03.09.2026 · РЕДАКЦИЯ GENIUS SYSTEMS

ИБ-дайджест за август 2026: угрозы, уязвимости и динамика в Казахстане и мире

ИБ-дайджест Genius Systems — это ежемесячный обзор киберугроз, уязвимостей и изменений в регулировании для руководителей и ИБ-специалистов организаций Казахстана: Усть-Каменогорск, Астана, Алматы, Караганда, Павлодар. Только проверенные цифры с источниками, без пересказа пресс-релизов. Первый выпуск — за август 2026 года.

Главное за месяц

- **Ransomware на максимуме.** По данным Check Point, в июле на сайтах вымогателей опубликовано 964 жертвы — на 87 % больше, чем годом ранее. По ransomware.live август ещё выше: 709 жертв против 618 в июле.
- **31 уязвимость с подтверждённой эксплуатацией** добавлена в каталог CISA KEV за август — вдвое больше, чем в августе 2025. Под ударом периметр: Cisco ASA, Citrix NetScaler, Fortinet, Zimbra, VMware vCenter.
- **Казахстан: инцидентов стало меньше, но они опаснее.** KZ-CERT за первое полугодие зафиксировал 24,3 тыс. инцидентов (минус 30 %), при этом заражений вредоносным ПО стало в 2,3 раза больше, а случаев несанкционированного доступа — в 26 раз.
- **Две APT-кампании против госорганов РК** раскрыты за июль–август: SilkParasite (Bitdefender) и OctLurk/SilkLurk (Kaspersky). Обе — кибершпионаж, обе — китайскоязычные группы.
- **С 25 августа 2026 утечку персональных данных скрыть нельзя:** заработал реестр нарушений безопасности ПДн, уведомление регулятора — в течение одного рабочего дня, штрафы до 2000 МРП.

Казахстан

Статистика KZ-CERT за первое полугодие 2026

24,3 тыс.
инцидентов зафиксировал KZ-CERT за полугодие
−30 % г/г

×2,3
рост заражений вирусами, червями и троянами
20,4 тыс. случаев

×26
рост несанкционированного доступа и модификации
266 случаев

13,1 тыс.
интернет-мошенничеств за январь–июль
−10 % г/г

1-е полугодие 2025: 34,8 тыс. инцидентов, 71 % — ботнеты.

1-е полугодие 2026: 24,3 тыс. инцидентов, 84 % — вредоносное ПО. Источник: KZ-CERT в изложении finprom.kz, 14.08.2026.

Что это значит. Падение общего числа — за счёт ботнетов, которые в прошлом году составляли 71 % статистики. Структура сместилась к тому, что действительно бьёт по организациям: заражения вредоносным ПО (84 % всех инцидентов) и взломы. Рост несанкционированного доступа в 26 раз — это уже не «шум», а целенаправленные атаки.

Другие цифры за период:

- **Интернет-мошенничество:** 57 % всех мошенничеств в стране. Лидеры — Астана (2,3 тыс.), Алматы (1,4 тыс.), Павлодарская область (1,1 тыс.). МВД вернуло потерпевшим 4,8 млрд ₸ за полугодие.
- **КНБ:** 2,5 млрд кибератак на Казахстан с 2022 года, 20,5 тыс. целенаправленных DDoS на критически важные объекты (Ермек Сагимбаев, 13 июля 2026).
- **Kaspersky по Казахстану, январь–май 2026:** атаки с эксплойтами на частных пользователей +54 %, атаки на бизнес с бэкдорами +56 % (WebShell, Remcos, Androm). По майнерам Казахстан — 10-е место в мире (0,62 % пользователей, Securelist Q2 2026).
- **Утечки:** по данным F6, за полугодие опубликовано 12 утечек казахстанских компаний — столько же, сколько за весь 2025 год. 79 % записей — госсектор.

