MSSP GLOBAL

Отчет по мониторингу событий информационной безопасности

Апрель, 2026 г.

рег. №206/1 от 04.05.2026 г.

DOC ID KZBW2Z1202600001907 93EEBBA

DOC ID KZBW2Z120260000190793E
Электронный документ подпис

Содержание

1. Введение.....3
2. Определения.....4
3. Источники событий.....5
4. Классификация событий ИБ.....6
5. Результат мониторинга.....7
6. Рекомендация.....14
7. Заключение.....15

DOC ID KZBW2Z120260000190793EEBBA

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

1. Введение

В рамках договора №150540018634/260069/00 от 02.03.2026 г., заключенного между ГУ «Министерство туризма и спорта Республики Казахстан» *(далее - Заказчик)* и ТОО «MSSP.GL» *(далее - Исполнитель*), за апрель 2026 года Исполнителем, в соответствии с технической спецификацией, были оказаны услуги мониторинга событий информационной безопасности (далее - ИБ):

- Круглосуточный мониторинг событий ИБ 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:

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

- Выдача рекомендаций по устранению инцидентов ИБ и дальнейшему их предупреждению;
- Мониторинг всех доступных извне цифровых активов организации, с целью выявления уязвимостей, приоритезация критических рисков и отслеживание эффективности принимаемых мер;
- Предоставление доступа к онлайн-платформе повышения уровня осведомленности в области кибербезопасности и цифровой гигиены.

DOC ID KZBW2Z120260000190793EEBBA

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

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.

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.

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 KZBW2Z120260000190793EEBBA

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

3. Источники событий

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

Status	Host	Agent policy	CPU	Memory	Last activity	Version
Healthy	php.local	eqonaq rev. 9	2.53 %	208 MB	36 seconds ago	8.17.9
Healthy	mysql-server	eqonaq rev. 9	1.93 %	205 MB	35 seconds ago	8.17.9
Healthy	eqonaq.kz	eqonaq rev. 9	2.61 %	247 MB	12 seconds ago	8.17.9
Healthy	localhost	eqonaq_NetDev rev. 9	0.28 %	194 MB	38 seconds ago	8.17.9

Рисунок 2. Подключенные к системе мониторинга хосты Заказчика

DOC ID KZBW2Z120260000190793EEBBA

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

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.

DOC ID KZBW2Z120260000190793EEBBA

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

5. РЕЗУЛЬТАТ 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: **82 853 909;**
- Количество зафиксированных событий ИБ: **7.**

DOC ID KZBW2Z120260000190793EEBBA

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

№	Наименование события ИБ	Дата и время уведомления	Описание	Уровень критичности	Векторы атак по MITRE ATT&CK	Статус события ИБ
1	Hosts File Modified	01.04.2025 21:49	На хосте php.local (10.10.10.3) было инициировано создание файла hosts по пути \etc\ hosts.	Средний	T1565.001 (Stored Data Manipulation)	Заказчик проинформирован, ожидается обратная связь
2	Kill Command Execution	03.04.2025 20:26	Пользователь root на хосте eqonaq.kz-server (ip: 94.247.133.122) запустил команду sudo kill 2651534 2651540 2651543 2651544 с родительским процессом sudo.	Низкий	T1489 (Service Stop)	Заказчик проинформирован, подтверждена легитимность события
3	Potential Suspicious File Edit	11.04.2025 23:59	На хосте mysql-server (10.10.10.2) пользователем root было инициировано создание файла через процесс "vi" по пути: /etc/.passwd.swp	Низкий	T1565.001 (Stored Data Manipulation)	Заказчик проинформирован, подтверждена легитимность события
4	Security File Access via Common Utilities	13.04.2025 22:32	На хостах php.local (10.10.10.3) и mysql-server (10.10.10.2) был запущен процесс cat, пользователем root, инициированный родительским процессом bash была совершена попытка получить доступ к потенциально	Низкий	T1005 (Data from Local System)	Заказчик проинформирован, подтверждена легитимность

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

			чувствительным файлам, связанным с безопасностью системы. Это может свидетельствовать о попытке сбора информации о конфигурации системы или её безопасности. Использованные команды: php.local: cat /etc/security/faillock.conf cat /etc/pam.d/common-account cat /etc/pam.d/common-auth cat /etc/pam.d/common-password mysql-server: cat /etc/security/faillock.conf cat /etc/pam.d/common-account cat /etc/pam.d/common-auth cat /etc/pam.d/common-password cat /etc/security/faillock.conf cat /etc/pam.d/common-account cat /etc/pam.d/common-auth cat /etc/pam.d/common-password cat /etc/pam.d/common-auth cat /etc/pam.d/common-password cat /etc/security/faillock.conf cat /etc/pam.d/common-account cat /etc/pam.d/common-auth cat /etc/pam.d/common-password			события

