MSSP GLOBAL

Отчет по мониторингу событий информационной безопасности

Август, 2025 г.

рег. №452/1 от 08.09.25 г.

DOC ID KZBW2Z12025000015 14DB1D6C3

DOC ID KZBW2Z12025000015 14DB1D6C3
Электронный документ подписан в Document

Содержание

Оглавление

1. Введение 3
2. Определения 4
3. Источники событий 6
4. Классификация событий ИБ 10
5. Результат мониторинга 11
6. Рекомендации 166
7. Заключение 177

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

1. Введение

В рамках Договора о государственных закупках услуг №6 от 10.02.2025 года, заключенного между КГУ «Управление цифровых технологий акимата Северо-Казахстанской области» *(далее - Заказчик)* и ТОО «MSSP.GL» *(далее - Исполнитель)*, за период август 2025 года Исполнителем, в соответствии с технической спецификацией, были оказаны следующие услуги по мониторингу событий информационной безопасности *(далее - ИБ)*, в состав которых входят работы:

- Круглосуточный мониторинг событий ИБ [1] в режиме 24/7/365 и техническая поддержка;

- Проведение процедур по первичной аналитике и реагированию инцидентов ИБ;

- Обеспечение защищенных каналов взаимодействия между Заказчиком и Поставщиком;

- Мониторинг состояния защищенных каналов передачи журналов событий:

- Выдача рекомендаций по устранению инцидентов ИБ и дальнейшему их предупреждению.

[1] Событие информационной безопасности - состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объекта информатизации

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z1202500001514DB1D6C3

2. Определения

В настоящем документе использованы следующие определения:

Информационная безопасность (ИБ) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Оперативный центр информационной безопасности (ОЦИБ) – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.

Национальный координационный центр информационной безопасности (НКЦИБ) – структурное подразделение акционерного общества "Государственная техническая служба".

Платформа информационного взаимодействия Национального координационного центра информационной безопасности (платформа взаимодействия ОЦИБ-НКЦИБ) – программное обеспечение, предназначенное для обмена данными и информацией об угрозах и инцидентах ИБ с НКЦИБ.

Источник событий ИБ – устройства, генерирующие события (операционные системы, базы данных, прикладное программное обеспечение, средства защиты информации, сетевое и серверное оборудование).

Событие ИБ – состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объекта информатизации.

Security Information and Event Management (SIEM) – система мониторинга и управления событиями ИБ.

НКЦИБ – Национальный координационный центр информационной безопасности акционерного общества «Государственная техническая служба».

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

АО «ГТС» – Акционерное общество «Государственная техническая служба».

Инцидент ИБ – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов.

IP-адрес – уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP.

