PROFIT SECURITY DAY · 2026

Как мы пережили атаку GlobeImposter 2.0, отказались от Active Directory в пользу Entra ID и пересобрали сеть вокруг Defender XDR

От критического ransomware-инцидента к архитектуре Zero Trust

НАО «КазНПУ имени Абая» · Блок цифровизации и информационной безопасности

Докладчик: Мусабаев Н.Б.



10 марта 2026 г.: таргетированный удар по виртуализации VMware vSphere и бэкапам

08:15 — Аномальная активность в VMware vSphere

08:40 — Массовая недоступность внутренних сервисов

09:00 — Обнаружена ransom-нота GlobeImposter 2.0

09:15 — Штаб ИБ и экстренная сетевая изоляция

10:00 — Снятие forensic-образов и уведомление KZ-CERT

Вредонос	GlobeImposter Ransomware 2.0 — записка How_to_back_files.html с требованием выкупа
Главная цель удара	Кластер виртуализации VMware vSphere (ESXi 8.0.3) и сервер резервных копий Veeam Backup & Replication
Затронутые сервисы	**Академический контур:** legacy LMS Univer (посреди семестра) **Админ-блок:** СЭД SalemOffice, 1С:Предприятие, SDGS **Инфраструктура:** Print Server / MyQ, WSUS, Wi-Fi, IP-телефония, OJS «Вестник»

Позиция организации

0 ₸

выкупа. Полный отказ от переговоров, курс на собственное восстановление и архитектурную перестройку

Анатомия атаки: арсенал злоумышленников и ночная попытка уничтожить бэкапы Veeam

Гипотезы первоначального доступа

Вектор А: легаси-VPN без MFA

Внешняя сессия из Вьетнама под УЗ сотрудника (~23 ч, малый трафик) — возможная разведка или decoy

Вектор Б: внутренний хост (с 09.03)

Активность на узле 192.168.225.127, сбор паролей из браузеров и памяти LSASS

Постэксплуатация и lateral movement

Разведка и кража УЗ

netscan.exe, CredentialsFileView, WebBrowserPassView, cmd_pass.exe

Продвижение и C2

PsExec.exe по плоской сети; канал TCP.Split.Handshake на РФ IP

Подавление защиты

DefenderControl 2.exe, фейковая служба winserv.exe

Ночной саботаж Veeam 10.03, 02:29

104

запуска консоли Veeam Backup для зачистки репозиториев

11 сек

на зачистку 5 журналов Windows: Security, System, PowerShell, Application, AppLocker

Корневые причины: три системных дефекта старой архитектуры и техдолг 2022–2025 гг.

АРХИТЕКТУРНЫЙ ДЕФЕКТ (AS-IS)	КАК ЭТИМ ВОСПОЛЬЗОВАЛИСЬ АТАКУЮЩИЕ
1. Классический локальный Active Directory без сегментации прав	Единая точка компрометации: кража паролей и токенов на одном узле + локальный админ открыли дорогу к доменным сервисам и Veeam
2. «Плоская» корпоративная сеть без микросегментации	Открытые SMB, RPC, WinRM и RDP (3389) между рабочими станциями, серверами и гипервизором позволили PsExec свободно ходить по сети
3. Легаси-VPN (FortiClient) без MFA и исторический техдолг (2022–2025)	Статичные пароли без проверки устройства и рисков; в ShimCache найдены старые следы KMSAuto, AnyDesk и нелицензионного ПО

Критический вывод для команды
До атаки уже инициирована закупка Defender for Endpoint P2 (1 000 лицензий) и Entra ID P2 (25 Faculty + 1 000 Student) — атака застала нас в момент перехода.

«Подлечить» старый AD и поставить антивирус поверх плоской сети недостаточно — нужно менять саму модель доверия.

