MSSP GLOBAL
Информационная безопасность
и защита от киберугроз

ТОО «MSSP.GL»
БИН 150140024604
010000, Республика Казахстан, г.Астана,
улица Момышулы 2/1,10 этаж
Тел.: +7 700 333 06 45
email: info@mssp.global

Исх.№82
от 06.03.2025 г.

КГУ «Управление цифровых технологий акимата Северо-Казахстанской области»

Настоящим ТОО «MSSP.GL» выражает благодарность за плодотворное сотрудничество и направляет ежемесячный аналитический отчет по мониторингу событий информационной безопасности за февраль 2025 года.

Приложение: 1. Отчет, рег.№82/1 от 06.03.2025 г., на 10 л., 1 экз.

Генеральный директор **Джансенгиров Р. С.**

исп: Аубакирова Салтанат
e-mail: s.aubakirova@mssp.global

MSSP GLOBAL

Отчет по мониторингу событий информационной безопасности

Февраль, 2025 г.

рег. №82/1 от 06.03.25 г.

Содержание

Оглавление

1. Введение 3
2. Определения 4
3. Источники событий 6
4. Классификация событий ИБ 7
5. Результат мониторинга 8
6. Заключение 10

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 с февраль 2025 года Исполнителем, в соответствии с технической спецификацией, были оказаны следующие услуги по мониторингу событий информационной безопасности *(далее - ИБ)*, в состав которой входят следующие работы:

- Восстановление предоставления сервиса: анализ поступления корректности соединения между площадками и поступление событий с ранее подключенных событий 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;
- 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

2. Определения

В настоящем документы 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 информационной безопасности с НКЦИБ.

Источник событий ИБ – устройства, генерирующие события (операционные системы, баз 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

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.

3. Источники событий

Заказчиком были заявлены и подключены к системе мониторинга Поставщика 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
zabbix	172.21.1.6	Ubuntu 20.04.6 LTS	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

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, сетей телекоммуникаций и другие объекты информатизации.
Средний	События ИБ, которые могут привести к ограничению доступности источника события 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.

5. Результат мониторинга

Исполнитель осуществляет постоянный мониторинг всех подключённых к мониторингу элементов инфраструктуры Заказчика. Все зарегистрированные, подтвержденные инциденты ИБ направляются в НКЦИБ 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 745,493,899 событий, событий ИБ не зафиксированы (Таблица 1).

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	-	-	-	-	-	-

6. Заключение

В рамках оказания услуг за февраль 2025 года в, заведенной за мониторинг, информационно-коммуникационной инфраструктуре Заказчика не были зарегистрированы инциденты информационной безопасности.