События июля–августа

1. **«Утечка 15 млн казахстанцев из eGov» — не подтверждена.** 11–12 августа в даркнете выставили базу «47 млн строк» за 0,5 BTC. Министерство искусственного интеллекта и цифрового развития заявило, что взлома eGov не было, а сканов паспортов в описанном виде в системе нет. Аккаунт продавца создан в августе, образец данных не показан — признаки компиляции старых утечек. Напоминание: реальная утечка 16 млн записей 2025 года всё ещё расследуется КНБ.
2. **SilkParasite — APT против госорганов Центральной Азии, включая РК** (Bitdefender, 19 августа). Семь семейств RAT, пять новых, около 65 заражений с октября 2025. Приманки — документы под конкретные министерства, архивы с паролем, проверка на наличие Kaspersky, следы разработки с помощью ИИ.
3. **OctLurk и SilkLurk** (Kaspersky GReAT, 30 июля) — бэкдоры в госорганах, медучреждениях, исследовательских институтах и логистике Казахстана, привязанные к конкретным машинам жертв.
4. **Сбой eGov и сайтов госорганов 21 августа.** АО «НИТ»: «в связи с повышенной активностью внешнего интернет-трафика сработали механизмы защиты». Слово DDoS не прозвучало. Ранее, 4 августа, гражданин после авторизации попал в чужой аккаунт eGov.
5. **DDoS на КазТАГ** 19–20 июля: провайдер временно заблокировал зарубежный трафик.

6. **ENERFORT 2026** — первые киберучения энергетики РК (27 июля). На фоне атак на ТЭЦ в Польше и электростанцию в Великобритании (см. ниже) — своевременно.

Регуляторика: что изменилось

- **С 12 июля** действует Цифровой кодекс РК, закон «Об информатизации» переименован в закон «О кибербезопасности».
- **С 12 июля** — новые правила уведомления об утечках ПДн: оператор сообщает регулятору в течение 1 рабочего дня, центры кибербезопасности — в течение 3 часов.
- **С 25 августа** — закон о цифровизации и защите ПДн: классификация операторов (малые до 10 тыс. субъектов, средние до 500 тыс., крупные свыше), реестр крупных операторов, автоматический реестр нарушений безопасности ПДн, контроль критических объектов переходит к КНБ.
- **С 29 августа** — Национальный антикризисный план реагирования на инциденты кибербезопасности: владельцы КВОИКИ обязаны утвердить планы реагирования, сохранять цифровые следы, назначить ответственного и передать планы регулятору.
- **Штрафы утроены:** 1000 МРП за нарушения по кибербезопасности, 2000 МРП по ПДн, срок давности — год. Типовые нарушения при проверках: нет согласий, нет MFA, нет криптозащиты и антивируса. Ежегодное обучение сотрудников по ИБ стало обязательным.

Если ваша организация обрабатывает более 10 тыс. субъектов ПДн — вы уже «средний оператор» с новыми обязанностями. Подробнее о требованиях — в статье Закон о персональных данных РК: что делать, контроль каналов утечек — DLP.

Мир

Ransomware и утечки

964

жертв на сайтах вымогателей в июле (Check Point)

+87 % г/г

2 336

атак на организацию в неделю (Check Point, июль)

+16 % г/г

$4,99 млн

средняя стоимость утечки (IBM 2026)

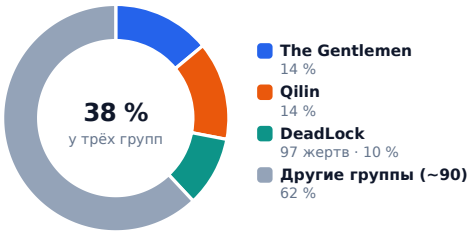
+12 %, рекорд

31 %

взломов начинаются с эксплуатации уязвимости (Verizon DBIR 2026)

впервые вектор № 1

Жертвы ransomware по регионам, июль 2026. Источник: Check Point, 12.08.2026.



Доля групп в жертвах, июль 2026. Источник: Check Point, 12.08.2026.

По ransomware.live август ещё выше июля: 709 жертв против 618. NCC Group насчитала в июле 894 инцидента — максимум 2026 года. За II квартал Check Point Research зафиксировал 2 139 жертв (+33 % г/г) и 93 активные группы. Самые атакуемые отрасли: образование (4 848 атак в неделю на организацию), госсектор (3 044), энергетика (2 759).

