Отчет по мониторингу событий информационной безопасности

Сентябрь, 2025 г.

рег. №506/1 от 07.10.2025 г.

Содержание

Оглавление

1. Введение 3
2. Определения 4
3. Источники событий 6
4. Классификация событий ИБ 8
5. Результат мониторинга 9
6. Рекомендации 14
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 товариществом с ограниченной ответственностью «MSSP.GL» *(далее - Исполнитель),* в сентябре 2025 года, Исполнителем были проведены следующие работы, в рамках оказания услуги мониторинга событий информационной безопасности *(далее - ИБ):*

– Круглосуточный мониторинг событий ИБ [1] в режиме 24/7/365 и техническая поддержка;

– Обеспечение защищенных каналов взаимодействия между Заказчиком и Поставщиком;

– Мониторинг состояния защищенных каналов передачи журналов событий (Рис. 1).

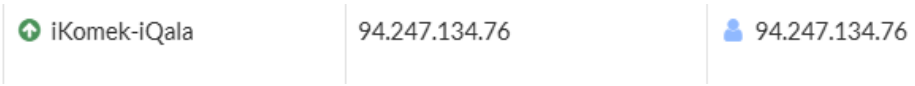

Рисунок 1. Мониторинг туннеля [Заказчик – Исполнитель] для сбора событий ИБ

[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

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.

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.

3. Источники событий

На момент выдачи отчета к системе мониторинга Исполнителя были подключены следующие источники событий:

Showing 6 agents Clear filters Healthy 6 Unhealthy 0 Updating 0 Offline 0 Inactive 0 Unenrolled 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	jardem	jardem rev. 23	95.82 %	197 MB	40 seconds ago	8.17.4 Upgrade available	
Healthy	ubuntu	iQala_SKO_NetDev rev. 18	0.16 %	193 MB	35 seconds ago	8.17.6 Upgrade available	
Healthy	appsko	iQala_SKO rev. 11	0.73 %	190 MB	35 seconds ago	8.17.6 Upgrade available	
Healthy	avroradb	iQala_SKO rev. 11	0.57 %	192 MB	39 seconds ago	8.17.6 Upgrade available	
Healthy	frontdb	iQala_SKO rev. 11	0.56 %	192 MB	21 seconds ago	8.17.6 Upgrade available	
Healthy	oldtime.integro.kz	iQala_SKO rev. 11	0.66 %	215 MB	14 seconds ago	8.17.6 Upgrade available	

Рисунок 2. Статус агентов, подключенных к системе мониторинга

Общие рекомендации:

1. Производитель: Cisco.

Уровень критичности: критический.

Известная эксплуатация: подтверждена CISA (Cybersecurity and Infrastructure Security Agency) и Cisco, уязвимости активно эксплуатируются в рамках кампании, связанной с ArcaneDoor.

Краткое описание уязвимостей

CVE-2025-20333 – уязвимость связана с некорректной валидацией пользовательского ввода в HTTP(S)-запросах веб-сервера VPN в Cisco ASA и Cisco FTD. Эксплуатация может позволить аутентифицированному удалённому злоумышленнику выполнить произвольный код с правами root, что может привести к полной компрометации устройства.

CVE-2025-20362 – уязвимость связана с некорректной валидацией пользовательского ввода в HTTP(S)-запросах веб-сервера VPN. Эксплуатация может позволить неаутентифицированному удалённому злоумышленнику получить доступ к защищённым URL-эндпоинтам без прохождения аутентификации.

Типы уязвимостей:

• Remote Code Execution (RCE);

• Privilege Escalation;

• Authentication Bypass.

Затронутые версии и продукты:

• Cisco Adaptive Security Appliance (ASA) Software (включая аппаратные платформы ASA, ASA-SM, ASAv);

• Cisco Secure Firewall Threat Defense (FTD) Software (включая Firepower 2100, 4100, 9300).