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

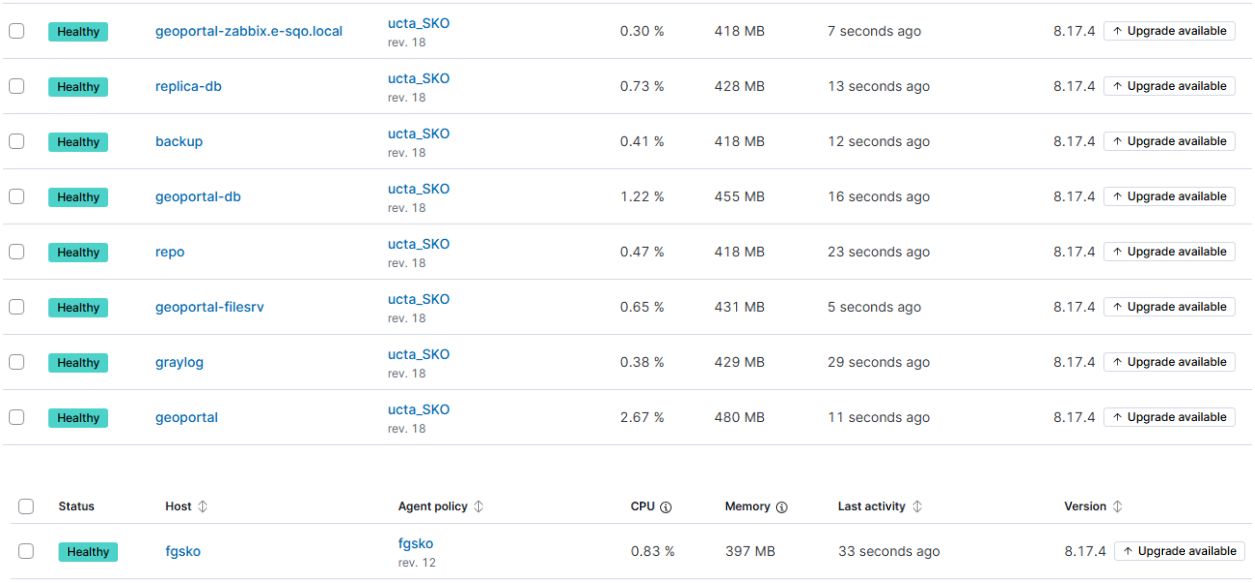
3. Источники событий

Заказчиком были заявлены и подключены к системе мониторинга Исполнителя следующие источники событий:

Наименование устройства	IP – адрес	ОС	Назначение
geoportal	172.21.1.2	Ubuntu 20.04.6 LTS	Сервер приложения
geoportal-db	172.21.1.3	Ubuntu 20.04.6 LTS	Сервер БД
graylog	172.21.1.4	Ubuntu 20.04.6 LTS	Сервер логирования
backup	172.21.1.5	Ubuntu 20.04.6 LTS	Сервер бэкапирования
geoportal-zabbix.e-sqo.local	172.21.1.6	Oracle Linux Server(9.6)	Сервер мониторинга
geoportal-filesrv	172.21.1.9	Ubuntu 20.04.6 LTS	Файловый сервер
repo	172.21.1.10	Ubuntu 20.04.6 LTS	Сервер репозитория
replica-db	172.21.1.11	Ubuntu 20.04.6 LTS	Сервер репликации
Fortigate-40F	172.21.1.1	FortiOS v6.4.14	Fortigate

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business



	Status	Host	Agent policy	CPU	Memory	Last activity	Version
	Healthy	geoportal-zabbix.e-sqo.local	ucta_SKO rev. 18	0.30 %	418 MB	7 seconds ago	8.17.4 Upgrade available
	Healthy	replica-db	ucta_SKO rev. 18	0.73 %	428 MB	13 seconds ago	8.17.4 Upgrade available
	Healthy	backup	ucta_SKO rev. 18	0.41 %	418 MB	12 seconds ago	8.17.4 Upgrade available
	Healthy	geoportal-db	ucta_SKO rev. 18	1.22 %	455 MB	16 seconds ago	8.17.4 Upgrade available
	Healthy	repo	ucta_SKO rev. 18	0.47 %	418 MB	23 seconds ago	8.17.4 Upgrade available
	Healthy	geoportal-filesrv	ucta_SKO rev. 18	0.65 %	431 MB	5 seconds ago	8.17.4 Upgrade available
	Healthy	graylog	ucta_SKO rev. 18	0.38 %	429 MB	29 seconds ago	8.17.4 Upgrade available
	Healthy	geoportal	ucta_SKO rev. 18	2.67 %	480 MB	11 seconds ago	8.17.4 Upgrade available
	Healthy	fgsko	fgsko rev. 12	0.83 %	397 MB	33 seconds ago	8.17.4 Upgrade available

Рисунок 1. Агенты, подключенные к системе мониторинга Заказчика

Мониторинг состояния защищенных каналов передачи журналов событий (Рис. 2).

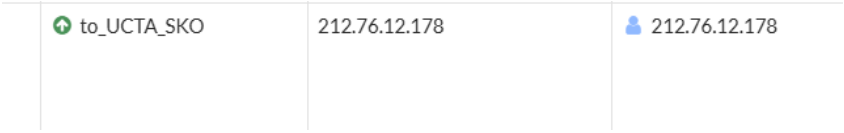


Рисунок 2. Мониторинг туннеля [Заказчик – Исполнитель] для сбора событий ИБ

Рекомендации:

Fortinet выпустил обновление для исправления критической уязвимости в продукте FortiSIEM с идентификатором CVE-2025-25256 (CVSS 9.8 из 10), которая активно эксплуатируется злоумышленниками.