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

5	Potential Suspicious File Edit	14.04.2025 22:32	На хосте php.local (10.10.10.3) пользователем root было инициировано создание файла через процесс "vi" по пути: /etc/.passwd.swp	Низкий	T1565.001 (Stored Data Manipulation)	Заказчик проинформирован, подтверждена легитимность события
6	SSH Key Generated via ssh-keygen	22.04.2025 11:36	На хосте localhost (ip: 10.10.10.1) от имени пользователя ilya был сгенерирован SSH ключ с помощью процесса ssh-keygen. Путь к ключу: /home/ilya/.ssh/id_rsa.pub	Низкий	T1098.004 (SSH Authorized Keys)	Заказчик проинформирован, подтверждена легитимность события
7	SSH Key Generated via ssh-keygen	22.04.2025 22:39	На хосте php.local (ip: 10.10.10.3) от имени пользователя root был сгенерирован SSH ключ с помощью процесса ssh-keygen. Путь к ключу: /root/.ssh/id_rsa	Низкий	T1098.004 (SSH Authorized Keys)	Заказчик проинформирован, подтверждена легитимность события

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

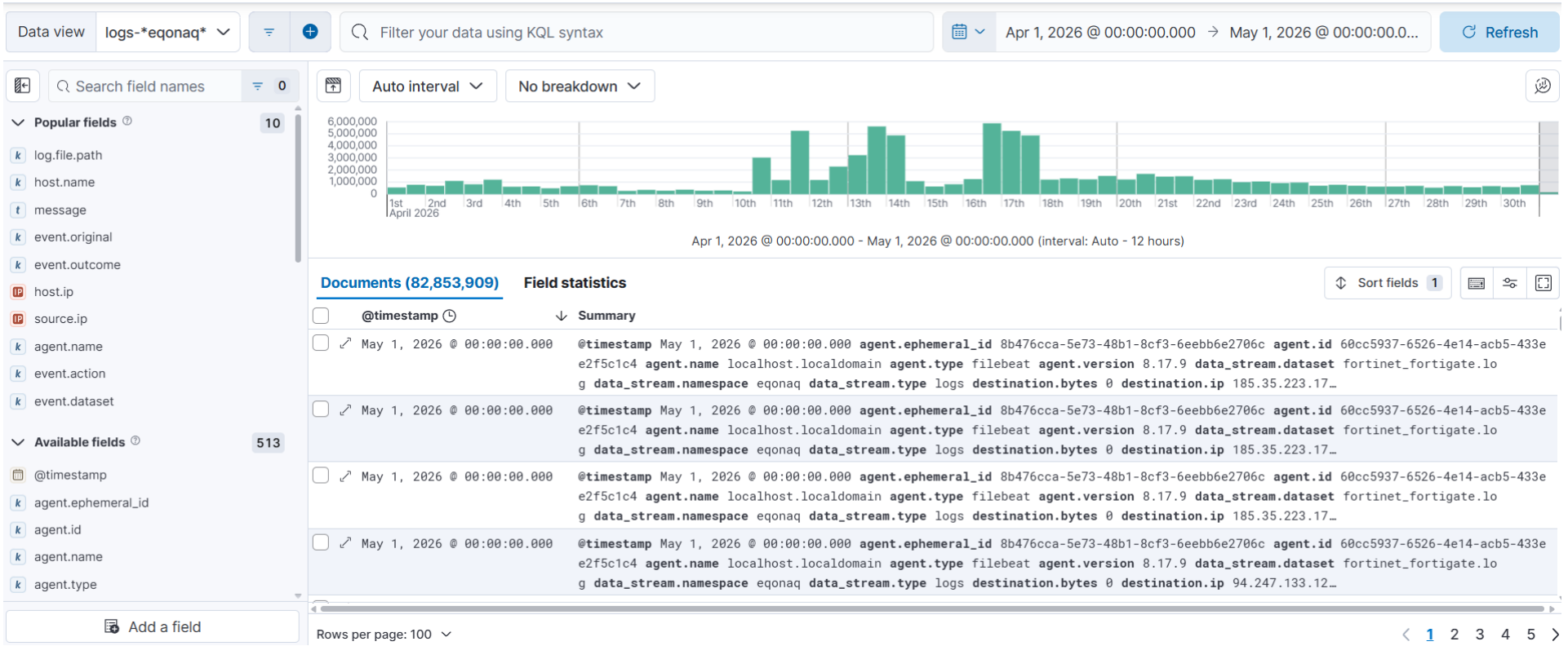

Рисунок 3. Поступление событий ИБ в систему мониторинга

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

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 (50,9%) событий поступает от хоста mysql-server.

