ИСПОЛНИТЕЛЬ	ЗАКАЗЧИК
Заместитель генерального директора	Заместитель руководителя КГУ «Управления цифровизации города Алматы»
ТОО «MSSP.GL»	
Р.С. Джансенгиров	М.А. Дюсюков
_____	_____

Отчет об оказанных услугах по обеспечению информационной безопасности акимата города Алматы по сервисной модели информатизации

КГУ "Управление цифровизации города Алматы"

Отчетный период: 01.02.2026 – 28.02.2026 г.

Оглавление

1. ОБЩАЯ ИНФОРМАЦИЯ 3
1.1. Ключевые показатели эффективности 3
2. ВВЕДЕНИЕ 4
2.1. Цель отчета 4
2.2. Область действия 5
3. АНАЛИЗ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 6
3.1. Состояние агентов 6
3.2 Настройка и актуализация представлений данных (Data Views) 7
3.3. Усиление мониторинга и анализа событий через SIEM-систему 7
4. МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 10
4.1. Статистика событий безопасности 10
4.2. Сопровождение и реагирование на инциденты информационной безопасности 12
4.3 Поиск угроз информационной безопасности (Threat Hunting) 13
4.4. Проверка безопасности веб-ресурса 13
4.5. Автоматическое реагирование на угрозы 14
4.5. Проанализированные программы в рамках мониторинга 14
5. АНАЛИЗ УЯЗВИМОСТЕЙ 15
5.1 Инструментальное сканирование 15
5.2 Статистика управления уязвимости 18
6. ПЛАТФОРМА АНАЛИЗА УГРОЗ И ЗАЩИТА ОТ ТАРГЕТИРОВАННЫХ АТАК 19
6.1. OpenCTI — Платформа киберразведки 19
6.2. MISP — Обмен индикаторами компрометации 20
6.3. T-Lab Sandbox — Защита от таргетированных атак 22
6.4. DLP – Предотвращение утечек данных (safetica) 23
6.4.1. Анализ веб – активности 24
6.4.2. Передачи данных 25
6.4.3. Служебные операции через интернет и внутренние сервисы 27
6.5 Checkpoint - межсетевой экран 29
7. РЕАЛИЗОВАННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 33
8. ВЫВОДЫ И РЕКОМЕНДАЦИИ 36
8.1. Общие выводы 36
8.2. Приоритетные планы работ 36
8.3. Рекомендации 37

1. ОБЩАЯ ИНФОРМАЦИЯ

Настоящий отчет представляет результаты оказания услуг по обеспечению информационной безопасности для Акимата города Алматы (далее - Заказчик) за отчетный период 01.02.2026 – 28.02.2026 года. Услуги предоставлялись в рамках комплексного подхода к защите информационной инфраструктуры Заказчика с использованием передовых технологий мониторинга, обнаружения и реагирования на угрозы информационной безопасности.

1.1. Ключевые показатели эффективности

В отчётном периоде (февраль 2026 года) в рамках сопровождения и эксплуатации системы информационной безопасности достигнуты следующие ключевые результаты:

- Обеспечена работоспособность агентов информационной безопасности (EDR, DLP, Sysmon) на рабочих станциях и серверах Заказчика; выполнен ручной обход и восстановление агентов на 12 рабочих станциях, функционирующих под управлением Windows 11 Home;
- SIEM-системой зарегистрировано 8 416 срабатывания корреляционных и поведенческих правил, охватывающих события аномальной активности процессов, доменной среды и пользовательских действий;
- Все выявленные события проанализированы аналитиками, по результатам рассмотрения нарушений функционирования информационных систем не выявлено;
- В рамках реагирования все кейсы информационной безопасности обработаны и закрыты, признаков успешной реализации инцидентов не зафиксировано;
- Выполнено инструментальное сканирование уязвимостей внутреннего и внешнего периметра; выявлены уязвимости уровней *Critical, High и Medium*, при этом по результатам сравнения текущего и предыдущего запусков изменений не выявлено;
- Обеспечено функционирование платформы OpenCTI: все выявленные индикаторы компрометации (IoC) по результатам анализа и расследований добавлены в базу Threat Intelligence для последующей корреляции и проактивного выявления угроз;
- С использованием системы T-Lab Sandbox выполнен динамический и статический анализ объектов: проверено 320 объектов, из которых выявлено 3 угрозы и 57 подозрительных, что составляет незначительную долю от общего потока и не указывает на массовые инциденты; основная