Затронутые версии:

- FortiSIEM 5.4 (все версии)
- FortiSIEM 6.1 (все версии)
- FortiSIEM 6.2 (все версии)
- FortiSIEM 6.3 (все версии)
- FortiSIEM 6.4 (все версии)
- FortiSIEM 6.5 (все версии)

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

• FortiSIEM 6.6 (все версии)

• FortiSIEM 6.7.0 – 6.7.9 (обновить до 6.7.10 или выше)

• FortiSIEM 7.0.0 – 7.0.3 (обновить до 7.0.4 или выше)

• FortiSIEM 7.1.0 – 7.1.7 (обновить до 7.1.8 или выше)

• FortiSIEM 7.2.0 – 7.2.5 (обновить до 7.2.6 или выше)

• FortiSIEM 7.3.0 – 7.3.1 (обновить до 7.3.2 или выше)

Рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации. При отсутствии возможности обновления рекомендуется ограничить доступ к службе phMonitor (TCP-порт 7900) только доверенными внутренними хостами/IP-адресами.

В WinRAR обнаружена уязвимость высокой степени критичности с идентификатором CVE-2025-8088 (CVSS 8.4 из 10), позволяющая злоумышленнику выполнять произвольный код при распаковке специально подготовленных архивов.

Затронутые версии:

• Все версии WinRAR до и включая 7.12 (включая Windows-версии командной утилиты RAR, UnRAR.dll и портируемый исходный код UnRAR)

Рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации.

Уязвимость CVE-2025-53779 связана с относительным обходом пути в Windows Kerberos, который может быть использован при уязвимой конфигурации делегированных сервисных учетных записей (dMSA) для повышения привилегий по сети.

Критические уязвимости:

• Azure OpenAI (CVE-2025-53767) – CVSS 10.0

• Microsoft Graphics Component (CVE-2025-50165) – CVSS 9.8

• Windows GDI+ (CVE-2025-53766) – CVSS 9.8

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

• Remote Desktop Server (CVE-2025-50171) – CVSS 9.1

• Azure Portal (CVE-2025-53792) – CVSS 9.1

Рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации.

В VMware VMXNET3 обнаружена критическая уязвимость с идентификатором CVE-2025-41236 (CVSS 9.3 из 10).

Затронутые продукты и версии:

• VMware ESXi 8.0.x до (не включая) ESXi80U2e-24789317 и ESXi80U3f-24784735

• VMware ESXi 7.0.x до (не включая) ESXi70U3w-24784741

• VMware Workstation 17.0.x до 17.6.4

• VMware Fusion 13.0.x до 13.6.4

Рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации. Дополнительно рекомендуется ограничить административный доступ внутри гостевых ОС до минимума, особенно для виртуальных машин с VMXNET3.

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

4. Классификация событий ИБ

В целях своевременного реагирования и принятия соответствующих мер по обеспечению ИБ, события ИБ в данной области подразделяются на три ключевые категории по уровню критичности.

Уровень критичности	Описание
Низкий	События ИБ, не оказывающие влияние на электронные информационные ресурсы, информационные системы, сети телекоммуникаций и другие объекты информатизации.
Средний	События ИБ, которые могут привести к ограничению доступности источника событий ИБ, ухудшению ситуации или негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.
Высокий	События ИБ, которые могут привести к серьезным нарушениям безопасности, существенному ухудшению условий функционирования информационных систем и инфраструктуры, а также неблагоприятным последствиям для организации.

Следует добавить, что аналитик ОЦИБ имеет полномочия самостоятельно определять уровень критичности, если считает, что инцидент может вызвать значительно отрицательные последствия.

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

5. РЕЗУЛЬТАТ МОНИТОРИНГА

Исполнитель осуществляет постоянный мониторинг всех подключённых к мониторингу элементов инфраструктуры Заказчика. Все зарегистрированные, подтвержденные инциденты ИБ направляются в НКЦИБ АО «ГТС» в соответствии с «Правилами обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности» утвержденных Приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19 марта 2018 года № 48/НҚ.

За отчетный период ОЦИБ Исполнителя было обработано 422 258 597 событий, зафиксировано 3 события ИБ (Таблица 1).

