MSSP GLOBAL

# Отчет по мониторингу событий информационной безопасности

Май, 2026 г.
рег. №256/1 от 01.06.2026 г.

DOC ID KZBW2Z1202600001946962380 6

DOC ID KZBW2Z1202600001946962380 6
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.....19
7. Заключение.....20

DOC ID KZBW2Z12026000019469623806



DOC ID KZBW2Z12026000019469623806
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 май 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 KZBW2Z12026000019469623806



DOC ID KZBW2Z12026000019469623806
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 KZBW2Z1202600001946962380 6



DOC ID KZBW2Z12026000019469623806
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 | localhost.localdomain.mssp.local | eqonaq_NetDev rev. 15 | 0.72 % | 213 MB | 19 seconds ago | 8.17.9 |
| Healthy | php.local | eqonaq rev. 46 | 3.98 % | 245 MB | 20 seconds ago | 8.17.9 |
| Healthy | mysql-server | eqonaq rev. 46 | 2.50 % | 233 MB | 16 seconds ago | 8.17.9 |
| Healthy | localhost | eqonaq rev. 46 | 3.02 % | 264 MB | 17 seconds ago | 8.17.9 |

*Рисунок 2. Подключенные к системе мониторинга хосты Заказчика*

DOC ID KZBW2Z120260000194696238 06



DOC ID KZBW2Z120260000194696238 06
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<br>- Эксплуатация уязвимости<br>- Шифровальщик<br>- Вредоносное ПО<br>- Отказ в обслуживании (DoS/DDoS-атака)<br>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<br>- Шифровальщик<br>- Вредоносное ПО<br>- Отказ в обслуживании (DoS/DDoS-атака)<br>- Эксплуатация уязвимости<br>И т.д. |
| Низкий (2) | Инциденты ИБ, не влияющие на предоставление услуги/выполнение работ. | - Вредоносное ПО<br>- Отказ в обслуживании (DoS/DdoS-атака)<br>- Эксплуатация уязвимости<br>- Спам<br>- Фишинговая атака<br>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 KZBW2Z12026000019469623806



DOC ID KZBW2Z12026000019469623806
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: **224 427 691;**
- Количество зафиксированных событий ИБ: **31.**

DOC ID KZBW2Z12026000019469623806



DOC ID KZBW2Z12026000019469623806
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 | Successful SSH Authentication from Unusual SSH Public Key | 04.05.2025 11:56 | На хосте php.local (10.10.10.3) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя user. Source IP - 10.10.10.1 | Низкий | Initial Access (TA0001) | Заказчик проинформирован, подтверждена легитимность события |
| 2 | Enumeration of Kernel Modules | 05.05.2025 14:41 | На хосте localhost (10.100.0.1) пользователем root было инициировано получения информации о модуле ядра fuse.ko через команду modinfo. Родительским процессом этой активности является fuse.<br>Введённая команда:<br>modinfo-k5.10.0-41-amd64-Ffirmware/lib/modules/5.10.0-41-amd64/kernel/fs/fuse/fuse.ko | Средний | Discovery (TA0007) | Заказчик проинформирован, подтверждена легитимность события |
| 3 | File Permission Modification in Writable Directory | 09.05.2025 07:41 | Был запущен процесс "chmod" с родительским процессом "sh" пользователем user на хосте php.local (ip: 10.10.10.3).<br>Введённая команды:<br>chmod +x 7zz | Низкий | Defense Evasion (TA0005) | Заказчик проинформирован, ожидается обратная связь |
| 4 | Deprecated - Suspicious File Creation in /etc for Persistence | 12.05.2025 10:19 | На хосте "localhost" (ip: 10.10.10.1) пользователем " root" было зафиксировано событие с процессом "/usr/bin/vi", путь до исполняемого файла: | Низкий | Persistence (TA0003) Execution (TA0002) | Заказчик проинформирован, подтверждена |



DOC ID KZBW2Z1202600001946962380 6
Электронный документ подписан в Documentolog Business

