024-56336 (CVSS 9.5) в серво-приводах Sinamics S200, позволяющая внедрять вредоносную прошивку и полностью компрометировать оборудование.

Schneider Electric устранила несколько уязвимостей в системах EcoStruxure Power Monitoring и контроллерах Modicon (модули M340 и BMENOR2200H), которые могли привести к утечке данных или отказу оборудования.

Rockwell Automation исправила критические уязвимости в своих платформах ControlLogix Ethernet и FactoryTalk: например, CVE-2025-9161 в FactoryTalk Optix позволяла загружать вредоносные плагины через MQTT.

В продуктах ABB (ASPECT, Nexus, Matrix) были найдены уязвимости обхода аутентификации и RCE с оценками CVSS до 9.8.

Многие из этих проблем уже покрываются патчами – однако совокупность уязвимостей остаётся серьёзной угрозой.

Рекомендации по защите и обеспечению отказоустойчивости

Реактивный подход, основанный на установке патчей только после выявленного инцидента, уже не обеспечивает достаточного уровня безопасности для объектов критической инфраструктуры. Для предотвращения сбоев и минимизации рисков необходима устойчивая, «resilient» архитектура, предполагающая заблаговременное выявление уязвимостей, их приоритетное устранение и применение компенсирующих мер в случаях, когда обновления недоступны.

Такой подход позволяет поддерживать непрерывность технологических процессов и снижать вероятность успешной эксплуатации уязвимостей. Организации должны приоритетно устранять обнаруженные уязвимости и, где обновление невозможно, применять компенсирующие меры. Быстрое применение исправлений и проактивный мониторинг важны для минимизации рисков.

- **Управление обновлениями:**

  Вести реестр устройств и ПО, фиксируя версии и известные проблемы. Перед установкой патча проводить тесты в изолированной среде, оценивать влияние на технологический процесс. Если обновление недоступно – использовать виртуальный патчинг или отключать неиспользуемые сервисы (FTP, Redis, web-debug и др.) вплоть до полного обновления. Регулярно проверять бюллетени производителей (Siemens, Schneider, ABB, Rockwell и др.) и CISA/ICS-CERT.

- **Сегментация сети:**

  Разделять сеть по уровням (офисная сеть, DMZ, SCADA/SCADA-серверы, контроллеры, полевой уровень) по модели Purdue. Исключить прямой доступ контроллеров к интернету. Для обмена между сегментами использовать jump-серверы и data diode. Внедрять принципы «минимальных прав» и многофакторную аутентификацию на все доступы. Ограничивать по спискам нужные протоколы и порты (CIP, Modbus/TCP, Profinet, OPC UA и др.), закрывая всё лишнее.

- **Мониторинг и обнаружение аномалий:**

  Разворачивать специализированные системы OT-мониторинга (OT – Operational Technology) и интегрировать их с общим SOC/SIEM. Контролировать целостность конфигураций PLC (Programmable Logic Controller) и SCADA, записывать контрольные суммы. Использовать Threat Intelligence для своевременного выявления новых атак по CVE и сигнатурам. Настроить детектирование подозрительного поведения (нетипичные FTP-команды, неожиданный доступ к Redis, множественные неудачные авторизации и пр.).

- **Реагирование и обучение:**

  Обновить планы реагирования на сценарии атаки (DDoS, компрометация PLC, отключение датчиков и т.п.) с учётом специфики производства. Регулярно проводить учения по реальным сценариям атак, оттачивая взаимодействие IT- и OT-персонала. Обучать инженеров и операторов распознавать фишинговые письма, социальную инженерию и признаки взлома. После каждого инцидента проводить постфактум-разбор и вносить правки в политику безопасности.

- **Защита устаревших систем:**

  Внедрять белые списки приложений (Application Whitelisting) на контроллерах и промышленных ПК. Строго контролировать и логировать использование USB-накопителей и других внешних носителей – перед использованием проверять их антивирусом. Жёстко ограничивать и мониторить удалённый доступ (VPN/TACACS+ с MFA). Если устаревшее оборудование не поддерживает обновления, рекомендуется полностью изолировать его от сети предприятия (например, поместить в демилитаризованную зону) либо заменить на современные аналоги.