Рекомендации:

Организациям, использующим затронутые версии, рекомендуется незамедлительно применить обновления до исправленных версий в соответствии с правилами политики организации

4. Классификация событий ИБ

В целях своевременного реагирования и принятия соответствующих мер по обеспечению ИБ, события ИБ в данной области подразделяются на три ключевые категории по уровню критичности.

Уровень критичности	Описание
Низкий	События ИБ, не оказывающие влияние на электронные информационные ресурсы, информационные системы, сетей телекоммуникаций и другие объекты информатизации.
Средний	События ИБ, которые могут привести к ограничению доступности источника события ИБ, ухудшению ситуации или негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.
Высокий	События ИБ, которые могут привести к серьезным нарушениям безопасности, существенному ухудшению условий функционирования информационных систем и инфраструктуры, а также неблагоприятным последствиям для организации.

Следует добавить, что аналитик ОЦИБ имеет полномочия самостоятельно определять уровень критичности, если считает, что инцидент может вызвать значительно отрицательные последствия.

4. Результат мониторинга

Исполнитель осуществляет постоянный мониторинг всех подключённых к мониторингу элементов инфраструктуры Заказчика. Все зарегистрированные, подтвержденные инциденты ИБ направляются в 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 Исполнителя было обработано 127 056 789 событий и зафиксировано 3 события ИБ (Таблица 1).

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
1.	Potential External Linux SSH Brute Force Detected.	16.09.2025 00:11	С адреса 142.93.50.50 зафиксировано множество неудачных попыток входа по sshd под пользователем root на хосте jardem (10.10.76.60). Данный IP отмечен как вредоносный 5 антивирусными вендорами.	Низкий	Credential Access (TA0006)	Заказчик проинформирован, IP адрес был заблокирован.
2.	Potential External Linux SSH Brute Force Detected.	16.09.2025 00:11	С адреса 91.224.92.79 зафиксировано множество неудачных попыток входа по sshd под пользователем root на хосте jardem (10.10.76.60). Данный IP отмечен как вредоносный 17 антивирусными вендорами.	Низкий	Credential Access (TA0006)	Заказчик проинформирован, IP адрес был заблокирован.
3.	Successful SSH Authentication from Unusual User	16.09.2025 00:11	На хосте oldtime.integro.kz (172.21.10.2) произошла успешная попытка аутентификации по протоколу SSH от имени пользователя oleg. Source IP - 212.76.12.228	Низкий	Initial Access (TA0001)	Заказчик проинформирован, подтверждена легитимность активности.

Рисунок 3. Поступление событий ИБ в систему мониторинга

На Рис. 4 указано количество зафиксированных событий ИБ по уровню критичности

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

На Рис. 5 показано процентное соотношение количества генерируемых событий подключенными источниками, Все события поступают на хост oldtime.integro.kz, (172.21.10.2).