Растёт доля «вымогательства без шифрования»: украли данные — требуют выкуп за непубликацию. Платят около 23 % жертв.

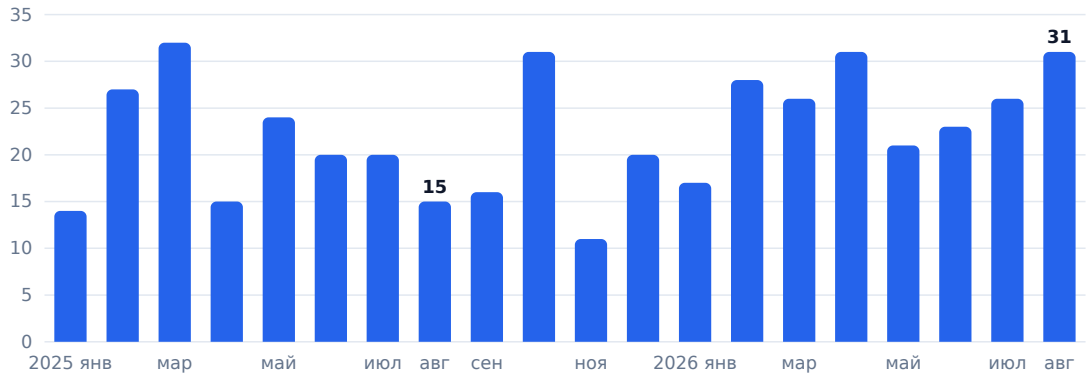
Инциденты августа

- **McKesson** (28 августа): вишинг сотрудников → компрометация Okta → выгрузка из Salesforce и Snowflake. Заявлено 284 млн записей пациентов, требование $55 млн. Группа ShinyHunters.
- **Manchester Airports Group** (27 августа): данные 8,7 млн пассажиров трёх аэропортов.
- **Boston Scientific** (26 августа): остановка производства и отгрузок медизделий по всему миру.
- **ТЭЦ в Польше** (раскрыто 8 августа): вход через VPN ветропарка, далее через сотовый APN оператора к SCADA, контроллеры Siemens переведены в STOP. Первый задокументированный переход из ИТ в технологическую сеть через мобильную сеть.
- **Электростанция в Великобритании:** остановлена на 4 дня иранской группой.
- **Cl0p и PTC Windchill:** массовое вымогательство через zero-day в системе управления инженерными данными. Среди 40+ жертв — Shell, GE, Philips.
- **Medusa:** по данным CISA и ФБР, взломано более 500 организаций критической инфраструктуры США.

Тренд, который касается всех: атаки на энергетику и промышленность переходят от кражи данных к физическому эффекту. Для Казахстана с его ТЭЦ, ГРЭС и горно-металлургическим сектором это прямой сигнал сегментировать технологические сети и закрывать удалённый доступ. См. NGFW и сегментация.

Уязвимости: август — рекорд за полтора года

Каталог CISA KEV (Known Exploited Vulnerabilities) — список уязвимостей с подтверждённой эксплуатацией в реальных атаках. Это самый практичный индикатор: не «сколько CVE опубликовано», а «что реально ломают».



Уязвимости, добавленные в CISA KEV по месяцам, январь 2025 — август 2026. Источник: каталог CISA KEV, версия от 2 сентября 2026.

- **31 запись за август 2026** — максимум с марта 2025. В августе 2025-го было 15.
- **За январь–август 2026 — 203 записи против 167** за тот же период 2025 года (+22 %).
- **6 из 31 — старые CVE 2015–2023 годов** (Red Hat libuser, ядро Linux, Microsoft SQL Server, ownCloud, Ajax.NET). Злоумышленники добивают то, что не обновляли годами. Инвентаризация и управление уязвимостями важнее охоты за zero-day.
- **Периметр под ударом.** За июль–август в KEV попали Cisco ASA/FTD и FMC, Citrix NetScaler, Fortinet FortiOS и FortiSandbox, SonicWall SMA1000, Check Point SmartConsole, Arista VeloCloud. Это устройства, которые смотрят в интернет в каждой организации.
- **Инструменты ИТ и разработки:** N-able N-central, JetBrains TeamCity, Gitea, JFrog Artifactory, PaperCut, Metabase, Zimbra, VMware vCenter. Взлом системы управления даёт доступ сразу ко всей инфраструктуре.
- **ИИ-стек стал целью:** Langflow, MLflow, Ray — три платформы для ИИ-приложений за один месяц. Если запускаете свои LLM-сервисы, см. защиту ИИ.