Первые 48 часов: локализация, криминалистика и спасение данных без переговоров

1 Containment

Отключение ESXi, изоляция Veeam, отзыв 83 VPN-УЗ

2 Forensics

Образы ВМ, дампы RAM, логи FortiGate / vCenter переданы в KZ-CERT

3 Decryption

Дешифрование БД legacy LMS Univer силами ИТ-команды — без выкупа

4 Isolation & Run

Архив Univer в Read-Only, опора на Abai Digital, 1С и Salem — 100% Up

100%

ключевых систем в штатном режиме

СЭД Salem, 1С:Предприятие, SDGS, eLibrary и официальные веб-порталы вернулись в строй.

Read-Only

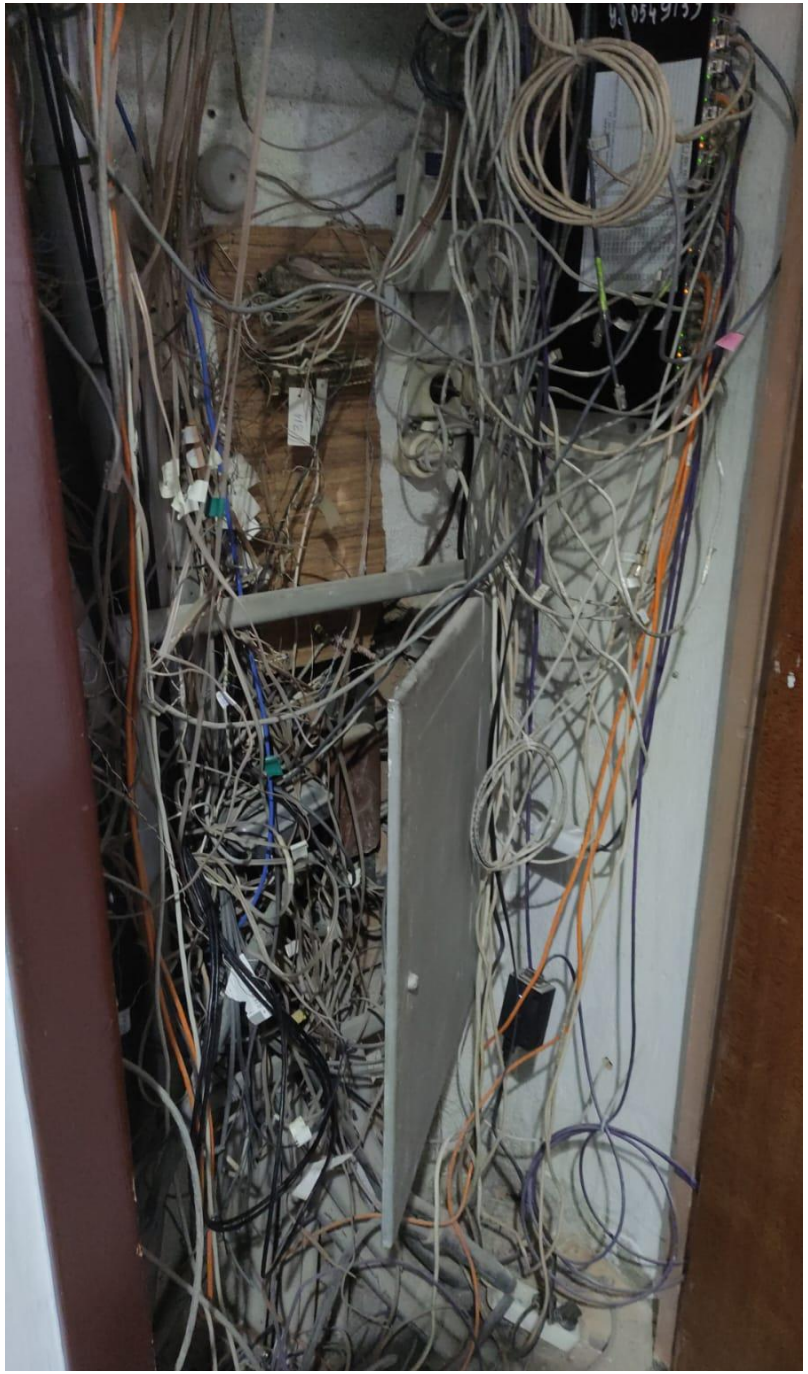
спасение базы LMS Univer

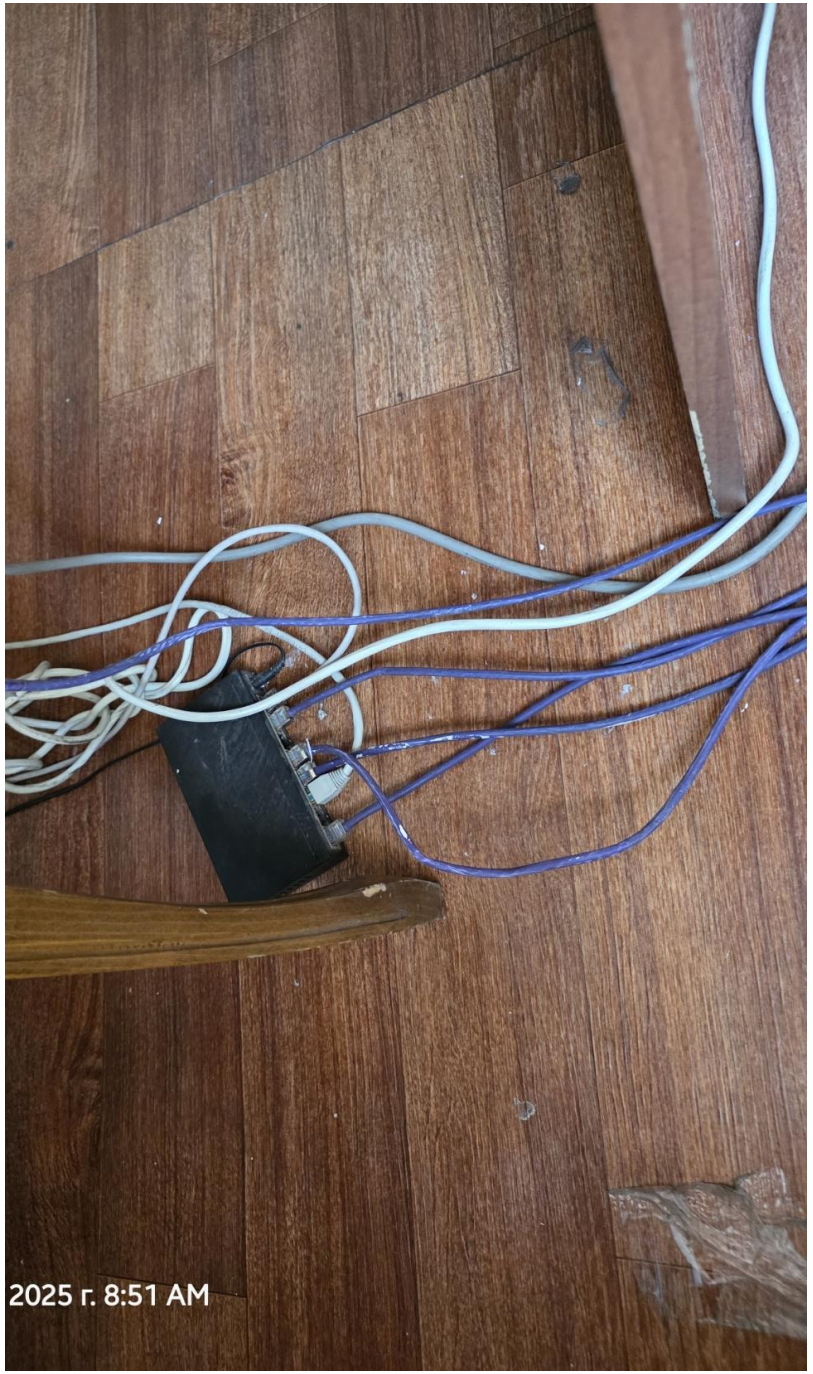
База дешифрована без выкупа. Уязвимый код Univer в прод не вернули: поднят изолированный портал архива для сверки оценок и сдачи отчётности в ЕПВО (до 26 марта).