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | "/etc/systemd/system/.backup.timer.swp". | | Privilege Escalation (TA0004) | легитимность события |
| 5 | Successful administrator login detected | 13.05.2025 17:56 | На хосте php.local (ip: 10.10.10.3) обнаружен успешный вход пользователя Адлет с IP-адресса 45.86.83.20.<br>user.email: info@eqonaq.kz | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 6 | Successful administrator login detected | 14.05.2025 11:18 | На хосте php.local (ip: 10.10.10.3) обнаружен успешный вход пользователя Адлет с IP-адресса 45.86.83.20.<br>user.email: info@eqonaq.kz | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 7 | Berkut integration status changed. | 14.05.2025 11:21 | На хосте php.local (ip: 10.10.10.3) пользователем Адлет был изменен статус интеграции Berkut<br>user.email: info@eqonaq.kz | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 8 | MySQL - Failed login attempt. | 14.05.2025 12:44 | На хосте mysql-server (ip: 10.10.10.2) пользователем ilya произошла неудачная попытка подключения к БД | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 9 | Virtualization - | 14.05.2025 | На хосте localhost (ip: 10.10.10.1) пользователь | Низкий | - | Заказчик |



DOC ID KZBW2Z12026000019469623806
Электронный документ подписан в Documentolog Business

| | | | | | | |
|---|---|---|---|---|---|---|
| | Stopping (soft shutdown) virtual machine. | 13:09 | ilya выполнил команду: virsh shutdown test-vm | | | проинформирован, подтверждена легитимность события |
| 10 | Virtualization - Shutting down virtual machine. | 14.05.2025 13:11 | На хосте localhost (ip: 10.10.10.1) пользователь ilya выполнил команду: virsh destroy test-vm | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 11 | MySQL - Successful login. | 14.05.2025 13:16 | На хосте mysql-server (ip: 10.10.10.2) обнаружен успешный вход в базу данных с пользователем ilya | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 12 | Virtualization - New virtual machine created. | 14.05.2025 14:25 | На хосте localhost (ip: 10.10.10.1) пользователем ilya была создана новая виртуальная машина со статусом SUCCESS.<br>Исполняемая команда:<br>virt-install --name test-vm --ram 2048 --vcpus 2 --disk path=/var/lib/libvirt/images/test-vm.qcow2,size=10 --os-variant generic --network network=br-vms --cdrom /var/lib/libvirt/images/debian-13.2.0-amd64-netinst.iso --noautoconsole | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |



DOC ID KZBW2Z1202600001946962380 6
Электронный документ подписан в Documentolog Business

| | | | | | | |
|---|---|---|---|---|---|---|
| 13 | MySQL - Successful login. | 14.05.2025 14:27 | На хосте mysql-server (ip: 10.10.10.2) обнаружен успешный вход в базу данных с пользователем ilya | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 14 | MySQL - RENAME TABLE query. | 14.05.2025 14:31 | На хосте mysql-server (ip: 10.10.10.2) пользователем ilya была выполнен запрос RENAME_TABLE.<br>Исполняемая команда:<br>RENAME TABLE test_table TO renamed_table | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 15 | Successful administrator login detected | 14.05.2025 14:33 | На хосте php.local (ip: 10.10.10.3) обнаружен успешный вход пользователя Адлет с IP-адресса 45.86.83.20.<br>user.email: info@eqonaq.kz | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 16 | MySQL - TRUNCATE query. | 14.05.2025 15:26 | На хосте mysql-server (ip: 10.10.10.2) пользователем ilya был выполнен запрос TRUNCATE.<br>Исполняемая команда:<br>TRUNCATE TABLE test_table | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 17 | MySQL - DROP TABLE query. | 14.05.2025 15:27 | На хосте mysql-server (ip: 10.10.10.2) пользователем ilya был выполнен запрос TRUNCATE.<br>Исполняемая команда: | Низкий | - | Заказчик проинформирован, подтверждена |



DOC ID KZBW2Z12026000019469623806
Электронный документ подписан в Documentolog Business

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | DROP TABLE renamed_table | | | легитимность события |
| 18 | MySQL - CREATE TABLE query. | 14.05.2025 15:28 | На хосте mysql-server (ip: 10.10.10.2) пользователем ilya был выполнен запрос CREATE.<br>Исполняемая команда:<br>CREATE TABLE test_table | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 19 | MySQL - RENAME TABLE query. | 14.05.2025 15:30 | На хосте mysql-server (ip: 10.10.10.2) пользователем ilya был выполнен запрос RENAME.<br>Исполняемая команда:<br>RENAME TABLE test_table TO renamed_table | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 20 | MySQL - ALTER TABLE query. | 14.05.2025 15:30 | На хосте mysql-server (ip: 10.10.10.2) пользователем ilya был выполнен запрос ALTER.<br>Исполняемая команда:<br>ALTER TABLE test_table ADD COLUMN email TEXT | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 21 | Virtualization - New virtual machine created. | 15.05.2025 13:24 | На хосте localhost (ip: 10.10.10.1) пользователем ilya была создана новая виртуальная машина со статусом SUCCESS.<br>Исполняемая команда:<br>virt-install --name test-vm --ram 2048 --vcpus 2 --disk path=/var/lib/libvirt/images/test-vm.qcow2,size=10 --os-variant generic --network network=br-vms --cdrom | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |



DOC ID KZBW2Z1202600001946962380 6
Электронный документ подписан в Documentolog Business

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | /var/lib/libvirt/images/debian-13.2.0-amd64-netinst.iso --noautoconsole | | | |
| 22 | Successful administrator login detected | 17.05.2025 18:25 | На хосте php.local (ip: 10.10.10.3) обнаружен успешный вход пользователя Адлет с IP-адресса 89.219.32.146.<br>user.email: info@eqonaq.kz | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 23 | Remote File Creation in World Writeable Directory | 19.05.2025 11:55 | На хосте localhost( 10.10.10.1) пользователем gts было инициировано создание файла a885-e174-1a65-8ffe через процесс /usr/lib/openssh/sftp-server. | Средний | Lateral Movement (TA0008) | Заказчик проинформирован, подтверждена легитимность события |
| 24 | Cron Job Created or Modified | 21.05.2025 15:18 | На хосте localhost (ip: 10.10.10.1) ользователем root был создан или изменён запланированный запуск задачи через планировщик cron.<br>Был переименован файл debsecan с помощью процесса debsecan-create-cron на /etc/cron.d/debsecan | Средний | Privilege Escalation (TA0004) Persistence (TA0003) Execution (TA0002) | Заказчик проинформирован, подтверждена легитимность события |
| 25 | Successful administrator login detected | 21.05.2025 18:31 | На хосте php.local (ip: 10.10.10.3) обнаружен успешный вход пользователя Адлет с IP-адресса 89.219.32.146.<br>user.email: info@eqonaq.kz | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |
| 26 | Virtualization - | 21.05.2025 | На хосте eqonaq.kz-server (ip: 10.10.10.1) | Средний | - | Заказчик |



DOC ID KZBW2Z12026000019469623806
Электронный документ подписан в Documentolog Business

| | | | | | | |
|---|---|---|---|---|---|---|
| | Shutting down virtual machine. | 23:57 | пользователь ilya выполнил команду: virsh destroy test-vm | | | проинформирован, подтверждена легитимность события |
| 27 | Linux Restricted Shell Breakout via Linux Binary(s). | 22.05.2025 16:17 | Родительским процессом sudo был запущен процесс bash на хостах localhost (10.10.10.1), mysql-server (10.10.10.2), php.local (10.10.10.3), под пользователем root.<br>Введённая команда:<br>sudo, bash, -c, LANG=C LC_ALL=C ; no pager<br>sudo, bash, -c, LANG=C LC_ALL=C ; terminal pager 0<br>sudo, bash, -c, LANG=C LC_ALL=C ; pager 0<br>sudo, bash, -c, LANG=C LC_ALL=C ; set cli pager off | Низкий | Execution (TA0002) | Заказчик проинформирован, подтверждена легитимность события |
| 28 | Remote File Creation in World Writeable Directory | 22.05.2025 16:18 | На хостах localhost (10.10.10.1), mysql-server (10.10.10.2), php.local (10.10.10.3) пользователем gts было инициировано создание файлов a40c-ac82-6a33-1b91, 143c-1719-c4e2-fc18, 9966-f840-9457-b930, c761-e2a5-8430-b362, a70f-71f0-cfc1-cdec и c4dd-deaf-0aba-aecb через процесс /usr/lib/openssh/sftp-server. | Средний | Lateral Movement (TA0008) | Заказчик проинформирован, подтверждена легитимность события |
| 29 | Successful administrator login detected | 22.05.2025 23:31 | На хосте php.local (ip: 10.10.10.3) обнаружен успешный вход пользователя Адлет с IP-адресса 5.34.127.242.<br>user.email: info@eqonaq.kz | Низкий | - | Заказчик проинформирован, подтверждена |