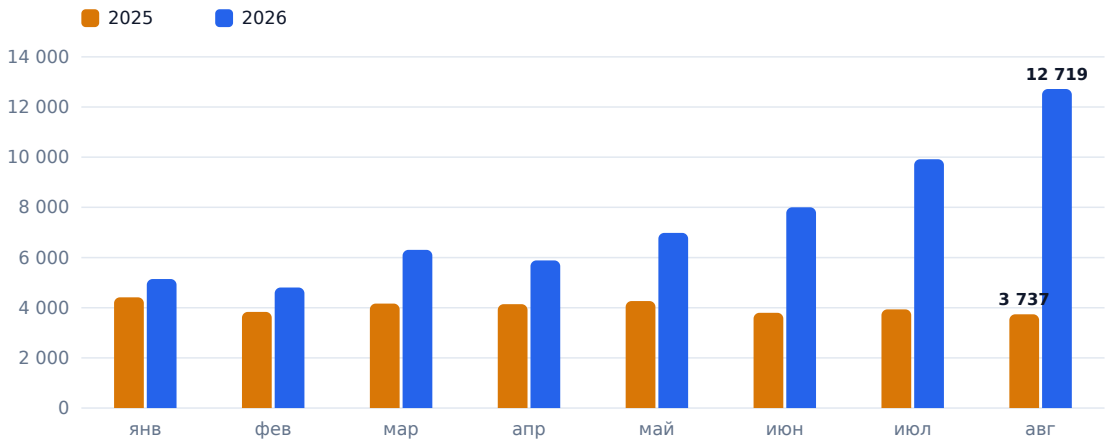
Записи CISA KEV за август 2026 по классам продуктов: серверы и ИТ-софт (TeamCity, vCenter, Zimbra, PaperCut…), ОС и ядро (Windows, Linux, macOS), периметр и VPN (Cisco ASA, Citrix, IKEv2), ИИ-платформы (Langflow, MLflow, Ray). Источник: каталог CISA KEV, версия от 2 сентября 2026.

Что патчить в первую очередь

CVE	ПРОДУКТ	ЧТО ПРОИСХОДИТ
CVE-2026-8452, CVE-2026-19490	Citrix NetScaler ADC / Gateway	Вебшеллы на взломанных шлюзах; обход аутентификации, эксплуатация ожидается
CVE-2026-20349	Cisco ASA / FTD (SSL VPN)	Эксплуатируется: перезагрузка устройства, отказ VPN
CVE-2026-33824	Windows IKEv2 (IKEEXT)	RCE 9.8 на VPN-серверах, эксплуатируется; патч вышел ещё в апреле
CVE-2026-68820	Windows afd.sys	Zero-day августовского Patch Tuesday, использовался группой Lazarus
CVE-2026-50522	Microsoft SharePoint Server	RCE 9.8, кража machine keys и вебшеллы с 21 июля
CVE-2026-59310	VMware vCenter	RCE 9.8, эксплуатация через 5 дней после раскрытия, 361 жертва в 47 странах
CVE-2026-73570	Zimbra Collaboration Suite	Pre-auth RCE через SNMP, не менее 274 взломанных серверов
CVE-2026-21962	Oracle HTTP Server / WebLogic	CVSS 10.0, более 140 тыс. попыток за 12

CVE	ПРОДУКТ	ЧТО ПРОИСХОДИТ
		дней, госсети 100+ стран
CVE-2025-68686	Fortinet FortiOS SSL-VPN	Обход патча symlink-персистентности, эксплуатируется
CVE-2026-72529/72530	TrueConf Server	Подмена инсталляторов клиентов — supply chain

Августовский Patch Tuesday Microsoft — 421 CVE, из них 62 критических (по Qualys), три zero-day. Palo Alto Networks закрыла 11 CVE в PAN-OS и GlobalProtect без активной эксплуатации.