Применение перечисленных мер с опорой на принципы «Zero Trust» и постоянный мониторинг создаёт многослойную защиту и повышает отказоустойчивость АСУ ТП. Только такой комплексный подход позволит минимизировать вероятность эксплуатации уязвимостей и сохранить непрерывность работы критических систем Казахстана даже при появлении новых киберугроз.

Уязвимости гигантов:
двойной удар по безопасности АСУ ТП

В современном мире устойчивость критической инфраструктуры напрямую зависит от надежности автоматизированных систем управления технологическими процессами (АСУ ТП). Энергетика, нефтегазовая отрасль, транспорт и промышленное производство — все эти сферы опираются на решения Siemens, Schneider Electric, Rockwell Automation, ABB и других производителей. Их системы обеспечивают бесперебойную работу объектов, однако именно сложность и взаимосвязанность делают их уязвимыми к кибератакам. В текущем году ведущие мировые компании сообщили о многочисленных критических уязвимостях в своих продуктах.

Среди них:

- **Siemens:**

Более 30 обновлений безопасности, включая CVE-2025-40804 (CVSS 9.3) для SIMATIC Virtualization as a Service и уязвимости в RTLS Locating Manager, Simotion и Industrial Edge.

Риски: удалённый доступ к инженерным станциям, сбои PCS7 и WinCC, подмена конфигураций контроллеров.

- **Siemens Sinamics S200 серво-приводы**

CVE-2024-56336, критическая уязвимость загрузчика прошивки (CVSS 9.5).
Рекомендации: настройка защищённой среды и соблюдение руководств по промышленной безопасности.

- **Schneider Electric:**

Критические уязвимости в EcoStruxure Power Monitoring, Modicon M340 и инструментах Software Update.

Риски: искажение данных мониторинга, подготовка атак на критическую инфраструктуру.

- **Schneider Electric System Monitor промышленные ПК**

Раскрытие учетных данных (CVSS 9.8).
Рекомендации: отключение неиспользуемых сервисов, сегментация сети, блокировка неавторизованного доступа.

- **Schneider Electric PLC Modicon M580**

CVE-2024-11425, DoS через некорректный буфер (CVSS 8.7).
Рекомендации: обновление прошивки и ограничение сетевого доступа.

- **Rockwell Automation:**

CVE-2025-7353 (CVSS 9.3) в ControlLogix Ethernet, CVE-2025-9364 в FactoryTalk Analytics LogixAI, CVE-2025-9161 в FactoryTalk Optix.

Риски: полный захват контроллеров, компрометация аналитических платформ.

- **Rockwell Automation FactoryTalk AssetCentre**

CVE-2025-0477, недостаточная криптографическая защита (CVSS 9.3).
Рекомендации: обновление до версии 15.00.01, ограничение доступа к базе данных.

- **ABB:**

Критические уязвимости в ASPECT, Nexus и Matrix с CVSS до 9.8.

Риски: удалённый захват управления и компрометация промышленных систем.

Анализ выявляет рост комплексных атак, когда злоумышленники используют сразу несколько уязвимостей.

«Реактивная» установка патчей после инцидента уже неэффективна — необходимо строить устойчивую архитектуру.

Особенности казахстанского сегмента

Мониторинг показал открытые IP-адреса с доступом по протоколам **Modbus (порт 502) и IEC 60870-5-104 (порт 2404).** Эти протоколы широко используются в АСУ ТП и критической инфраструктуре, но лишены встроенных механизмов безопасности, что делает их мишенью для атак MITM, подмены сообщений и DDoS. Открытые порты позволяют злоумышленникам вмешиваться в управление объектами, что может привести к отключению энергосетей или остановке производственных процессов.

Принципы защиты

Устойчивость АСУ ТП обеспечивается сочетанием организационных и технических мер:

1. **Управление обновлениями:**

вести реестр устройств, тестировать патчи в изолированной среде, применять виртуальный патчинг.

2. **Сегментация сети:**

деление на офисную часть, DMZ, SCADA, контроллеры и поле; исключение прямого интернет-доступа; использование jump-серверов и data diode.