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

Таблица 1. Анализ выявленных событий ИБ в период мониторинга

№	Наименование события/инцидента ИБ	Дата и время уведомления	Описание	Уровень критичности	Векторы атак по MITRE ATT&CK	Статус инцидента
1	Linux Group Creation	20.08.2025 10:19	На хосте geoportal-zabbix.e-sqo.local (172.21.1.6) была создана группа chrony GID=994	Низкий	Persistence (TA0003))	Заказчик проинформирован, подтверждена легитимность активности.
2	Linux User Account Creation	20.08.2025 10:20	На хосте geoportal-zabbix.e-sqo.local (172.21.1.6) было инициировано создание пользователя chrony.	Низкий	Persistence (TA0003)	Заказчик проинформирован, подтверждена легитимность активности.
3	Successful SSH Authentication from Unusual User	20.08.2025 10:21	На хосте geoportal-zabbix.e-sqo.local (172.21.1.6) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя "adminkazgisa".	Низкий	Initial Access (TA0001)	Заказчик проинформирован, подтверждена легитимность активности.

DOC-[illegible]ZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

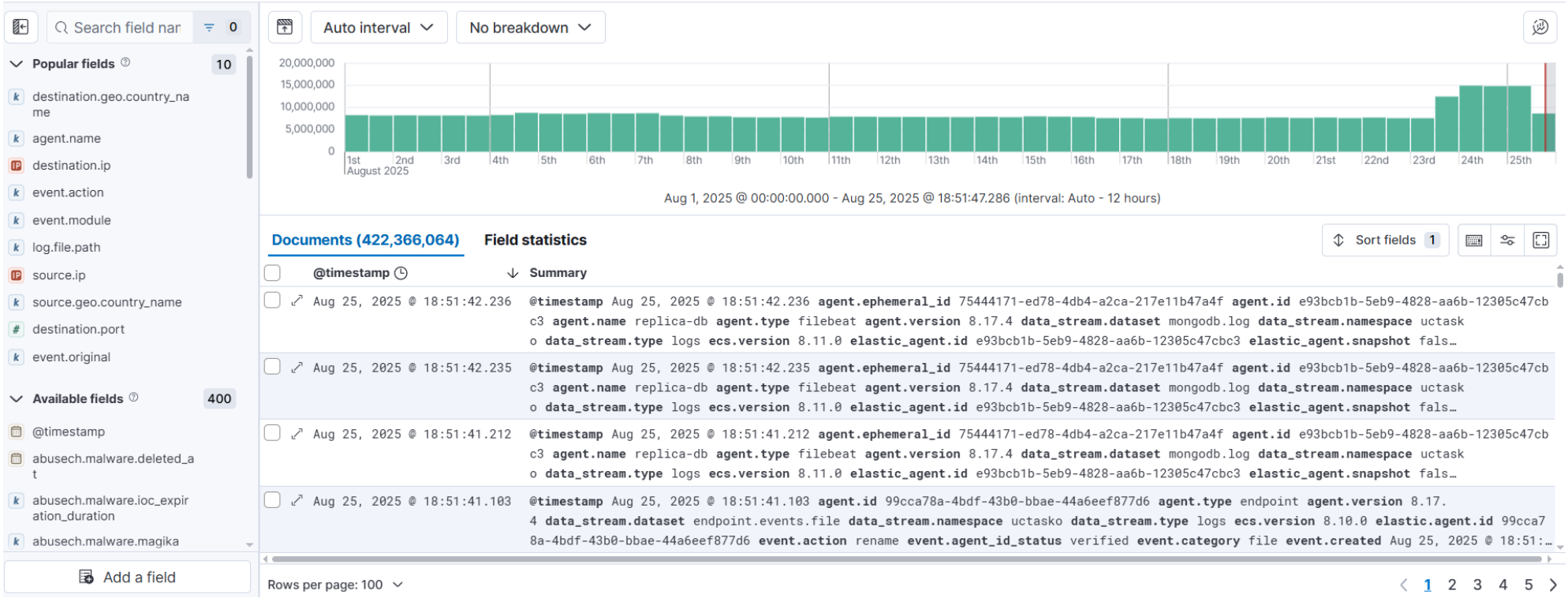


Рисунок 3. Поступление событий ИБ в систему мониторинга Исполнителя

DOCID: ZBW2Z12025000015 14DB1D6C3
Электронный документ подписан в Documentolog Business

На Рис. 4 указано количество зафиксированных событий ИБ по уровню критичности.

