Отчет по мониторингу событий информационной безопасности

Октябрь, 2025 г.

рег. № 570/1 от 06.11.25 г.

DOC ID KZBW2Z120250000016 19B505679

DOC ID KZBW2Z120250000
Электронный докумен

Содержание

Оглавление

1. Введение.....3
2. Определения.....4
3. Источники событий.....5
4. Классификация событий ИБ.....6
5. Результаты мониторинга.....7
6. Рекомендации.....10
7. Заключение.....12

DOC ID KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

1. Введение

На основании технической спецификации к договору о государственных закупках услуг №6 от 10.02.2025 г., заключенному между КГУ «Управление цифровых технологий акимата Северо-Казахстанской области» *(далее - Заказчик)* и ТОО «MSSP.GL» *(далее - Исполнитель)*, в октябре 2025 года, Исполнителем были проведены следующие работы:

1. Мониторинг событий информационной безопасности:

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

- Проведение процедур по первичной аналитике и реагированию на инциденты ИБ;

- Обеспечение защищенных каналов взаимодействия между Заказчиком и Поставщиком;

- Мониторинг состояния защищенных каналов передачи журналов событий:

to_UCTA_SKO	212.76.12.178	212.76.12.178

Рисунок 1. Мониторинг туннеля [Заказчик – Исполнитель] для сбора событий ИБ

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

2. Мониторинг и анализ внешнего цифрового периметра.

- Осуществляется выявление потенциальных уязвимостей, автоматизированный учет активов, проверка ресурсов даркнета и хакерских форумов на предмет выявления утечек данных в пределах корпоративного сегмента, приоритизацию рисков;

- Заказчику предоставлен доступ к личному кабинету системы, для самостоятельной выгрузки, записи и сохранения отчетов сканирования;

- По результатам сканирования сформирован отчет по мониторингу и анализу внешнего цифрового периметра *(приложение 2 к письму)*.

[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 KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

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.

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».

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.

Malware Information Sharing Platform (MISP) — платформа с открытым исходным кодом для обмена информацией об угрозах ИБ.

DOC ID KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

3. Источники событий

Заказчиком были заявлены и подключены к системе мониторинга Исполнителя следующие хосты:

☐	Healthy	geoportal-zabbix.e-sqo.local	ucta_SKO rev. 25	0.33 %	471 MB	15 seconds ago	8.17.4	↑ Upgrade available
☐	Healthy	replica-db	ucta_SKO rev. 25	0.73 %	493 MB	31 seconds ago	8.17.4	↑ Upgrade available
☐	Healthy	backup	ucta_SKO rev. 25	0.34 %	484 MB	38 seconds ago	8.17.4	↑ Upgrade available
☐	Healthy	geoportal-db	ucta_SKO rev. 25	1.32 %	489 MB	14 seconds ago	8.17.4	↑ Upgrade available
☐	Healthy	repo	ucta_SKO rev. 25	0.45 %	472 MB	21 seconds ago	8.17.4	↑ Upgrade available
☐	Healthy	geoportal-filesrv	ucta_SKO rev. 25	0.40 %	474 MB	16 seconds ago	8.17.4	↑ Upgrade available
☐	Healthy	graylog	ucta_SKO rev. 25	0.42 %	474 MB	23 seconds ago	8.17.4	↑ Upgrade available
☐	Healthy	geoportal	ucta_SKO rev. 25	2.58 %	516 MB	15 seconds ago	8.17.4	↑ Upgrade available

Рисунок 2. Подключенные к системе мониторинга хосты Заказчика

DOC ID KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

4. Классификация событий ИБ

События ИБ подразделяются ключевые категории по уровню критичности, с целью своевременного реагирования и принятия соответствующих мер по обеспечению ИБ.

