Отчет по мониторингу событий информационной безопасности

Март, 2026 г.

рег. №158/1 от 03.04.2026 г.

DOC ID KZBW2Z1202600001880008E48A8

DOC ID KZBW2Z1202600001880008E
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.....16
7. Заключение.....17

DOC ID KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
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 март 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 KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
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 KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
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	Actions
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	

Рисунок 2. Подключенные к системе мониторинга хосты Заказчика

DOC ID KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
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 KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
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: **117 454 179;**
- Количество зафиксированных событий ИБ: **17.**

DOC ID KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z1202600001880008E48A8

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

№	Наименование события ИБ	Дата и время уведомления	Описание	Уровень критичности	Векторы атак по MITRE ATT&CK	Статус инцидента
1	Successful SSH Authentication from Unusual SSH Public Key	04.03.2026 12:01	На хосте eqonaq.kz (10.10.10.1) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя eqonaq. Source IP - 89.219.32.150	Низкий	Initial Access (TA0001)	Заказчик проинформирован, легитимность активности подтверждена.
2	Potential Non-Standard Port SSH connection	10.03.2026 19:12	На хосте eqonaq.kz (10.10.10.1) был запущен процесс ssh пользователем eqonaq с конечным IP 85.29.133.222	Низкий	Command and Control (TA0011)	Заказчик проинформирован, ожидается обратная связь.
3	Successful SSH Authentication from Unusual SSH Public Key	11.03.2026 20:04	На хосте eqonaq.kz-server (94.247.133.122) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя eqonaq. Source IP - 85.29.133.222	Низкий	Initial Access (TA0001)	Заказчик проинформирован, легитимность активности подтверждена.
4	Cron Job Created or Modified	17.03.2026 08:39	На хосте eqonaq.kz-server (94.247.133.122) ользователем eqonaq был создан или изменён запланированный запуск задачи через планировщик cron. Был переименован файл /var/spool/cron/crontabs/tmp.yN9Yn8 с помощью процесса crontab на	Средний	Persistence (TA0003) Privilege Escalation (TA0004) Execution	Заказчик проинформирован, легитимность активности подтверждена.

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

			/var/spool/cron/crontabs/eqonaq		(TA0002)	
5	Linux User Account Creation	18.03.2026 13:19	На хосте eqonaq.kz-server (94.247.133.122) было инициировано создание учетной записи пользователем tcpdump.	Низкий	Persistence (TA0003)	Заказчик проинформирован, ожидается обратная связь.
6	SSL Certificate Deletion	18.03.2026 13:19	На хосте eqonaq.kz-server (94.247.133.122) пользователем root была инициирована операция удаления SSL-сертификатов Chambers_of_Commerce_Root_-_2008.pem Cybertrust_Global_Root.pem DST_Root_CA_X3.pem EC-ACC.pem GeoTrust_Primary_Certification_Authority_-_G2.pem Global_Chambersign_Root_-_2008.pem GlobalSign_Root_CA_-_R2.pem Hellenic_Academic_and_Research_Institutions_RootCA_2011.pem Network_Solutions_Certificate_Authority.pem Sonera_Class_2_Root_CA.pem Staat_der_Nederlanden_Root_CA_-_G3.pem	Низкий	Defense Evasion (TA0005) Impact (TA0040)	Заказчик проинформирован, ожидается обратная связь.

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

			Trustis_FPS_Root_CA.pem VeriSign_Universal_Root_Certification_Authority.pem с помощью команды rm.			
7	Hosts File Modified	18.03.2026 22:15	На хосте eqonaq.kz-server (ip: 94.247.133.122) было инициировано создание файла hosts по пути \etc\hosts.	Средний	Impact (TA0040)	Заказчик проинформирован, легитимность активности подтверждена.
8	Successful SSH Authentication from Unusual SSH Public Key	19.03.2026 18:13	На хосте eqonaq.kz-server (10.10.10.1) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя ilya. Source IP - 42.1.103.41	Низкий	Initial Access (TA0001)	Заказчик проинформирован, легитимность активности подтверждена.
9	Successful SSH Authentication from Unusual User	20.03.2026 10:58	На хосте localhost (94.247.133.122) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя nurlan. Source IP - 42.1.90.62:5678	Низкий	Initial Access (TA0001)	Заказчик проинформирован, легитимность активности подтверждена.
10	Linux User Account Creation	20.03.2026 13:28	На хосте mysql-server (10.10.10.2) было инициировано создание учетной записи пользователем proxysql.	Низкий	Persistence (TA0003)	Заказчик проинформирован, легитимность активности