3. **Мониторинг и обнаружение угроз:**

специализированный OT-мониторинг, интеграция с SOC/SIEM, контроль целостности конфигураций, Threat Intelligence и детектирование аномалий.

4. **Реагирование и обучение:**

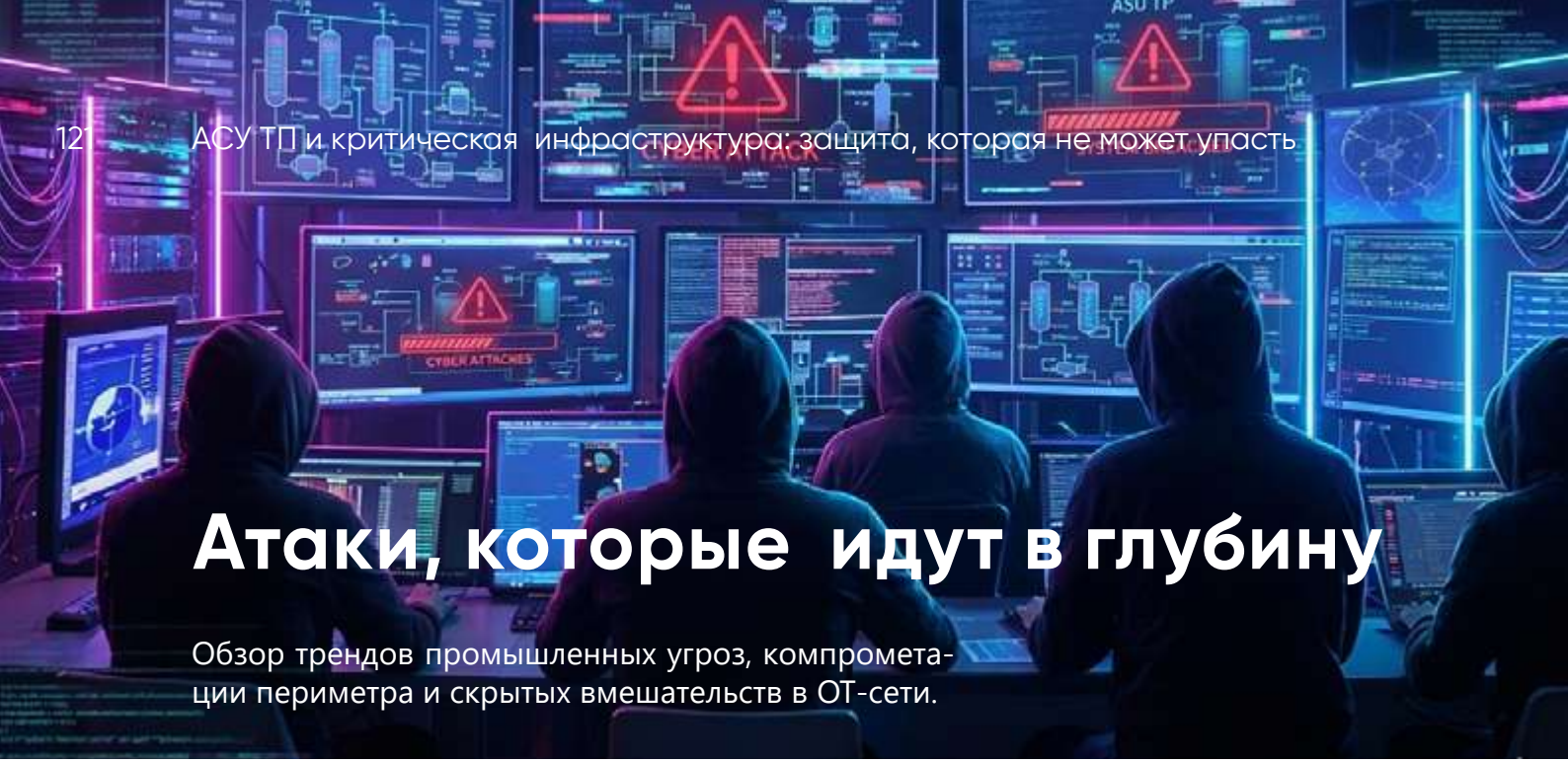
актуализация планов реагирования, тренировки по сценариям DoS и компрометации PLC, обучение персонала.