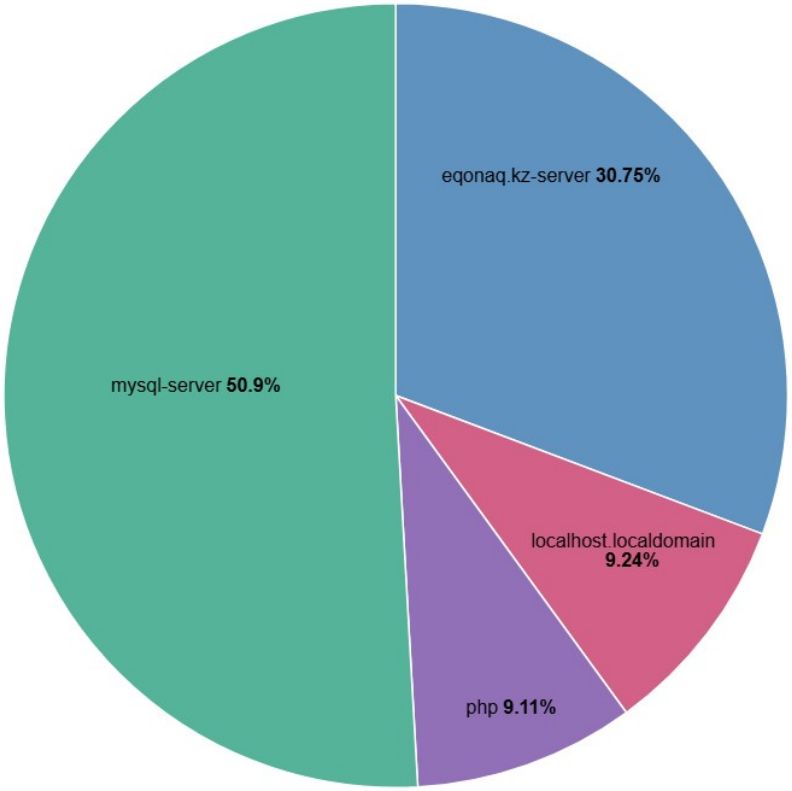

Рисунок 5. Агент, направляющий основную часть событий ИБ

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

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000190793EEBBA

- **Закрыт**: Заказчик проинформирован, легитимность активности подтверждена.
- **В работе:** Заказчик проинформирован, ожидается обратная связь.

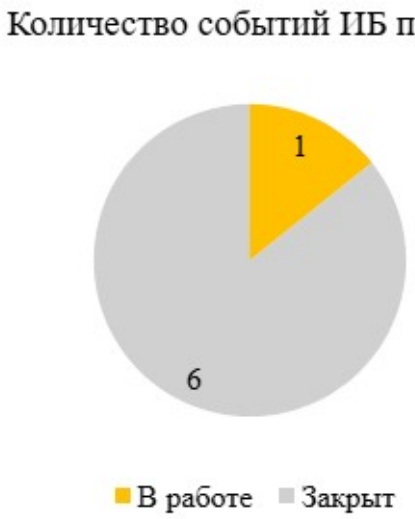

Рисунок 6. Количество зафиксированных событий ИБ по статусу

DOC ID KZBW2Z120260000190793EEBBA

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

6. РЕКОМЕНДАЦИЯ

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

1. Исключить прямой доступ к локальным серверам с публичных IP-адресов, обеспечив подключение пользователей исключительно через VPN;
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.

DOC ID KZBW2Z120260000190793EEBBA

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

7. ЗАКЛЮЧЕНИЕ

В рамках оказания услуг в заведенной за мониторинг информационно-коммуникационной инфраструктуре Заказчика в апреле 2026 года инциденты ИБ не зафиксированы.

DOC ID KZBW2Z1202600001907 93EEBBA

DOC ID KZBW2Z120260000190793EEBBA
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z120260000190793EEBBA
Тип документа	Исходящее письмо
Тема	Отчеты за апрель 2026 года
Статус	Отправлен
Рег. Номер:	01-01/155
Рег. Дата:	04.05.2026
Количество страниц	16
Подписи	2

Информация об отправителе

Отправитель	ТОО "MSSP.GL"
IP-адрес	109.163.197.162

Информация о получателях

Получатель 1	Министерство туризма и спорта Республики Казахстан, 012000100000, Казахстан
Получатель 2	Министерство туризма и спорта , t.akchabaev@tsm.gov.kz t.akchabaev@tsm.gov.kz
Получатель 3	Министерство туризма и спорта , r.kuderbaev@tsm.gov.kz r.kuderbaev@tsm.gov.kz

Информация о подписантах

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Генеральный директор
IP-адрес	109.163.197.162
Email	d.salipov@mssp.global
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWMAYJ...qBX8h19o=
Дата подписания	04.05.2026 16:58

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Генеральный директор

IP-адрес	109.163.197.162
Email	d.salipov@mssp.global
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWaQYJ...l/xlZkko=
Дата подписания	04.05.2026 16:59

DOC ID KZBW2Z120260000190793EEBBA