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

						подтверждена.
11	Linux User Account Creation	20.03.2026 15:26	На хосте localhost (94.247.133.122) было инициировано создание учетной записи пользователем ci-user.	Низкий	Persistence (TA0003)	Заказчик проинформирован, легитимность активности подтверждена.
12	Successful SSH Authentication from Unusual User	20.03.2026 15:33	На хосте php.local (10.10.10.3) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя ci-user. Source IP - 10.10.10.1:43118	Низкий	Initial Access (TA0001)	Заказчик проинформирован, легитимность активности подтверждена.
13	Linux User Account Creation	20.03.2026 20:28	На хосте mysql-server (10.10.10.2) было инициировано создание учетной записи пользователем redis.	Низкий	Persistence (TA0003)	Заказчик проинформирован, легитимность активности подтверждена.
14	Potential Suspicious File Edit	26.03.2026 10:14	На хосте localhost (172.17.0.1) пользователем root было инициировано создание файла через процесс "nano" по пути: /home/eqonaq/..bashrc.swp	Низкий	Persistence (TA0003) Privilege Escalation (TA0004)	Заказчик проинформирован, легитимность активности подтверждена.
15	SSH Authorized Keys File	26.03.2026 15:16	На хосте localhost (10.10.10.1) был зафиксировано создание файла процессом "sh" от учетной записи Nurlan.	Средний	Persistence (TA0003)	Заказчик проинформирован,

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

	Modification		Файл: /home/nurlan/.ssh/authorized_keys		Lateral Movement (TA0008)	легитимность активности подтверждена.
16	Remote File Creation in World Writeable Directory	27.03.2026 12:25	На хосте mysql-server(10.10.10.2) пользователем gts было инициировано создание файлов 78a3-b727-ce5f-c347, 5e50-8f82-f27a-91b0 и af1b-2389-80e3-158f через процесс /usr/lib/openssh/sftp-server.	Средний	Lateral Movement (TA0008)	Заказчик проинформирован, легитимность активности подтверждена.
17	Linux User Account Creation	31.03.2026 09:27	На хосте php.local (10.10.10.3) было инициировано создание учетной записи пользователем tcpdump.	Низкий	Persistence (TA0003)	Заказчик проинформирован, легитимность активности подтверждена.

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

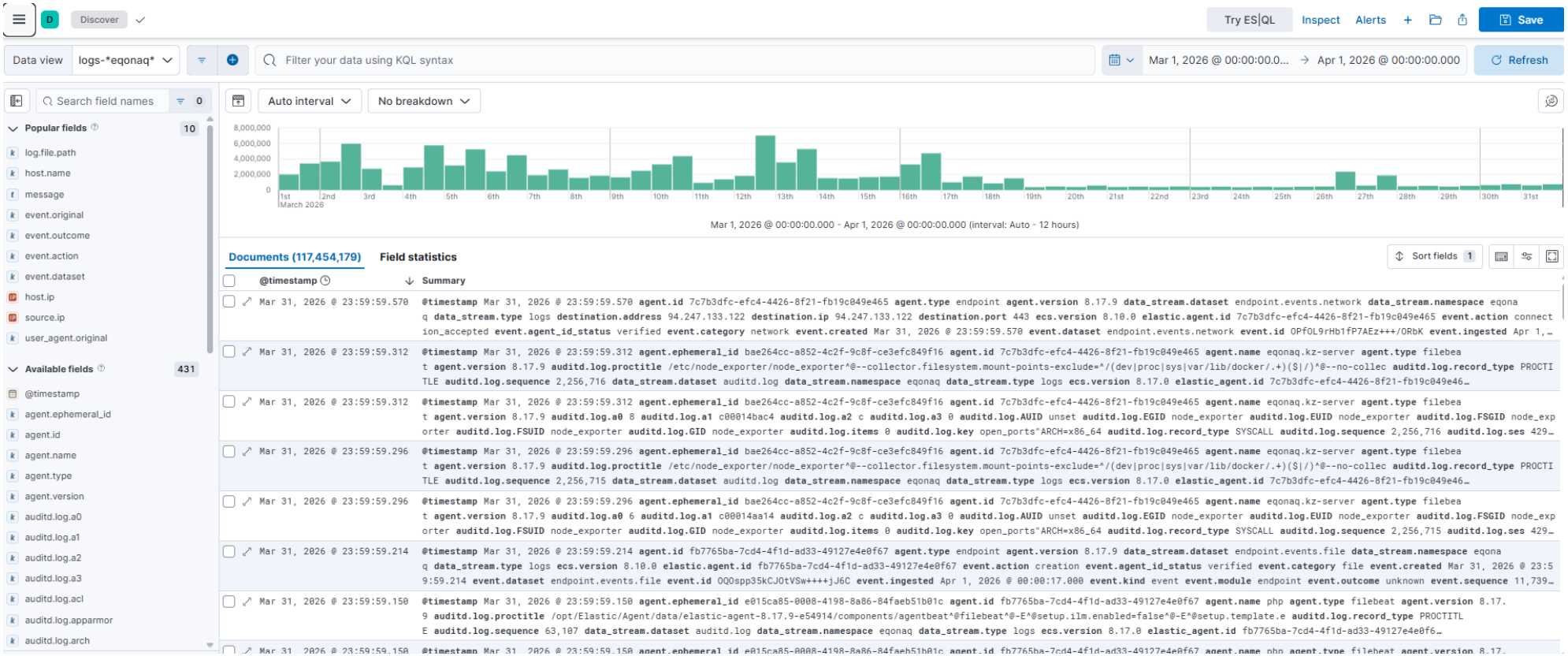

Рисунок 3. Поступление событий ИБ в систему мониторинга

DOC ID KZBW2Z120260000188008E48A8
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 (67,72%) событий поступает от хоста mysql-server.