5. **Работа со старыми системами:**

белые списки приложений, контроль USB-устройств, изоляция устаревших систем.

Заключение

Кибербезопасность АСУ ТП — это не «пункт о безопасности», а стратегический фактор устойчивости критической инфраструктуры. Соблюдение рекомендованных мер снижает риск эксплуатации уязвимостей и обеспечивает стабильность технологических процессов, даже в условиях современных комплексных кибератак.



Атаки, которые идут в глубину

Обзор трендов промышленных угроз, компрометации периметра и скрытых вмешательств в OT-сети.

ТОП-5 трендов киберугроз в промышленных системах

По данным Dragos (OT/ICS Report 2025), число групп, нацеленных на OT, выросло до ~80 — это на 60 % больше, чем было в 2023 году.

Кроме классического шифрования, появляются вредоносы специально для OT (например, FrostyGoop), манипулирующие Modbus TCP.

Ударное воздействие:
в ~25 % случаев — полная остановка OT-сайта;
в остальных — частичные сбои.

Компрометация VPN / RDP

Многие инциденты начинаются с уязвимых шлюзов.

- Dragos выявил RCE-эксплуатацию уязвимостей FortiGate (CVE-2024-55591, CVE-2024-21762).
- При строгой сегментации IT ↔ OT время восстановления значительно ниже.

Глубокие уязвимости в OT

«70% advisories касаются компонентов внутри OT-уровней.»

- Риск потери контроля (loss of control) или визуализации (loss of view).
- Значимый процент «network-exploitable» уязвимостей.

Новые акторы и инструменты

- Новые угрозы: GRAPHITE и BAUXITE.
- Агрессивные хактивисты (BlackJack/Fuxnet) нацелены на сенсоры.
- Wiper-поведение: комбинация шифрования и уничтожения данных.

Supply-chain атаки

- Использование подрядчиков и интеграторов для проникновения.
- Обход барьеров через «доверительные каналы».

Как проникают из IT в OT

Злоумышленники используют слабые места на стыке зон:

1. **Уязвимости VPN**

Эксплуатация CVE в FortiGate и других устройствах для первичного доступа.

2. **Социальная инженерия**

Фишинг и звонки («я техподдержка») — подтверждено за Q2 2025.

3. **Слабая сегментация**

Перемещение из IT в OT там, где зоны не разграничены.

4. **Компрометация AD**

Захват Active Directory позволяет выдавать себя за сервисные учетные записи.

Zero-day и уязвимости протоколов

PLC/RTU: значительная часть уязвимостей находится глубоко в ICS сети.

Modbus/BACnet: устаревшие устройства BMS используют «наследственные» уязвимости (нет шифрования, дефолтная аутентификация).

KEV: ~12% OT-устройств содержат известные эксплуатируемые уязвимости (KEV).

Риск: около 40% организаций имеют OT-активы с KEV, соединенные с Интернетом.

Фальсификация и саботаж

Манипуляция телеметрии:

Malware подменяет значения Modbus, скрывая реальное состояние процесса.

Вредоносные команды:

Отправка опасных команд (Write) на регистры управления.

Подмена прошивки

Компоненты отвечают «нормально», даже если физика процесса нарушена. Скрытый саботаж.

Выводы и рекомендации

Приоритет исправления

Фокус на OT-устройствах, которые имеют KEV и соединены с Интернетом.

Усиление сегментации

Строгое разделение IT/OT, использование jump-host для уменьшения латерального движения.

Мониторинг (OT-NDR)

Выявление аномалий в Modbus/IEC, указывающих на манипуляцию процессами.

Управление доступом

Контроль соединений поставщиков, аудит сессий и ограничение привилегий.

Проверка конфигураций

Регулярные ревизии контроллеров, сенсоров, HMI (дефолтные пароли, прошивки).