DOC ID KZBW2Z12026000019469623806
Электронный документ подписан в Documentolog Business

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | легитимность события |
| 30 | Kill Command Execution | 25.05.2025 13:45 | Пользователь root на хосте localhost (ip: 10.10.10.1) запустил команду<br>pkill -TERM -t pts/0<br>с родительским процессом sudo. | Низкий | Execution (TA0002) Defense Evasion (TA0005) | Заказчик проинформирован, подтверждена легитимность события |
| 31 | MySQL - Successful login. | 26.05.2025 15:10 | На хосте mysql-server (ip: 10.10.10.2) обнаружен успешный вход в базу данных с пользователем ilya | Низкий | - | Заказчик проинформирован, подтверждена легитимность события |



DOC ID KZBW2Z1202600001946962380 6
Электронный документ подписан в Documentolog Business

*Рисунок 3. Поступление событий ИБ в систему мониторинга*



DOC ID KZBW2Z1202600001946962380 6
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 (65,97%) событий поступает от хоста mysql-server.

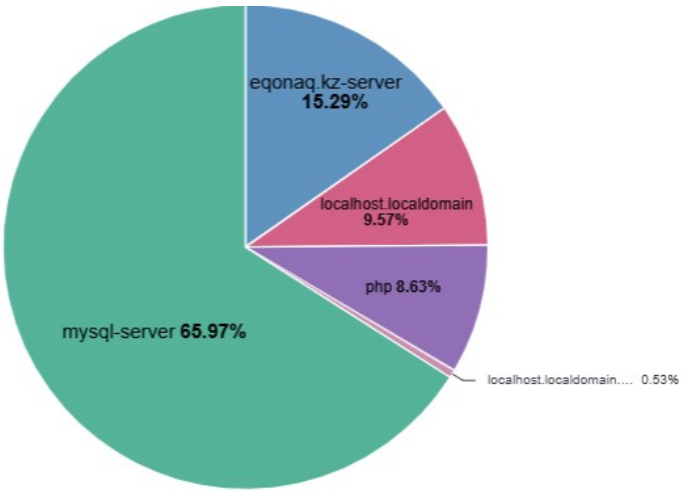


*Рисунок 5. Агент, направляющий основную часть событий ИБ*

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

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



DOC ID KZBW2Z12026000019469623806
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019469623806

*Рисунок 6. Количество зафиксированных событий ИБ по статусу*

DOC ID KZBW2Z120260000019469623806



DOC ID KZBW2Z120260000019469623806
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 KZBW2Z1202600001946962380 6



DOC ID KZBW2Z1202600001946962380 6
Электронный документ подписан в Documentolog Business

## 7. Заключение

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

DOC ID KZBW2Z1202600001946962380 6



DOC ID KZBW2Z1202600001946962380 6
Электронный документ подписан в Documentolog Business

# Квитанция о подписании

## Основная информация

| | |
|---|---|
| DOC ID | KZBW2Z12026000019469623806 |
| Тип документа | Исходящее письмо |
| Тема | Отчеты за май 2026 г. пароль передан исполнителю |
| Статус | Доставлен |
| Рег. Номер: | 01-01/194 |
| Рег. Дата: | 02.06.2026 |
| Количество страниц | 1 |
| Подписи | 1 |

## Информация об отправителе

| | |
|---|---|
| Отправитель | ТОО "MSSP.GL" |
| IP-адрес | 109.163.197.162 |

## Информация о получателях

| | |
|---|---|
| Получатель 1 | ГУ "Министерство туризма и спорта Республики Казахстан" kense@tsm.gov.kz |
| Получатель 2 | ГУ "Министерство туризма и спорта Республики Казахстан", t.akchabaev@tsm.gov.kz t.akchabaev@tsm.gov.kz |
| Получатель 3 | ГУ "Министерство туризма и спорта Республики Казахстан", r.kuderbaev@tsm.gov.kz r.kuderbaev@tsm.gov.kz |

## Информация о подписантах

| | |
|---|---|
| Подписал(а) | ДЖАНСЕНГИРОВ РУСЛАН |
| 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 |
| | Лицо, наделенное правом подписи |
| Подпись | MIIWQgYJ...+dpeWOfQ= |
| Дата подписания | 02.06.2026 11:48 |

DOC ID KZBW2Z12026000019469623806