MSSP GLOBAL

Отчет по мониторингу событий информационной безопасности

Сентябрь, 2025 г.

рег. № 505/1 от 06.10.2025 г.

DOC ID KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
Электронный документ подписан в Document

Содержание

Оглавление

1. Введение.....3
2. Определения.....4
3. Источники событий.....6
4. Классификация событий ИБ.....8
5. Результат мониторинга.....9
6. Рекомендации.....16
7. Заключение.....17

DOC ID KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
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 сентябре 2025 года, Исполнителем были проведены следующие работы, в рамках оказания услуги мониторинга событий информационной безопасности *(далее - ИБ):*

- 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:

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.

■

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 KZBW2Z1202500001571B3B7522
Электронный документ подписан в Documentolog Business
DOC ID KZBW2Z1202500001571B3B7522

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 информационной безопасности.

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)

DOC ID KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
Электронный документ подписан в Documentolog Business

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 KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
Электронный документ подписан в Documentolog Business

3. Источники событий

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

Healthy	geoportal-zabbix.e-sqo.local	ucta_SKO rev. 23	0.39 %	423 MB	13 seconds ago	8.17.4	↑ Upgrade available
Healthy	replica-db	ucta_SKO rev. 23	0.75 %	428 MB	28 seconds ago	8.17.4	↑ Upgrade available
Healthy	backup	ucta_SKO rev. 23	0.37 %	418 MB	31 seconds ago	8.17.4	↑ Upgrade available
Healthy	geoportal-db	ucta_SKO rev. 23	1.25 %	456 MB	21 seconds ago	8.17.4	↑ Upgrade available
Healthy	repo	ucta_SKO rev. 23	0.43 %	418 MB	26 seconds ago	8.17.4	↑ Upgrade available
Healthy	geoportal-filesrv	ucta_SKO rev. 23	0.68 %	431 MB	16 seconds ago	8.17.4	↑ Upgrade available
Healthy	graylog	ucta_SKO rev. 23	0.40 %	430 MB	35 seconds ago	8.17.4	↑ Upgrade available
Healthy	geoportal	ucta_SKO rev. 23	2.51 %	484 MB	34 seconds ago	8.17.4	↑ Upgrade available
Healthy	fgsko	fgsko rev. 15	0.82 %	398 MB	11 seconds ago	8.17.4	↑ Upgrade available

Рисунок 2. Агенты, подключенные к системе мониторинга Заказчика

Рекомендации:

Производитель: Cisco.

Уровень критичности: критический.

Известная эксплуатация: подтверждена CISA (Cybersecurity and Infrastructure Security Agency) и Cisco, уязвимости активно эксплуатируются в рамках кампании, связанной с ArcaneDoor.

Краткое описание уязвимостей

CVE-2025-20333 – уязвимость связана с некорректной валидацией пользовательского ввода в HTTP(S)-запросах веб-сервера VPN в Cisco ASA и Cisco FTD. Эксплуатация может позволить аутентифицированному удалённому злоумышленнику выполнить произвольный код с правами root, что может привести к полной компрометации устройства.

CVE-2025-20362 – уязвимость связана с некорректной валидацией пользовательского ввода в HTTP(S)-запросах веб-сервера VPN. Эксплуатация может позволить неаутентифицированному удалённому злоумышленнику

DOC ID KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
Электронный документ подписан в Documentolog Business

получить доступ к защищённым URL-эндпоинтам без прохождения аутентификации.

Типы уязвимостей:

• Remote Code Execution (RCE);

• Privilege Escalation;

• Authentication Bypass.

Затронутые версии и продукты:

• Cisco Adaptive Security Appliance (ASA) Software (включая аппаратные платформы ASA, ASA-SM, ASAv);

• Cisco Secure Firewall Threat Defense (FTD) Software (включая Firepower 2100, 4100, 9300).

Рекомендации:

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

DOC ID KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
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 KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
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 445 763 465 событий, зафиксировано 6 событий ИБ (Таблица 1).

DOC ID KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
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	Successful SSH Authentication from Unusual User	02.09.2025 01:51	На хосте "geoportal" (172.21.1.2) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя "adminkazgisa". Source IP - 10.200.200.1	Низкий	Initial Access (TA0001)	Заказчик проинформирован, подтверждена легитимность активности.
2	Unusual Remote File Creation	02.09.2025 11:34	На хосте geoportal-zabbix.e-sqo.local (172.21.1.6) был создан файл /home/adminkazgisa/OracleLinux-R9-U6-x86_64-dvd.iso пользователем adminkazgisa через процесс scp	Низкий	Lateral Movement (TA0008)	Заказчик проинформирован, подтверждена легитимность активности.
3	Attempt to Disable Syslog Service	07.09.2025 00:12	На хосте geoportal-zabbix.e-sqo.local (172.21.1.6) с помощью процесса systemctl, запущенного через родительский процесс sh от учетной записи "root" была запущена команда: /usr/bin/systemctl -s HUP kill	Низкий	Defence Evasion (TA0005)	Заказчик проинформирован, подтверждена легитимность активности.