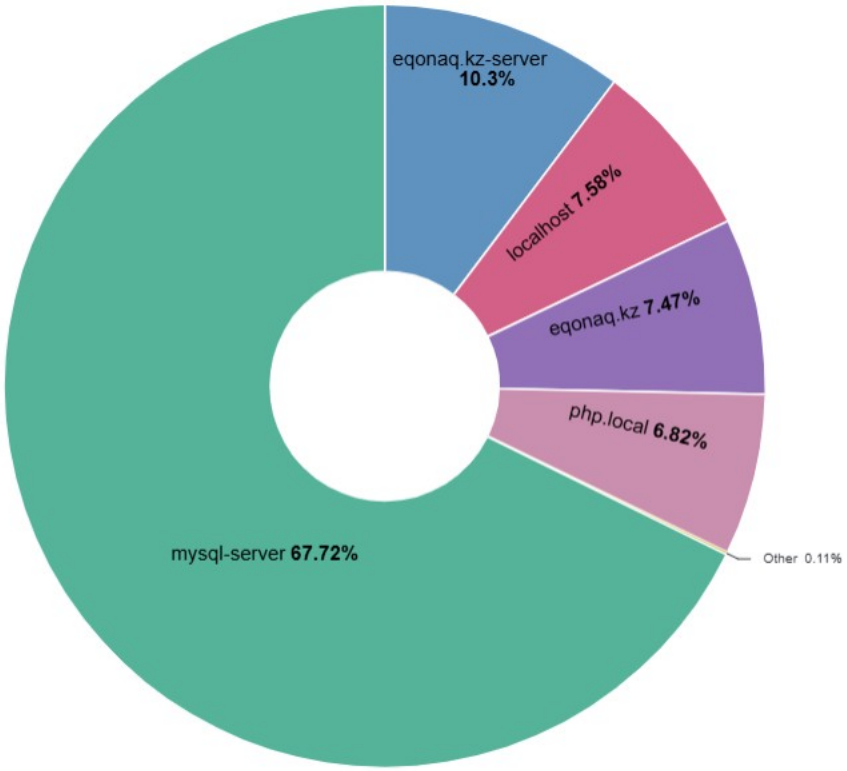

Рисунок 5. Агент, направляющий основную часть событий ИБ

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

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000188008E48A8

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

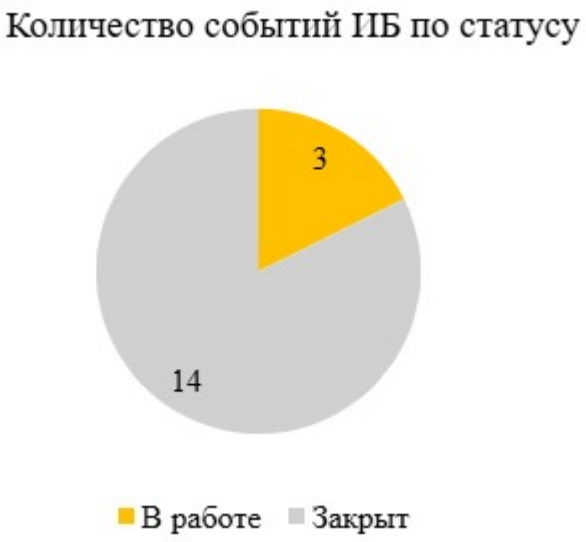

Рисунок 6. Количество зафиксированных событий ИБ по статусу

DOC ID KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

6. Рекомендация

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

1. Внедрить процесс управления уязвимостями для своевременного устранения уязвимостей в инфраструктуре, при необходимости.
2. Установить график создания резервных копий критически важных производственных систем, при необходимости.
3. Провести проверку корпоративных учетных записей на предмет соблюдения корпоративной парольной политики и соблюдения принципа наименьших привилегий.
4. Внедрить двухфакторную аутентификацию для повышения безопасности пользователей в домене.

DOC ID KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

7. Заключение

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

DOC ID KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z120260000188008E48A8
Тип документа	Исходящее письмо
Тема	Отчет за март 2026 года
Статус	Отправлен
Рег. Номер:	01-01/128
Рег. Дата:	03.04.2026
Количество страниц	19
Подписи	2

Информация об отправителе

Отправитель	ТОО "MSSP.GL"
IP-адрес	185.143.21.18

Информация о получателях

Получатель 1	Министерство туризма и спорта Республики Казахстан, 012000100000, Казахстан

Информация о подписантах

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Генеральный директор
IP-адрес	185.143.21.18
Email	d.salipov@mssp.global
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWGQYJ...tFec3VOs5
Дата подписания	03.04.2026 13:21

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Генеральный директор
IP-адрес	185.143.21.18
Email	d.salipov@mssp.global
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWUQYJ...PjxWrycw=

Дата подписания 03.04.2026 13:22

DOC ID KZBW2Z120260000188008E48A8

DOC ID KZBW2Z120260000188008E48A8
Электронный документ подписан в Documentolog Business