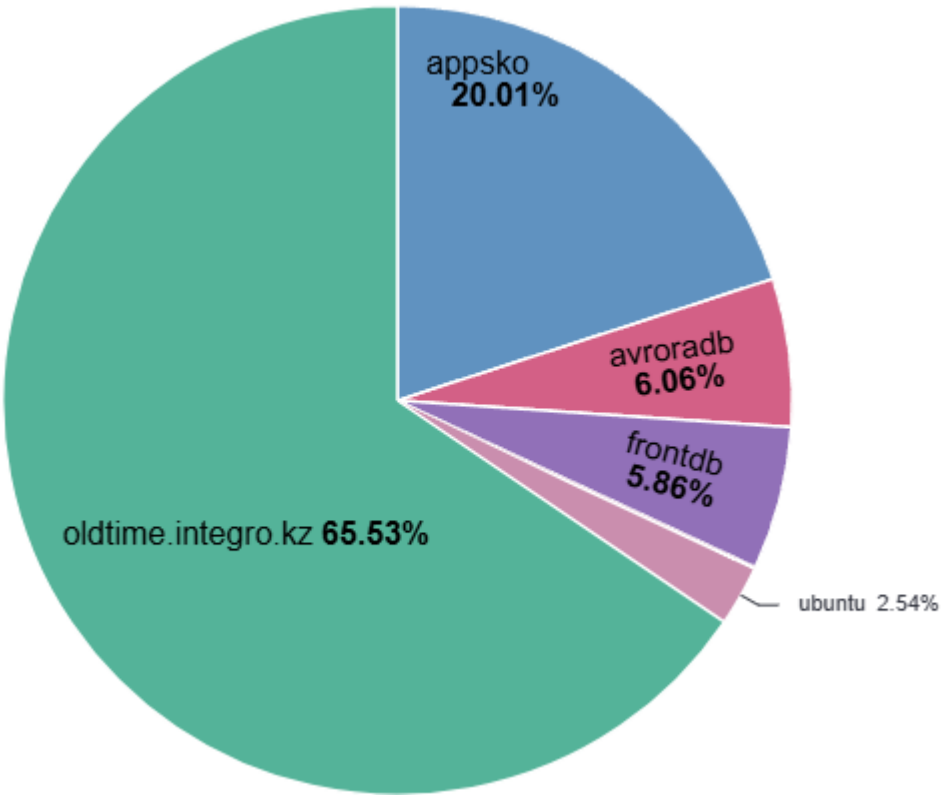

Рисунок 5. Источники, направляющие основную часть событий ИБ

На Рис. 6 указано количество зафиксированных событий ИБ по статусу инцидента ИБ:

Закрыт: Заказчик проинформирован, подтверждена легитимность активности.

В работе: Заказчик проинформирован, ожидается обратная связь.

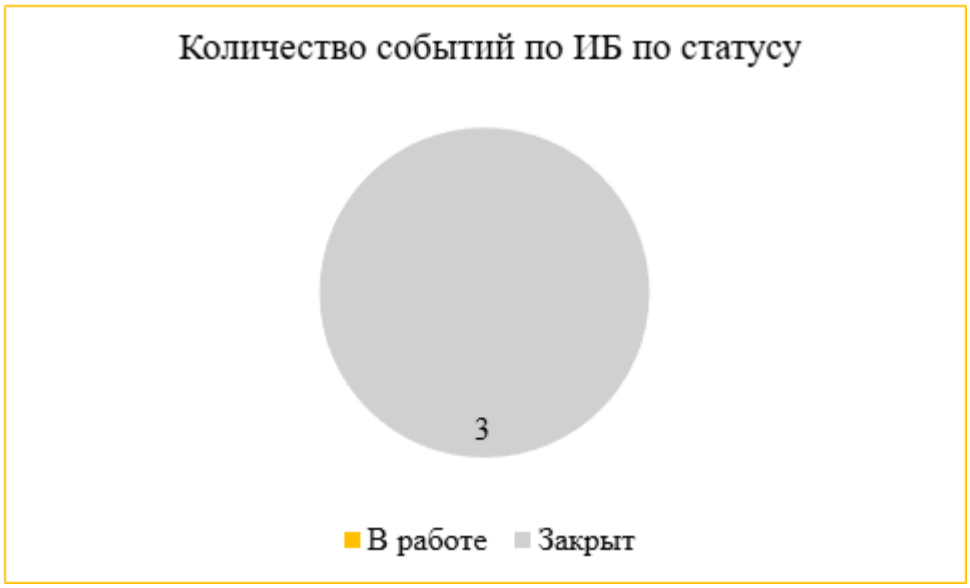

Рисунок 6. Количество зафиксированных событий ИБ по статусу

5. Рекомендации

1. Провести 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. Провести инвентаризацию установленных систем и приложений на всех корпоративных хостах с проверкой актуальности версий.

3. Проверить отключение всех неиспользуемых сервисов, протоколов и портов.

4. Проверить соответствие настроек нестандартных портов документированным политикам безопасности (к примеру, заменить стандартные порты на иные).

5. Ограничить удаленный доступ защищенными каналами (VPN, SSH с двухфакторной аутентификацией).

6. Ограничить внешний доступ до корпоративных ресурсов только для казахстанского интернет-сегмента.

6. Заключение

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