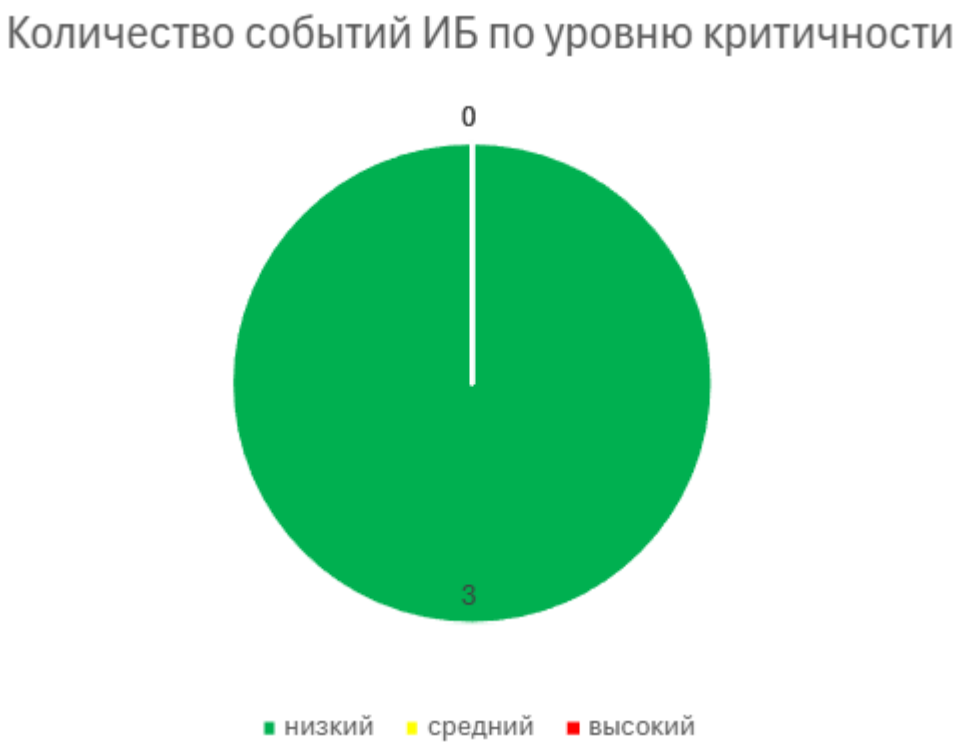
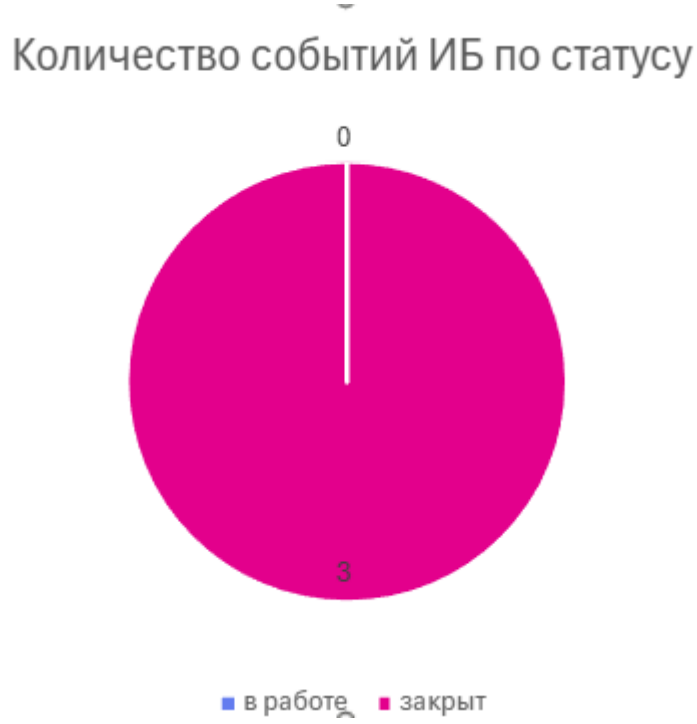


Рисунок 4. Кол-во зафиксированных событий ИБ по статусу



DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

На Рис. 5 представлено процентное соотношение количества генерируемых событий подключенными источниками: 19.64% основных событий направляет источник geoportal-db.