Рекомендации по кибергигиене

на рабочем месте:

1. **Запрещается передавать служебную конфиденциальную информацию через внешние, незащищённые сети. Использовать только официально утверждённые защищённые каналы связи.**

   Внутри корпоративной сети данные могут быть перехвачены или неправильно направлены, если использовать неподтверждённые или незащищённые каналы (например, личные мессенджеры или сторонние файлообменники). Любая служебная информация - документы, переписка должна передаваться только через корпоративные системы, защищённую корпоративную почту, внутренние файловые хранилища и VPN. Это гарантирует контроль доступа, шифрование данных и защиту от утечек даже внутри организации.

2. **Не загружать и не открывать файлы или программы из неизвестных или непроверенных источников.**

   Файлы и программы из Интернета, электронных писем от неизвестных отправителей или сторонних ресурсов могут содержать вирусы, трояны или шпионские программы. Если открыть такой файл на рабочем устройстве, вредоносное ПО может незаметно заразить корпоративную сеть, украсть конфиденциальные данные или нарушить работу систем. Чтобы защитить компанию и свои рабочие устройства, используйте только официально утверждённое программное обеспечение и проверенные источники файлов.

3. **Не хранить пароли и логины в открытом виде, на рабочем столе, в блокнотах или других доступных местах. Использовать только защищённые методы хранения.**

   Записи паролей и логинов на бумаге, в текстовых файлах или на рабочем столе легко могут быть обнаружены коллегами, посторонними или злоумышленниками. Это создаёт серьёзный риск несанкционированного доступа к корпоративным системам и конфиденциальной информации. Чтобы защитить свои учетные данные, используйте корпоративные менеджеры паролей, защищённые хранилища и средства аутентификации, одобренные ИБ-службой. Даже временное хранение пароля в открытом виде может привести к утечке данных.

4. **Запрещается фотографировать или снимать на видео экран компьютера и служебные документы, содержащие конфиденциальную информацию.**

   Любые фотографии или видео служебных документов и экрана компьютера могут быть случайно или намеренно переданы третьим лицам. Это создаёт риск утечки конфиденциальной информации: данные могут попасть к конкурентам, злоумышленникам или в открытый доступ. Даже кратковременная фиксация на камеру ставит под угрозу безопасность компании. Для защиты информации работайте с документами только на экране и используйте утверждённые корпоративные средства для совместной работы и обмена файлами.

5. **Не использовать личную электронную почту для служебной переписки или передачи служебных данных.**

   Личные почтовые аккаунты обычно не защищены корпоративными средствами безопасности. Письма с конфиденциальной информацией, отправленные через них, могут быть перехвачены, взломаны или случайно отправлены не тому адресату. Это создаёт риск утечки корпоративных данных и нарушения политики безопасности. Для работы с документами и перепиской используйте только корпоративную почту, которая шифруется, контролируется ИБ-службой и позволяет отслеживать доступ к информации.

6. **Использовать для работы только утверждённое и официально разрешённое программное обеспечение.**

   Непроверенные или неофициальные программы могут содержать вредоносный код, шпионские модули или создавать уязвимости в системе. Особую опасность представляют стилеры - вредоносные программы, которые крадут учётные записи (логины, пароли) и другие конфиденциальные данные. Их установка на рабочем устройстве может привести к заражению корпоративной сети, краже информации или нарушению работы систем. Чтобы защитить данные и обеспечить безопасную работу, используйте только программы, официально разрешённые и проверенные ИБ-службой. Это гарантирует безопасность и соответствие корпоративным стандартам.

7. **Работать только на корпоративных устройствах.**

   Корпоративные устройства защищены антивирусами, средствами защиты информации и шифрованием данных. Личные устройства могут содержать вирусы или стилеры, которые крадут логины, пароли и другие служебные данные. Чтобы предотвратить утечки и защитить систему, все задачи выполняйте исключительно на корпоративных устройствах.

8. **Не подключать личные мобильные устройства, ноутбуки и планшеты к корпоративной сети без официального разрешения и соответствующей защиты.**

   Личные устройства могут быть заражены вирусами, шпионским ПО или стилерами, которые крадут учётные данные и другую конфиденциальную информацию. Если подключить такое устройство к корпоративной сети, вредоносные программы могут незаметно распространяться, передавать служебные данные злоумышленникам и нарушать работу систем. Чтобы защитить корпоративные ресурсы, используйте только официально разрешённые и проверенные устройства, которые контролируются ИБ-службой, а доступ к сети осуществляется через защищённые корпоративные каналы.

