MSSP GLOBAL

Отчет по мониторингу событий информационной безопасности

Октябрь, 2025 г.

рег. № 581/1 от 10.11.25 г.

Оглавление

1.Введение 3
2.Определения 5
3.Источники событий 6
4.Классификация событий ИБ 7
5.Результаты мониторинга 8
6.Рекомендации 13
7.Заключение 15

1. Введение

На основании технической спецификации к договору о государственных закупках услуг №11 от 17.04.2025 года, заключенному между КГУ «Ситуационный центр города Петропавловска» КГУ «Аппарат акима города Петропавловска» *(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 инцидентов ИБ;
- Обеспечение защищенных каналов взаимодействия между Заказчиком и Поставщиком;
- Мониторинг состояния защищенных каналов передачи журналов событий;

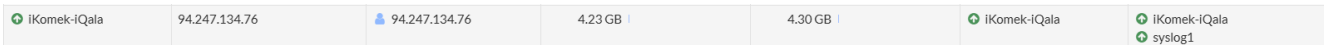

Рисунок 1. Мониторинг туннеля [Заказчик – Исполнитель] для сбора событий ИБ

- 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 мониторинга и анализа внешнего цифрового периметра *(приложение 2 к письму)*.

3. Онлайн-платформа для обучения кибербезопасности.

- В адрес Заказчика направлен запрос на предоставление информации в рамках подключения к онлайн-платформе Citizensec;
- Исполнителем предоставлен доступ для пользователей Заказчика;

[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

- Предоставлен доступ к обучающему материалу на казахском и русском языках;

- Подготовлены и направлены инструкции по входу и прохождению обучения на онлайн-платформе;

- В административной панели сформированы результаты прохождения обучения, реализована возможность управления доступами пользователей к обучающим материалам, а также доступно модерирование пользователей.

4. Система предотвращения утечки данных (DLP).

- Осуществлен подсчет числа агентов для дальнейшего развертывания системы DLP;

- Составлены системные требования, исходя из количества агентов;

- Передан комплект поставки программного обеспечения, включающего дистрибутивы, лицензии и аппаратный ключ;

- Развернут и настроен локальный сервер централизованного управления, активирована лицензия системы DLP и распространены агенты на рабочие станции.

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.

3. Источники событий

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

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	jardem	jardem rev. 25	94.88 %	198 MB	34 seconds ago	8.17.4 Upgrade available	
Healthy	ubuntu	iQala_SKO_NetDev rev. 20	0.18 %	193 MB	10 seconds ago	8.17.6 Upgrade available	
Healthy	appsko	iQala_SKO rev. 13	0.85 %	184 MB	10 seconds ago	8.17.6 Upgrade available	
Healthy	avroradb	iQala_SKO rev. 13	0.56 %	193 MB	31 seconds ago	8.17.6 Upgrade available	
Healthy	frontdb	iQala_SKO rev. 13	0.59 %	192 MB	13 seconds ago	8.17.6 Upgrade available	
Healthy	oldtime.integro.kz	iQala_SKO rev. 13	0.61 %	215 MB	9 seconds ago	8.17.6 Upgrade available	

Рисунок 2. Подключенные к системе мониторинга хосты Заказчика

4. КЛАССИФИКАЦИЯ СОБЫТИЙ ИБ

События ИБ подразделяются на 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.

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: **15 827 471**;
- Количество зафиксированных событий ИБ: **2**.

Таблица 1. Анализ выявленных событий ИБ в период мониторинга

	Наименование события ИБ	Дата и время уведомления	Описание	Уровень критичности	Векторы атак по MITRE ATT&CK	Статус инцидента
	Successful SSH Authentication from Unusual User	21.10.2025 23:36	На хосте vm12226 (10.8.0.50) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя "admin" Source IP - 37.150.27.184	Низкий	Initial Access (TA0001)	Заказчик проинформирован, подтверждена легитимность активности.
.	Potential External Linux SSH Brute Force Detected.	27.10.2025 15:37	С адреса 8.148.189.130 зафиксировано множество неудачных попыток входа по sshd под пользователем root на хосте vm12226 (10.8.0.50). Данный IP отмечен как вредоносный 1 антивирусным вендорам.	Низкий	Credential Access (TA0006)	Заказчик проинформирован, ожидается обратная связь.

Рисунок 3. Количество обработанных событий ИБ за отчетный период

На рисунке 4 представлено количество зафиксированных событий ИБ в разрезе уровней критичности.

Рисунок 4. Кол-во зафиксированных событий ИБ по уровни критичности

На рисунке 5 отображено процентное соотношение событий, генерируемых подключенными источниками.

Основная доля, в разрезе агентов:

(73,97%) событий поступает от хоста oldtime.integro.kz (IQala),

(100,00%) событий поступает от хоста jardem (Жардем).

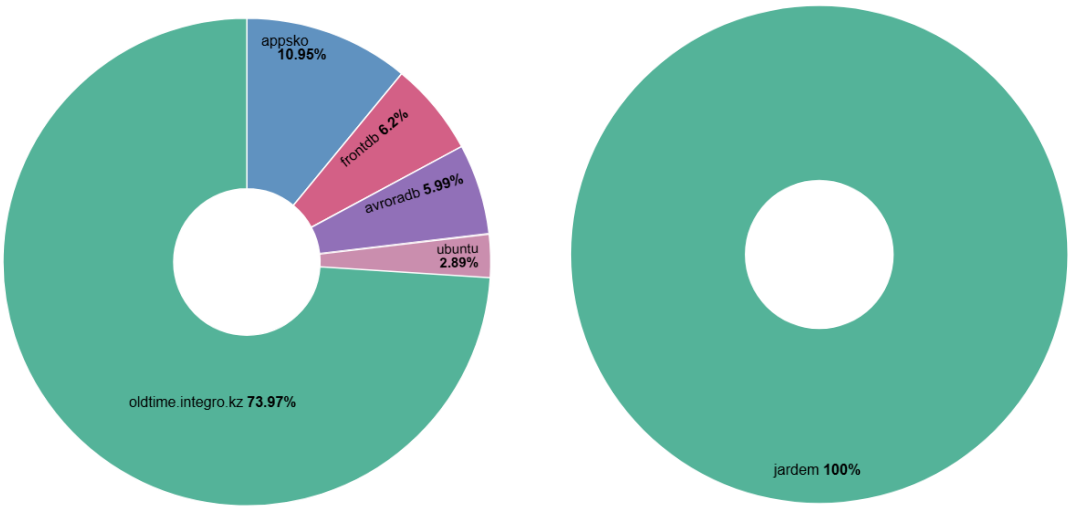

Рисунок 5. Источники, направляющие основную часть событий ИБ

На рисунке 6 представлено количество зафиксированных событий ИБ в разрезе их статуса инцидента ИБ:

– **Закрыт**: Заказчик проинформирован, легитимность активности подтверждена.

– **В работе:** Заказчик проинформирован, ожидается обратная связь.

Рисунок 6. Количество зафиксированных событий ИБ по статусу

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

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.

7. Заключение

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