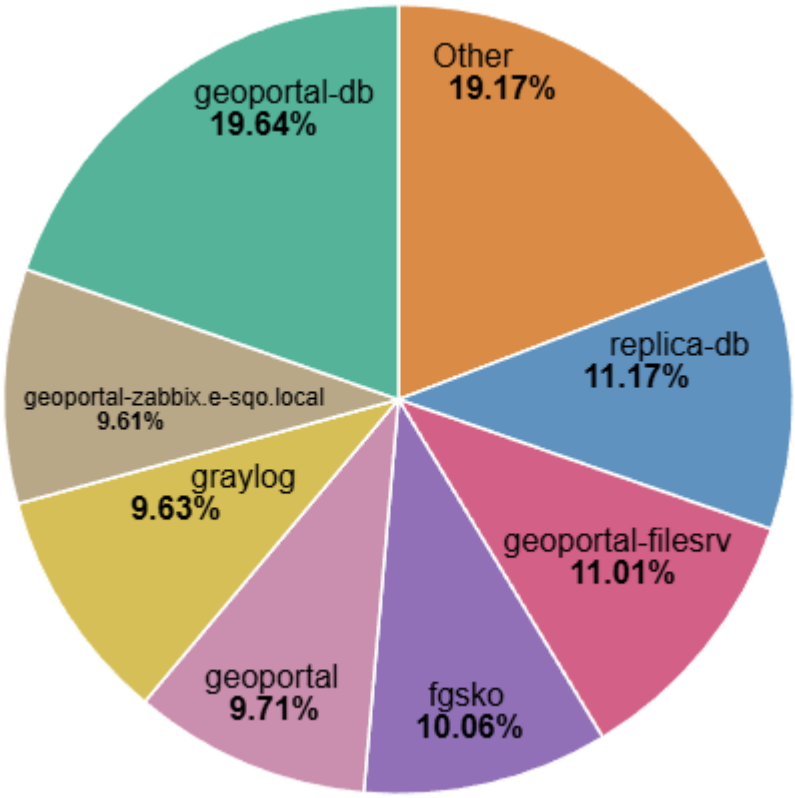


Рисунок 5. Агенты, направляющие основную часть событий ИБ

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

6. Рекомендации

1. Провести обновление рабочих станций, работающих на операционной системе (ОС) Windows 10 ввиду окончания официальной поддержки указанной версии. Устаревшие ОС несут высокие риски эксплуатации потенциальных новых угроз.

2. Провести инвентаризацию установленных систем и приложений на всех корпоративных хостах с проверкой актуальности версий.

3. Проверить отключение всех неиспользуемых сервисов, протоколов и портов.

4. Проверить соответствие настроек нестандартных портов документированным политикам безопасности (к примеру, заменить стандартные порты на иные).

5. Ограничить удаленный доступ защищенными каналами (VPN, SSH с двухфакторной аутентификацией).

6. Ограничить внешний доступ до корпоративных ресурсов только для казахстанского интернет-сегмента.

7. Убедиться, что используется многофакторная аутентификация для критических систем.

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

7. Заключение

В рамках оказания услуг за август 2025 года в заведенной за мониторинг информационно-коммуникационной инфраструктуре Заказчика инциденты ИБ не зарегистрированы.

DOC ID KZBW2Z1202500001514DB1D6C3

DOC ID KZBW2Z1202500001514DB1D6C3
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z1202500001514DB1D6C3
Тип документа	Исходящее письмо
Тема	Отчеты за август 2025 года. пароль передан исполнителю
Статус	Доставлен
Рег. Номер:	01-01/454
Рег. Дата:	08.09.2025
Количество страниц	18
Подписи	2

Информация об отправителе

Отправитель	ТОО "MSSP.GL"
IP-адрес	109.163.197.162

Информация о получателях

Получатель 1	КГУ «Управление цифровых технологий акимата Северо-Казахстанской области» , 055421500000, Казахстан

Информация о подписантах

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Генеральный директор
IP-адрес	109.163.197.162
Email	info@kazdream.kz
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWEQYJ...bHNf8sA==
Дата подписания	08.09.2025 13:32

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Генеральный директор
IP-адрес	109.163.197.162
Email	info@kazdream.kz
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWSAYJ...vPQYWEM0=

Дата подписания 08.09.2025 13:33

DOC ID KZBW2Z12025000001514DB1D6C3

DOC ID KZBW2Z12025000001514DB1D6C3
Электронный документ подписан в Documentolog Business