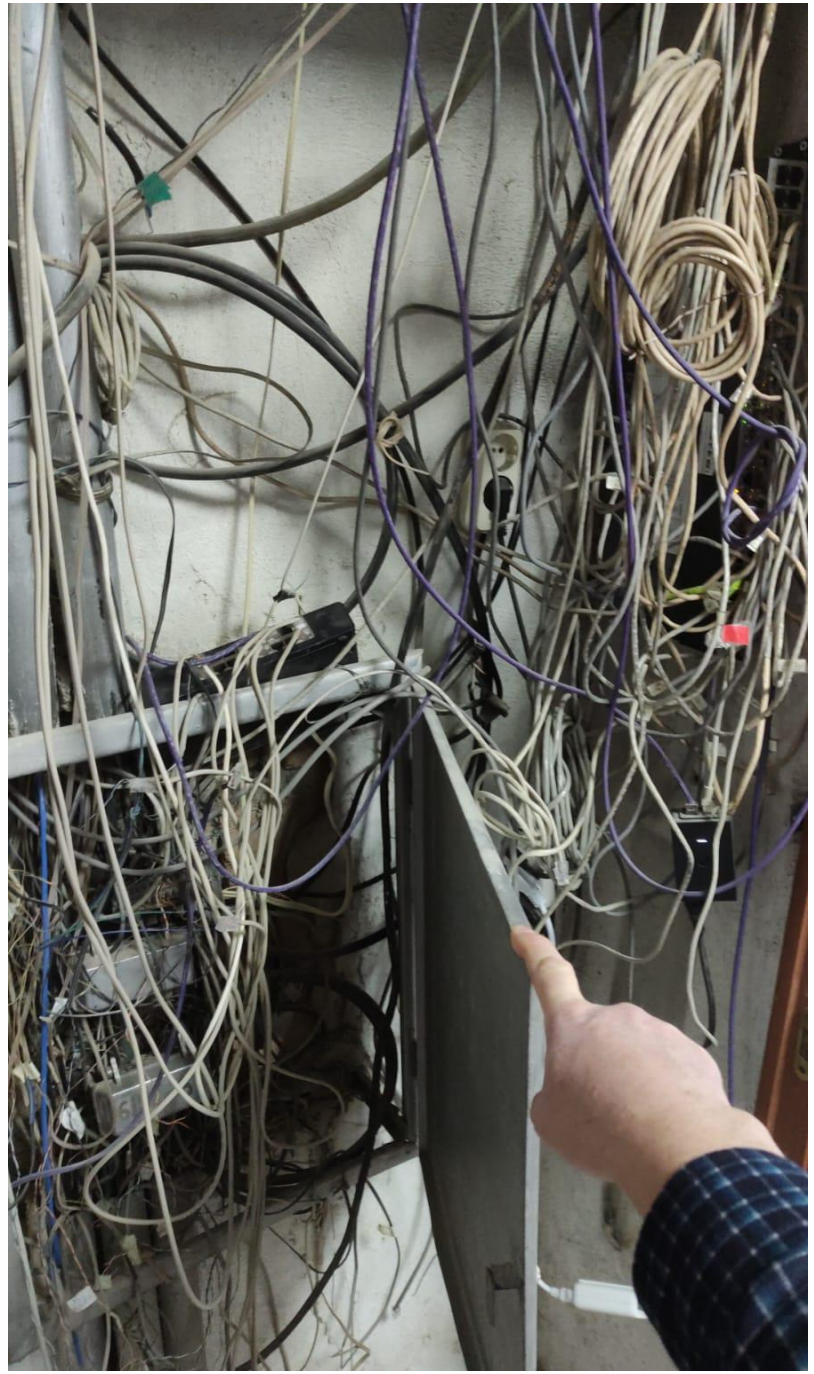
21 000+

студентов — на Abai Digital

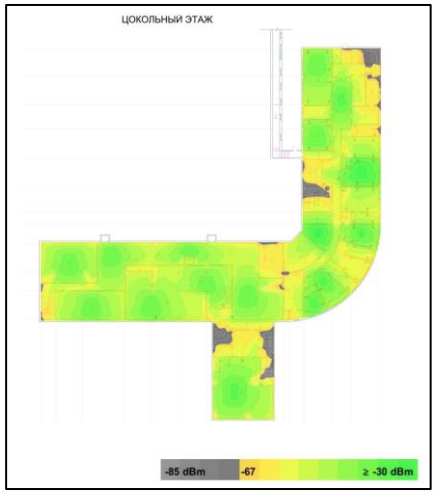
Весь текущий учебный контур (ведомости, сессия, выпуск) оперативно переведён на новую собственную платформу Abai Digital.

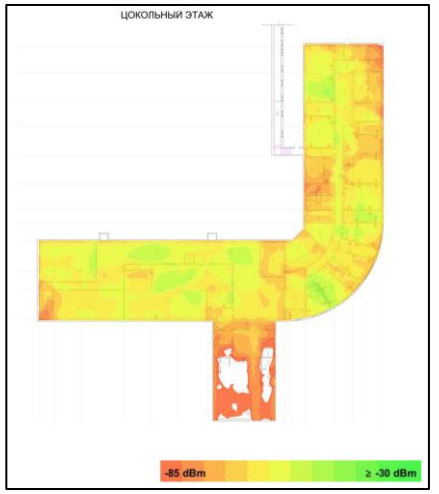


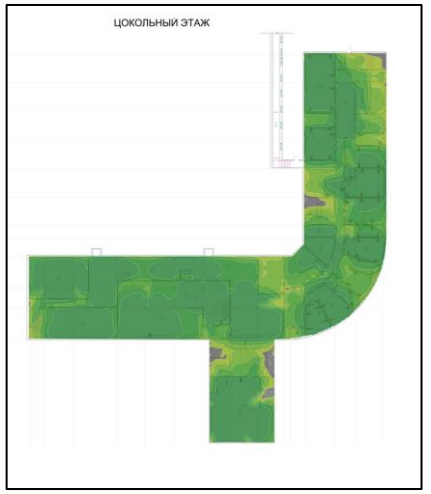

2025 г. 8:51 AM



Фаза	Фокус
1. Оценка	Базовый уровень и концепция
2. Сеть	Обновление проводной/беспроводной сети
3. Безопасность	Управление доступом и идентификацией
4. Умный кампус	IoT, автоматизация, безопасность
5. Обучение	Сотрудничество, обучение, VDI
6. Исследования	HPC, облако, услуги обработки данных
7. Устойчивое развитие	Оптимизация энергии и ресурсов
8. Управление	Поддержка, инновации













Отказ от Active Directory в пользу Microsoft Entra ID: Cloud-First Identity

БЫЛО: ЛОКАЛЬНЫЙ ACTIVE DIRECTORY	СТАЛО: ENTRA ID P2 + INTUNE
Локальные контроллеры домена — главная цель шифровальщика (NTLM, Kerberos, GPO, LSASS)	Облачный центр идентификации: нет локальных КД для захвата — нет Kerberoasting, Golden Ticket и рассылки шифровальщика через GPO
Постоянные права Domain Admin у администраторов	PIM: права Just-In-Time строго по запросу, с обязательным MFA и логированием
Статичные пароли в VPN и службах	Обязательный строгий MFA + risk-based Conditional Access (оценка риска входа)
Управление ПК через доменные GPO только внутри офисного периметра	Облачный MDM Intune: комплаенс устройства проверяется до выдачи токена

Conditional Access: формула доступа

Валидный пользователь

+

Строгий MFA

+

Compliant-устройство в Intune / Defender

= доступ к ресурсам и облаку

Единый SSO-периметр: ключевые сервисы и админ-контуры привязаны к Entra ID, сессии отзываются мгновенно при риске.