Число опубликованных CVE по месяцам (NVD), январь–август, 2025 против 2026. Источник: API NVD, запрос от 2 сентября 2026.

Общий поток CVE растёт быстрее, чем KEV: в августе 2026 NVD опубликовала 12 719 записей против 3 737 годом ранее. Kaspersky фиксирует рекорд регистраций критических уязвимостей (5,2 тыс. за полугодие, +47 %) и связывает это с поиском багов с помощью ИИ. Практический вывод: закрыть всё невозможно. Приоритизировать нужно по KEV, EPSS и доступности из интернета, а не по CVSS.

ИИ в атаках: три факта

- Check Point: число prompt-injection-нагрузок выросло в 5 раз за квартал, уязвимости найдены в 40 % из 10 тыс. MCP-серверов; при взломе 9 госорганов Мексики ИИ-агент выполнил 5 317 команд за 34 сессии.
- IBM: каждая четвёртая вредоносная утечка — с применением ИИ, её цена на $1 млн выше средней. Более 20 % организаций сообщили о взломе своих ИИ-моделей или приложений.
- Kaspersky: 92 тыс. атак вредоносным ПО под видом ИИ-сервисов за январь–май, фейковый ChatGPT — 49 %. На малый бизнес — в 5 раз больше, чем в 2025.

Что сделать в сентябре

1. Проверить периметр по таблице выше: Citrix, Cisco, Fortinet, Zimbra, vCenter, SharePoint, IKEv2. Обновить и проверить журналы на вебшеллы и новые учётные записи.
2. Закрыть старые CVE: пройтись сканером по серверам с Linux, SQL Server, ownCloud — 6 из 31 записей KEV августа старше трёх лет.
3. Если обрабатываете более 10 тыс. субъектов ПДн — проверить готовность к новым правилам: реестр, уведомление за 1 рабочий день, MFA, шифрование, согласия.
4. Владельцам КВОИКИ — утвердить план реагирования на инциденты по антикризисному плану от 29 августа.
5. Провести обязательное обучение сотрудников по ИБ. Вишинг стал главным входом для ShinyHunters, а фейковые ИИ-сервисы — для малого бизнеса.
6. Включить логи периметра и серверов в SIEM: при инциденте без журналов расследовать нечего.

Нужна проверка периметра или подготовка к требованиям по ПДн — напишите нам, оценим за один день.

Источники

- CISA KEV: cisa.gov/known-exploited-vulnerabilities-catalog (версия 2026.09.02); NVD API: services.nvd.nist.gov.
- KZ-CERT через finprom.kz: kapital.kz, inbusiness.kz, newsroom.kz (14.08.2026); МВД РК: inbusiness.kz (21.08.2026), kazpravda.kz (02.07.2026).
- Bitdefender, SilkParasite (19.08.2026); Kaspersky GReAT, OctLurk/SilkLurk (30.07.2026); Kaspersky Securelist Q2 2026; F6 (15.07.2026).
- Регуляторика: zakon.kz, kapital.kz (07.08.2026), kt.kz (19.08.2026), sputnik.kz (20.08.2026).
- Check Point Research (12.08 и 13.08.2026); NCC Group Threat Pulse (26.08.2026); ransomware.live; IBM Cost of a Data Breach 2026 (29.07.2026); Verizon DBIR 2026; SecurityWeek, Qualys (Patch Tuesday 11.08.2026); The Hacker News, BleepingComputer, Help Net Security (инциденты и CVE августа).

© Genius Systems, 2026 · ИБ-дайджест за август 2026 · gensystems.kz · +7 777 746 2422 · info@gensystems.kz · Усть-Каменогорск, ул. М. Горького 57, оф. 412