MSSP GLOBAL

Отчет по мониторингу событий информационной безопасности

Июль, 2026 г.
рег. №382/1 от 03.08.26г.

DOC ID KZBW2Z120260000002058D3C27AC

DOC ID KZBW2Z120260000002058D3C27AC
Электронный документ подписан в Documentolog Business

Содержание

1. Введение.....3
2. Определения.....4
3. Источники событий.....5
4. Классификация событий ИБ.....6
5. Результат мониторинга.....7
6. Рекомендация.....12
7. Заключение.....13

DOC ID KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
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 июль 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 (*см. Приложение 2*);
- Предоставление доступа к онлайн-платформе повышения уровня осведомленности в области кибербезопасности и цифровой гигиены.

DOC ID KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
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 KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
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
Healthy	php.local	eqonaq rev. 68	11.75 %	571 MB
Healthy	localhost.localdomain.mssp.local	eqonaq_NetDev rev. 17	1.11 %	659 MB
Healthy	mysql-server	eqonaq rev. 68	3.54 %	627 MB
Healthy	localhost	eqonaq rev. 68	3.78 %	705 MB

Рисунок 2. Подключенные к системе мониторинга хосты Заказчика

DOC ID KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
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 KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
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: 248 454 848;
- Количество зафиксированных событий ИБ: 2.

DOC ID KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
Электронный документ подписан в Documentolog Business

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 события ИБ
1	Successful SSH Authentication from Unusual IP Address	14.07.2026 13:58	На хосте localhost (10.10.10.1) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя "ilya".	Низкий	Initial Access (TA0001)	Заказчик проинформирован, подтверждена легитимность события
2	Cron Job Created or Modified	16.07.2026 17:11	На хосте php.local (ip: 10.10.10.3) пользователем root был создан или изменён запланированный запуск задачи через планировщик cron. Был переименован файл user с помощью процесса crontab на /var/spool/cron/crontabs/tmp.NaTiAv	Средний	Persistence (TA0003)	Заказчик проинформирован, подтверждена легитимность события

DOC ID KZBW2Z1202600002058D3C27AC
Электронный документ подписан в Documentolog Business

Рисунок 3. Поступление событий ИБ в систему мониторинга

DOC ID KZBW2Z12026000002058D3C27AC
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 (90,77%) событий поступает от хоста php.local.

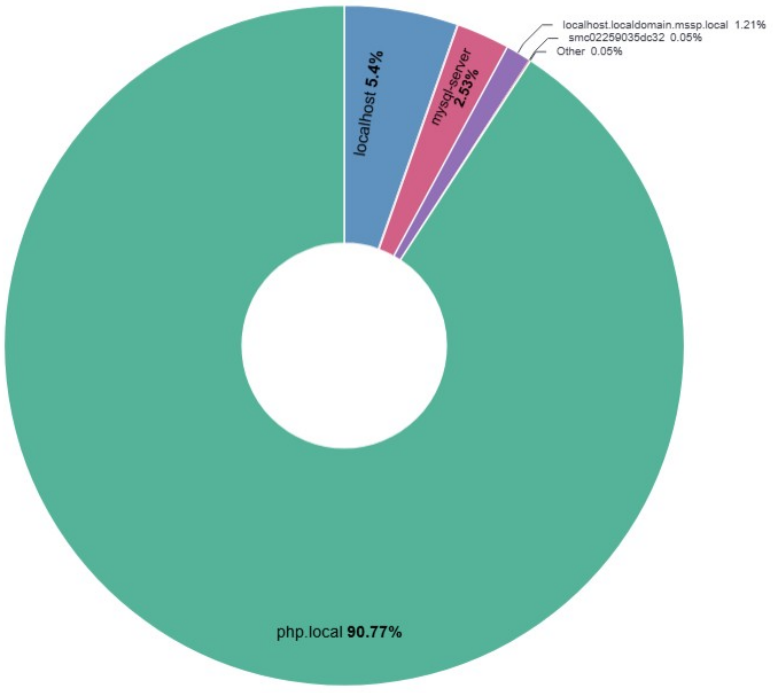

Рисунок 5. Агент, направляющий основную часть событий ИБ

DOC ID KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
Электронный документ подписан в Documentolog Business

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

DOC ID KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
Электронный документ подписан в Documentolog Business

6. Рекомендация

1. Обеспечить своевременное обновление всех компонентов информационно-коммуникационной инфраструктуры, включая операционные системы, программное обеспечение, серверное и сетевое оборудование, а также средства защиты информации. Устанавливать актуальные исправления безопасности и переводить используемые решения на поддерживаемые версии до завершения срока их официальной поддержки.
2. Организовать регулярное выявление и устранение уязвимостей в информационных системах, серверном и сетевом оборудовании с контролем сроков выполнения корректирующих мероприятий.
3. Проводить периодический пересмотр учетных записей и прав доступа, своевременно блокировать неиспользуемые учетные записи, исключать избыточные привилегии и соблюдать принцип минимально необходимых прав.
4. Использовать многофакторную аутентификацию и ограничивать удалённый доступ к критически важным системам, разрешая подключения только уполномоченным пользователям через защищённые каналы связи.
5. Обеспечить регулярное резервное копирование критически важных данных и систем, а также периодически проверять возможность восстановления информации из резервных копий

DOC ID KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
Электронный документ подписан в Documentolog Business

7. Заключение

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

DOC ID KZBW2Z1202600002058D3C27AC

DOC ID KZBW2Z1202600002058D3C27AC
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z1202600002058D3C27AC
Тип документа	Исходящее письмо
Статус	Доставлен
Рег. Номер:	01-01/295
Рег. Дата:	05.08.2026
Количество страниц	14
Подписи	1

Информация об отправителе

Отправитель	ТОО "MSSP.GL"
IP-адрес	185.143.21.26

Информация о получателях

Получатель 1	Министерство туризма и спорта РК kense@tsm.gov.kz
Получатель 2	Министерство туризма и спорта РК t.akchabaev@tsm.gov.kz
Получатель 3	Министерство туризма и спорта РК r.kuderbaev@tsm.gov.kz

Информация о подписантах

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Генеральный директор
IP-адрес	185.143.21.26
Email	d.salipov@mssp.global
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWoAYJ...qKW7xSfM8
Дата подписания	05.08.2026 10:20

DOC ID KZBW2Z1202600002058D3C27AC