Уровень критичности	Признаки	Примеры инцидентов ИБ
Высокий (4)	Инциденты ИБ, которые приводят к невозможности предоставления услуг/выполнения работ, и (или) потере/модификации критичных* данных, и (или) нарушению конфиденциальности объекта информатизации, обрабатывающего критичные* данные.	- Несанкционированный доступ - Эксплуатация уязвимости - Шифровальщик - Вредоносное ПО - Отказ в обслуживании (DoS/DDoS-атака) И т.д.
Средний (3)	Инциденты ИБ, которые приводят к существенному ограничению предоставления услуг/выполнения работ, и (или) потере/модификации данных, не являющихся критичными*, и (или) нарушению конфиденциальности объекта информатизации, обрабатывающего данные, не являющихся критичными*.	- Несанкционированный доступ - Шифровальщик - Вредоносное ПО - Отказ в обслуживании (DoS/DDoS-атака) - Эксплуатация уязвимости И т.д.
Низкий (2)	Инциденты ИБ, не влияющие на предоставление услуги/выполнение работ.	- Вредоносное ПО - Отказ в обслуживании (DoS/DdoS-атака) - Эксплуатация уязвимости - Спам - Фишинговая атака И т.д.
Не определено (1)**	Влияние инцидента ИБ на предоставление услуг не определено	Нехарактерная/ подозрительная активность

Следует отметить, что аналитик ОЦИБ имеет полномочия самостоятельного определения уровня критичности, при необходимости, во избежание значительных отрицательных последствий.

DOC ID KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

5. РЕЗУЛЬТАТЫ МОНИТОРИНГА

Исполнитель осуществляет постоянный мониторинг событий ИБ, в отношении подключённой к SIEM информационно-коммуникационной инфраструктуры Заказчика.

Все зарегистрированные, подтвержденные инциденты ИБ направляются в адрес 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 были определены следующие показатели:

- Количество обработанных событий: **489 095 165;**
- Количество зафиксированных событий ИБ: **0.**