9. **Включать двухфакторную аутентификацию (2FA) там, где это возможно.**

   Пароль сам по себе - это только половина защиты, поэтому двухфакторная аутентификация через приложение, SMS или токен предотвращает вход злоумышленника даже при краже пароля; это как дополнительный замок на двери, который есть только у вас, и примером служит случай, когда сотрудник ввёл пароль после фишингового письма, но без второго фактора войти не удалось, и атака была остановлена.

10. **Использовать сложные и уникальные пароли, регулярно их менять.**

    Простые пароли вроде 123456, qwerty, даты рождения или имени питомца взламываются за секунды, а использование одинакового пароля для нескольких сервисов создаёт эффект домино, когда одна утечка открывает доступ ко всем системам; например, пароль от старого сайта был украден, и злоумышленник смог войти в корпоративную почту и получить доступ к документам и контактам, поэтому важно генерировать сложные и уникальные пароли для каждого сервиса, хранить их в корпоративном менеджере и регулярно менять, особенно при подозрении на утечку.

11. **Не подключать съемные носители с пометкой «Для служебного пользования» (ДСП) к рабочим станциям внешнего и внутреннего контура.**

    Не подключать съемные носители с пометкой «ДСП» к рабочим станциям внешнего и внутреннего контура, так как эти носители предназначены для специальных данных, и неправильное подключение может вызвать сбои в системе, нарушить работу сети или привести к утечке информации; использовать их следует только если они официально разрешены для конкретного контура и проверены ИБ.

12. Не передавать пароли и учетные данные третьим лицам

Не передавать пароли и учетные данные третьим лицам даже коллеге для быстрого доступа, потому что если произойдёт утечка, удаление или взлом, все действия будут зафиксированы на вашей учётной записи, и ответственность будет считаться вашей; например, сотрудник разрешил коллеге войти под своим логином, и через час из этого аккаунта ушли документы, что создало серьёзные проблемы, поэтому каждый сотрудник должен использовать только свой аккаунт, а доступ другим предоставляется официально через ИТ.

13. При подключении съемных носителей обязательно сканировать их на наличие вредоносного кода.

При подключении съемных носителей обязательно сканировать их на наличие вредоносного кода, потому что флешки, карты памяти и внешние диски могут быть переносчиками вирусов, и даже новые устройства иногда заражены, способные распространять вредоносное ПО по сети, шифровать, удалять или копировать файлы; перед использованием необходимо подключать носитель к корпоративному антивирусу и проводить проверку, чтобы избежать заражения всей сети.

14. Не оставлять рабочий компьютер без блокировки, даже если отходите на минуту.

Не оставлять рабочий компьютер без блокировки, даже если отходите на минуту, крайне важно, потому что разблокированный компьютер - это как дверь с табличкой «Заходите, всё на столе», и за секунды любой человек может скопировать документы, отправить письма от вашего имени, установить вредоносное ПО или получить доступ к конфиденциальным данным; например, сотрудник вышел на 30 секунд к принтеру, а с его почты уже ушло письмо с просьбой о переводе денег, что могло иметь серьёзные последствия, поэтому при уходе следует нажимать Win+L или закрывать крышку ноутбука, что мгновенно защищает рабочее место.

15. Сообщать о подозрительных действиях или инцидентах службе информационной безопасности.

Любые подозрительные действия или инциденты, такие как странные письма, непонятные файлы, неожиданные системные сообщения или необычное поведение компьютера, следует немедленно сообщать службе информационной безопасности, потому что ранняя реакция предотвращает серьёзные последствия, включая утечку данных, заражение сети или финансовые потери; например, сотрудник заметил письмо с подозрительной ссылкой, сообщил в ИБ, и потенциальная атака была остановлена до того, как кто-либо пострадал.