Microsoft Defender XDR: от сигнатурного антивируса к автоматическому разрыву атаки

Телеметрия в реальном времени
1 000+ конечных точек (Defender for Endpoint P2) + сигналы Entra ID (Identity)

Microsoft Defender XDR
Единая корреляция инцидентов по конечным точкам и идентификации

Результат
Атаку уровня 10 марта остановили бы на первой минуте

1. Превентивно
ASR + Tamper Protection

Attack Surface Reduction
Блокировка дампа памяти LSASS (останавливает CredentialsFileView и аналоги), запуска скриптов, PsExec и WMI

Tamper Protection
Запуск DefenderControl 2.exe или остановка службы агента блокируется и поднимает критический алерт

2. В момент атаки
Automatic Attack Disruption

Авто-изоляция хоста
Хост автоматически отрезается от сети за секунды

Отзыв сессии в Entra ID
Токен учётной записи блокируется — не дожидаясь, пока дежурный инженер проснётся в 02:29 ночи

3. После и проактивно
Threat Hunting + Auto-Investigation

30+ дней телеметрии
Глубина данных для охоты за угрозами и расследований

Auto-Investigation & Remediation
Автоматическое расследование и устранение последствий

Как стек Microsoft работает вместе: идентичность, устройства, конечные точки и облако

Идентичность

Microsoft Entra ID P2

- Conditional Access: доступ по риску и состоянию устройства
- PIM: привилегии Just-In-Time с MFA
- ID Protection: оценка риска входа и учётной записи

Устройства

Microsoft Intune

- Политики соответствия (compliance) для Conditional Access
- Централизованные обновления и настройка базовой защиты
- Политики WDAC / AppLocker и правила ASR

Конечные точки и XDR

Defender for Endpoint P2 / Defender XDR

- EDR с поведенческим анализом
- ASR, Tamper Protection
- Automatic Attack Disruption, Advanced Hunting

Данные и резервирование

Microsoft Azure

- Облачная копия вне корпоративного контура
- Неизменяемое (WORM) хранилище
- Правило резервирования 3-2-1

Как это связано

Defender видит риск на устройстве → Intune помечает его как Non-compliant → Conditional Access в Entra ID блокирует доступ и сессии

Перестройка сети: от «плоской сети + AD» к Zero Trust и микросегментации

БЫЛО (AS-IS)
Плоская сеть + on-prem AD

Легаси-VPN без MFA → Рабочие станции (домен AD) → Серверы (1С, СЭД, LMS) → ESXi + Veeam в одном контуре доверия

SMB / RPC / PsExec / RDP — без ограничений

СТАЛО (TO-BE)
Zero Trust + Entra ID + Defender XDR

Устройства Entra Joined + Intune, агент Defender XDR → Conditional Access + MFA (только Compliant) → Сегментированный шлюз / NGFW → Серверный сегмент (App VLAN), мониторинг Defender XDR

Изолированный Management VLAN (Jump Host + MFA) → Кластер VMware vSphere

Запрет PsExec / WinRM / 3389 из user VLAN

WORM-бэкапы 3-2-1 + Azure (однонаправленная репликация)

Запрет lateral movement
SMB (445), RDP (3389), WinRM и PsExec закрыты между ПК и к серверам

Отказ от «широкого» VPN
Вход привязан к Conditional Access и здоровью устройства в Defender

Изоляция гипервизоров
ESXi в закрытом VLAN без привязки к пользовательским УЗ, вход через Jump Host

Неизменяемые бэкапы
WORM: даже администратор не удалит копию до истечения срока

Локализация ПДн в РК
Токены и телеметрия XDR — в облаке; базы ПДн — в ЦОД на территории РК

Новая архитектура закрыла 8 предписаний KZ-CERT и обеспечила 100% KPI по ПП РК № 832