DOC ID KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

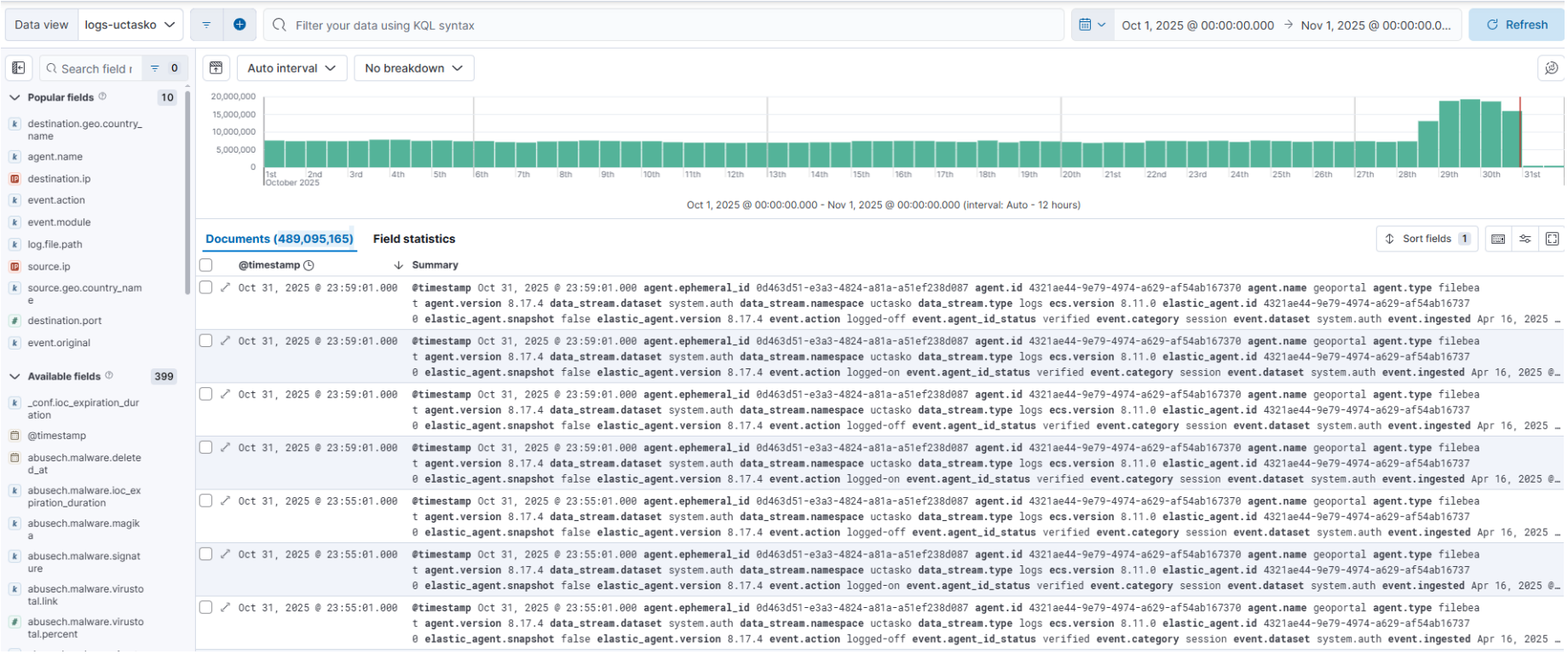

Рисунок 3. Количество обработанных событий ИБ за отчетный период

DOCID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

На рисунке 4 отображено процентное соотношение событий, генерируемых подключенными источниками.

Основная доля (50,8%) событий поступает от хоста graylog.