Прогнозы кибербезопасности

Шамбулов Улыкбек Кадыржанович
Первый Заместитель Председателя Правления АО «ГТС» | Начальник НКЦИБ

Это новый этап цифровой конкуренции, где эффективность обороны определяется не количеством регуляторных требований, а инженерным качеством систем и зрелостью команд, которые их поддерживают и развивают.

В условиях стремительного технологического прогресса и глобальной цифровизации киберпространство остаётся зоной высокой конкуренции и постоянных рисков. Как руководитель Национального центра киберинцидентов и представитель отрасли, считаю важным поделиться прогнозом ключевых трендов, на которые нам следует ориентироваться в ближайшем году. Эти выводы основаны на практическом опыте реагирования, результатах взаимодействия с государственными и частными организациями, а также на задачах, которые стоят перед национальной инфраструктурой.

В ближайший год киберпространство продолжит динамично трансформироваться под воздействием технологий искусственного интеллекта. Уже в 2025 году мы наблюдали существенный рост атак на государственные сервисы, телекомоператоров, энергетические компании, спутниковые системы связи, а также на информационные ресурсы, содержащие демографические и оборонные данные.

2026 год станет периодом, когда атаки будут ещё более точечными, интеллектуальными и технически сложными. Это новый этап цифровой конкуренции, где эффективность обороны определяется не количеством регуляторных требований, а инженерным качеством систем и зрелостью команд, которые их поддерживают и развивают.

На наших глазах ИИ перестаёт быть обычным инструментом автоматизации и превращается в новый слой инфраструктуры, который сам становится объектом атак. 2026 год станет годом, когда ИИ начнёт атаковать ИИ. Уже сегодня мы фиксируем случаи prompt-инъекций, передающихся через документы, цепочки интеграций и корпоративные базы знаний. Подмена данных в RAG-модулях, манипуляция embedding-векторами и внедрение adversarial-маркеров позволяют злоумышленникам нарушать работу аналитических моделей, используемых в SOC, финансовом мониторинге, антифрод-системах и сервисах классификации трафика.

На наших глазах ИИ перестаёт быть обычным инструментом автоматизации и превращается в новый слой инфраструктуры, который сам становится объектом атак.

Критически важным в 2026 году станет вопрос безопасности GPU-кластеров, суперкомпьютеров и платформ, где размещаются обучающие и инференс-модели. Многие организации стремятся внедрять AI/ML-решения, но не учитывают, что GPU-сегменты создают новую поверхность атаки. Уязвимости в Kubernetes, конфигурациях контейнеров, драйверах CUDA/ROCm и межконтейнерных IPC-механизмах уже используются злоумышленниками для побега из контейнеров, несанкционированного доступа к VRAM и анализа данных других пользователей. Особенно опасной является незаметная подмена весов модели: изменив всего несколько параметров, злоумышленник может ослабить модель обнаружения аномалий, изменить чувствительность антифрод-алгоритмов или внести логические «закладки» в государственные сервисы.

На этом фоне APT-группировки укрепляют своё присутствие в национальных сегментах связи, обработки данных и критической инфраструктуры. Мы наблюдаем всё более устойчивые и скрытные методы закрепления злоумышленников в корпоративной инфраструктуре: использование сервисных учётных записей CI/CD, манипуляция правилами почтовых ящиков, перехват токенов облачных сервисов и эксплуатация уязвимых библиотек в цепочках поставки.

Известные вредоносные семейства, такие как PlugX и ShadowPad, продолжают эволюционировать, внедряя новые методы DLL side-loading и шифруя C2-трафик под современные протоколы, включая QUIC и HTTP/3. Особое внимание вызывает активность в отношении спутниковых систем, где компрометация SDR-модулей и перехват телеметрии позволяют злоумышленникам собирать информацию, влияющую на национальную безопасность.

Наша страна стремится к полной цифровизации и ИИ-зации. Это, в свою очередь, требует мощностей и устойчивой энергетической инфраструктуры. Такие крупные проекты, как АЭС, будут особенно значимы. Промышленные сети и системы управления технологическими процессами в 2026 году будут находиться под давлением атак, направленных не просто на получение доступа, а на манипуляцию технологическими параметрами. Инженерные рабочие станции становятся основной точкой проникновения: в них внедряются вредоносные пакеты, подменяются библиотечные зависимости, используются удалённые доступы, оставленные по невнимательности инженеров. Подмена логических блоков PLC, атаки на OPC-UA, DNP3 и Modbus TCP, фальсификация данных в системах historian — всё это создаёт риски, непосредственно влияющие на работу производственных объектов и критической инфраструктуры страны.