DOC ID: KZBW2Z1202500001571B3B7522
Электронный документ подписан в Documentolog Business

Рисунок 3. Поступление событий ИБ в систему мониторинга Исполнителя

DOC ID: KZBW2Z1202500001571B3B7522
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

На Рис. 5 представлено процентное соотношение количества генерируемых событий подключенными источниками: 49.53% основных событий направляет источник geoportal-db.

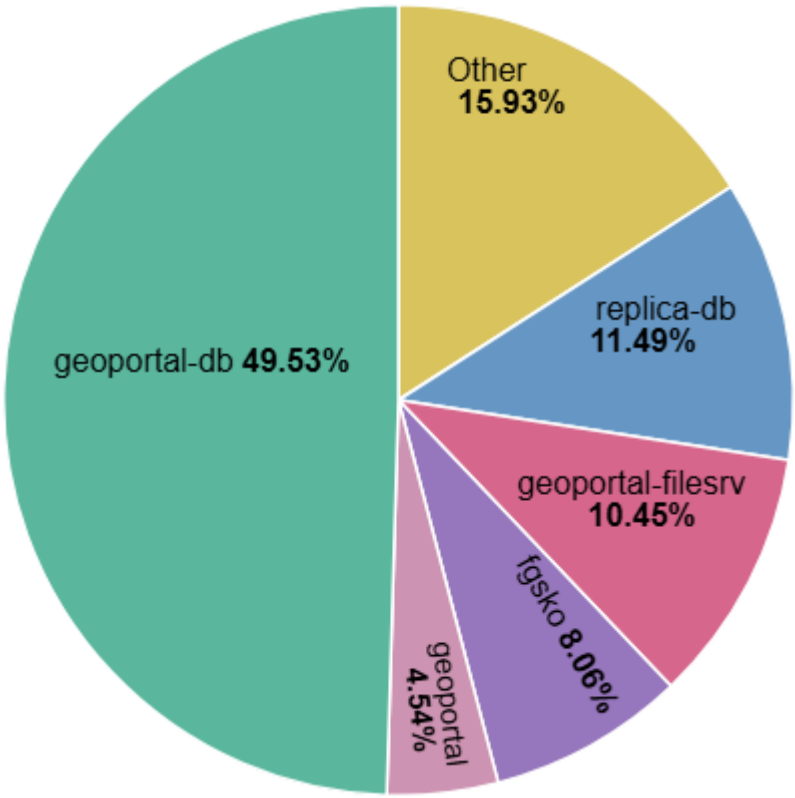

Рисунок 5. Агенты, направляющие основную часть событий ИБ

DOC ID KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
Электронный документ подписан в Documentolog Business

На Рис. 6 указано количество зафиксированных событий ИБ по статусу инцидента ИБ:

Закрыт: Заказчик проинформирован, подтверждена легитимность активности.

В работе: Заказчик проинформирован, ожидается обратная связь.

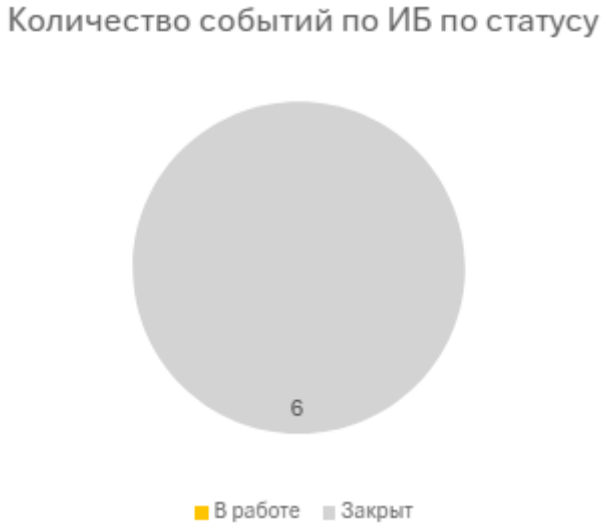

Рисунок 6. Количество зафиксированных событий ИБ по статусу

DOC ID KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
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 KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
Электронный документ подписан в Documentolog Business

7. Заключение

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

DOC ID KZBW2Z1202500001571B3B7522

DOC ID KZBW2Z1202500001571B3B7522
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z1202500001571B3B7522
Тип документа	Исходящее письмо
Тема	Отчеты за сентябрь 2025 года. Пароль передан исполнителю
Статус	Доставлен
Рег. Номер:	01-01/502
Рег. Дата:	06.10.2025
Количество страниц	16
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» , 211140037177, 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	MIIWOwYJ...TGdHKfw==
Дата подписания	06.10.2025 11:11

DOC ID KZBW2Z1202500001571B3B7522