	ПРЕДПИСАНИЕ KZ-CERT / НОРМА ПП РК № 832	КАК ЗАКРЫТО В НОВОЙ АРХИТЕКТУРЕ
1	Закрыть RDP (3389) и AnyDesk, доступ наружу только с MFA	**RDP/AnyDesk закрыты; доступ только с MFA и Conditional Access в Entra ID**
2	Включить MFA для всех УЗ; блокировка доступа и ЭЦП при увольнении ≤ 2 ч	**100% MFA: Entra ID P2 + PIM (JIT); связка HR/ЕСУТД с Entra ID, отзыв ЭЦП**
3	Внедрить EDR/XDR; изоляция узла ≤ 1 ч при критическом инциденте	**Defender XDR на 1 000+ узлах: Auto-Isolation за секунды (вместо 1 ч)**
4	Бэкапы 3-2-1 с WORM-копией; Audit Trail ≥ 3 лет	**Изолированный WORM + Azure; неизменяемый сбор логов ≥ 3 лет**
5	Патчинг систем за 7–14 дней	**Облачное управление обновлениями Intune**
6	Блокировка опасных скриптов и вложений	**ASR-правила Defender + шлюзовая очистка**
7	Контроль запуска ПО (Allowlisting)	**Политики WDAC / AppLocker через Intune**
8	Сегментация сети и независимость CISO (п. 13 ЕТИКТ)	**Микросегментация, ESXi Mgmt VLAN; CISO подчинён напрямую Ректору**

Результаты трансформации: измеримый эффект для непрерывности бизнеса и ИБ

0 ₸

Выплата выкупа злоумышленникам

Полный отказ, данные спасены

100%

Восстановление ключевых сервисов

1С, СЭД, LMS / Abai Digital, ЕПВО

0 КД

Зависимость от локальных контроллеров домена

Ликвидирована: переход на Entra ID + Intune

100%

Покрытие MFA и условным доступом

Администраторы (PIM / JIT) и сотрудники

1 000+

Узлов под защитой Defender XDR

ASR + изоляция за секунды

3-2-1

Бэкапы и комплаенс ПП РК № 832

WORM 3-2-1 + готовность к 100% KPI

Что дальше: четыре шага к зрелой киберустойчивости на базе Microsoft

01

Единая SecOps-платформа

- Microsoft Sentinel (SIEM/SOAR) вместе с Defender XDR
- Логи vCenter, FortiGate и Veeam в одном месте
- Плейбуки автоматизации реагирования

02

Защита идентичности

- Entra ID Protection: политики по риску входа
- Периодические access reviews привилегированных ролей
- Контроль аварийных (break-glass) учётных записей

03

Управление уязвимостями

- Defender Vulnerability Management
- Microsoft Secure Score как метрика зрелости
- Контроль сроков патчинга 7–14 дней по отчётам

04

Проверка готовности

- Регулярные тесты восстановления из WORM-копий
- Учения по сценарию 10 марта (tabletop)
- Пересмотр плана реагирования на инциденты

Рекомендации подготовлены на основе общих возможностей продуктов Microsoft; сроки, лицензирование и стоимость требуют отдельного согласования.

5 практических уроков для CISO и ИТ-архитекторов

1. **Уходите от локального AD к Cloud Identity**
   Локальный КД в плоской сети — главный ускоритель ransomware; Entra ID + Intune + PIM радикально режут поверхность атаки (при локализации баз ПДн в ЦОД РК).

2. **Свяжите EDR/XDR с Identity**
   Defender XDR + Entra ID автоматически отрезают заражённый хост и отзывают токен за секунды, даже в 02:29 ночи.

3. **Уберите «широкий» VPN и плоскую сеть**
   Взлом одного ПК не должен давать PsExec/SMB/RDP-маршрут к серверам; проверяйте не только пароль, но и состояние устройства.

4. **Отделите гипервизоры и бэкапы от домена**
   Отдельный Management VLAN для ESXi и неизменяемые бэкапы (WORM) — единственный надёжный страховой полис.

5. **Обеспечьте независимость CISO (п. 13 ЕТИКТ) и Compliance by Design**
   Служба ИБ подчиняется напрямую первому руководителю, а 100% KPI по ПП РК № 832 собирается как результат работающей архитектуры, а не бумажной отписки.

Спасибо за внимание!

Вопросы?

Мусабаев Н.Б.
Член Правления – Проректор по цифровизации