Биометрические системы идентификации также становятся целью атак. Рост числа решений, использующих 3D-моделирование лица, а также шаблоны ладони, вен или голоса, вместе с генерацией биометрических масок средствами машинного обучения приводит к необходимости переосмысления доверия к биометрии как к единственному идентификатору. Компрометация биометрического шаблона — событие необратимое, ведь его невозможно «заменить», как пароль. Поэтому в новом году ключевым станет внедрение комбинированной аутентификации и технологий обнаружения спуфинга.

Цепочки поставки программного обеспечения станут глобальной национальной уязвимостью. Компрометация GitHub Actions / GitLab CI/CD, подмена артефактов в Artifactory / Nexus, атаки на ключи подписи и внедрение вредоносного кода в зависимости открытого ПО могут привести к масштабным инцидентам. Мы ожидаем усиление атак на DevOps-инфраструктуру, поскольку именно она обеспечивает производство приложений и сервисов, используемых государственными структурами и критически важными операторами.

Вопрос управления привилегиями станет отдельным направлением риска. Суперадминистраторы остаются единой точкой катастрофы: компрометация их учётной записи открывает злоумышленнику путь ко всей инфраструктуре. В совокупности с атаками на AD, Kerberos, сервисные токены и ошибочные конфигурации LDAP/SMB это создаёт условия для быстрого lateral movement и полного захвата домена. Государственным системам требуется переход к временным привилегиям, жёсткому журналированию действий — возможно, с использованием блокчейн-технологий — и регулярной ревизии прав на уровне национального стандарта.

В 2026 году безопасность должна быть встроена на каждом этапе жизненного цикла разработки

Увеличение сложности атак предъявляет новые требования к DevSecOps-культуре. В 2026 году безопасность должна быть встроена на каждом этапе жизненного цикла разработки: от моделирования угроз на этапе планирования, статического и динамического анализа кода — до обязательного контроля инфраструктурного кода, секрет-сканирования, политики GitOps с использованием OPA/Kyverno и нулевого доверия в CI/CD-окружениях.

Без этой зрелости мы **рискуем получить масштабные инциденты через самый незаметный, но наиболее критичный слой — разработку.** В течение года мы видели инциденты, когда даже самые крупные компании и предприятия с сильными командами разработчиков пренебрегали практиками безопасной разработки. Это проявлялось в банальном хранении credential-данных и токенов, захардкоженных в исходных кодах, которые затем публиковались или могли быть извлечены через reverse engineering.

Важнейшее направление следующего года — реалистичные киберучения с моделированием реальных APT-сценариев. Стандартные лабораторные упражнения уже недостаточны: командам необходимо учиться работать в условиях, максимально приближённых к реальности. В этом году мы провели соревнование среди студентов по направлению Blue Teaming. Молодые специалисты показали очень обнадёживающие результаты, что даёт уверенность: у нас растёт сильное поколение киберзащитников.

В совокупности всё это требует обновления нормативных документов, регламентов тестирования и правил аудита. Новые стандарты должны учитывать ИИ, ML-пайплайны, GPU-инфраструктуру, проверку мобильных приложений по расширенным методикам OWASP, анализ цепочек поставки и угрозы, характерные для современных DevOps-сред.

В 2026 году НКЦИБ будет усиливать координацию реагирования, расширять национальную платформу для обмена Threat Intelligence и внедрять механизмы раннего предупреждения для объектов критической инфраструктуры.

Однако успешно противостоять вызовам мы сможем только в сотрудничестве — объединяя компетенции государства, частного сектора и научного сообщества.

Кибербезопасность уже вышла за рамки регуляторной задачи. Это инженерная, системная и стратегическая дисциплина, требующая глубокой экспертизы, постоянного обучения и совместной работы.

КОНТАКТЫ

STS.KZ