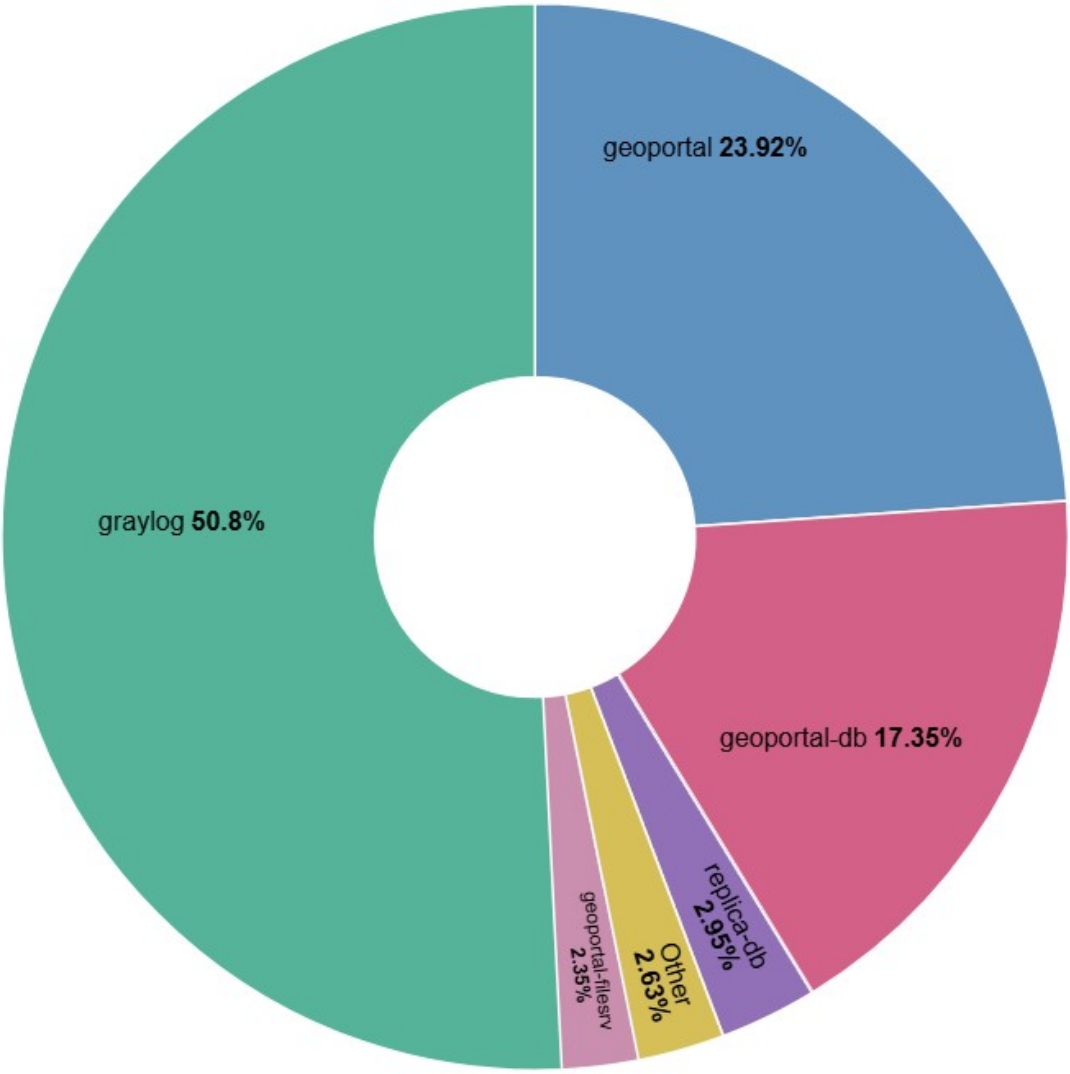

Рисунок 4. Источники, направляющие основную часть событий ИБ

DOC ID KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

6. Рекомендации

Комплекс мер по повышению уровня защищенности информационно-коммуникационной инфраструктуры Заказчика:

1. Запланировать 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. Внедрить процесс управления уязвимостями для своевременного устранения уязвимостей в инфраструктуре, при необходимости.
3. Установить график создания резервных копий критически важных производственных систем, при необходимости.
4. Провести проверку корпоративных учетных записей на предмет соблюдения корпоративной парольной политики и соблюдения принципа наименьших привилегий.
5. Внедрить двухфакторную аутентификацию для повышения безопасности пользователей в домене.

Рекомендации, разработанные на основе Threat Intelligence (TI) / данных MISP:

Уровень критичности: критический

Производитель: Microsoft Corporation

Известная эксплуатация: уязвимость внесена в каталог Cybersecurity & Infrastructure Security Agency (KEV) как известная эксплуатируемая. Также отмечены активные эксплуатации уязвимости в природе.

Краткое описание уязвимости

Уязвимость CVE 2025 59287 связана с ненадёжной десериализацией данных в компонентах сервера обновлений Windows Server Update Services (WSUS). Эксплуатация может позволить удалённому, неаутентифицированному злоумышленнику выполнить произвольный код с правами SYSTEM на уязвимом сервере.

Типы уязвимости

• Remote Code Execution (RCE)

• Information Disclosure (в процессе эксплуатации отмечено получение доменной информации)

• CWE-502: Deserialization of Untrusted Data

DOC ID KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

Затронутые версии и продукты:

• Windows Server 2012
• Windows Server 2012 R2
• Windows Server 2016
• Windows Server 2019
• Windows Server 2022 (включая редакцию 23H2)
• Windows Server 2025
(при условии, что на системе включена роль WSUS Server Role)

Рекомендации

Организациям, использующим затронутые версии, рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации.

DOC ID KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

7. Заключение

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

DOC ID KZBW2Z1202500001619B505679

DOC ID KZBW2Z1202500001619B505679
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z1202500001619B505679
Тип документа	Исходящее письмо
Тема	Отчеты за октябрь 2025 года, пароль передан исполнителю
Статус	Доставлен
Рег. Номер:	01-01/546
Рег. Дата:	06.11.2025
Количество страниц	13
Подписи	1

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”, sh.disimbaeva@sqo.gov.kz sh.disimbaeva@sqo.gov.kz

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	MIIWFwYJ...4jm/gTQ==
Дата подписания	06.11.2025 15:18

DOC ID KZBW2Z1202500001619B505679