нагрузка носит неравномерный характер с пиковыми значениями в отдельные периоды (до ~150 загрузок), при этом в остальное время сохраняется низкий уровень активности; максимальные оценки угроз достигают порядка 100, что свидетельствует о наличии отдельных потенциально опасных объектов; в структуре файлов преобладают текстовые, далее следуют исполняемые, остальные типы (Java, PDF, MS Office, изображения) занимают малую долю; в разрезе недели наибольшая активность зафиксирована 26 февраля, после чего отмечается спад к концу периода, что в целом соответствует нормальному рабочему режиму системы без критических отклонений.

- В рамках эксплуатации NGFW Check Point зафиксировано и обработано:
  - **16 920 481** Anti-Bot-событий;
  - **9 296 982** Anti-Virus-срабатываний;
  - **1 153 090** IPS-событий, включая попытки сетевого сканирования и эксплуатации уязвимостей;
  - все сетевые воздействия автоматически заблокированы на периметре;
- В системе DLP зафиксированы единичные события контроля операций с данными; все события проанализированы, фактов утечки или несанкционированной передачи конфиденциальной информации не выявлено;
- Реализована и поддерживается сквозная интеграция средств защиты информации с SIEM, включая EDR, DLP, Check Point NGFW, Nessus, T-Lab Sandbox и OpenCTI, обеспечивающая централизованный мониторинг и реагирование в режиме 24×7.

2. ВВЕДЕНИЕ

Настоящий отчет подготовлен в соответствии с пунктом 4.5 технической спецификации на услуги по обеспечению информационной безопасности и охватывает период 01.02.2026 – 28.02.2026 года.

2.1. Цель отчета

Целью настоящего отчета является предоставление Заказчику комплексной информации о:

- Текущем состоянии систем мониторинга и защиты информационной безопасности;
- Выявленных инцидентах безопасности и принятых мерах реагирования;
- Результатах проведенного тестирования и сканирования на уязвимости;
- Статистике обработанных событий и уведомлений;

- Рекомендациях по повышению уровня защищенности инфраструктуры.

2.2. Область действия

Услуги по обеспечению информационной безопасности предоставляются для всех структурных подразделений Акимата города Алматы, включая:

- Аппарат акима города;
- **24** управлений акимата;
- Территориальные подразделения (районные акиматы).

Общий объем защищаемых объектов включает более 1000 рабочих станций, **15** серверов, **205** сетевых устройств и **12** межсетевых экранов, распределенных по **12** территориально удаленным площадкам Заказчика.

3. АНАЛИЗ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С момента заключения договора Поставщиком проведена комплексная инвентаризация агентов системы управления событиями информационной безопасности (SIEM), системы обнаружения и реагирования на угрозы (EDR), а также дополнительных средств защиты, установленных на рабочих станциях и серверах Заказчика. Помимо EDR-агентов, на части инфраструктуры также развернуты и используются агенты DLP и Sysmon, обеспечивающие расширенный контроль утечек данных и детализацию событий безопасности.

3.1. Состояние агентов

В феврале Поставщиком был выполнен ручной обход рабочих станций и произведён перезапуск EDR-агентов. Необходимость ручного вмешательства была обусловлена тем, что часть инфраструктуры Заказчика функционирует под управлением операционной системы Windows 11 Home, не поддерживающей корпоративные механизмы централизованного управления, доставки политик безопасности и удалённого перезапуска агентов. По итогам выполнения мероприятий агенты функционируют в штатном режиме, замечания и отклонения устранены.

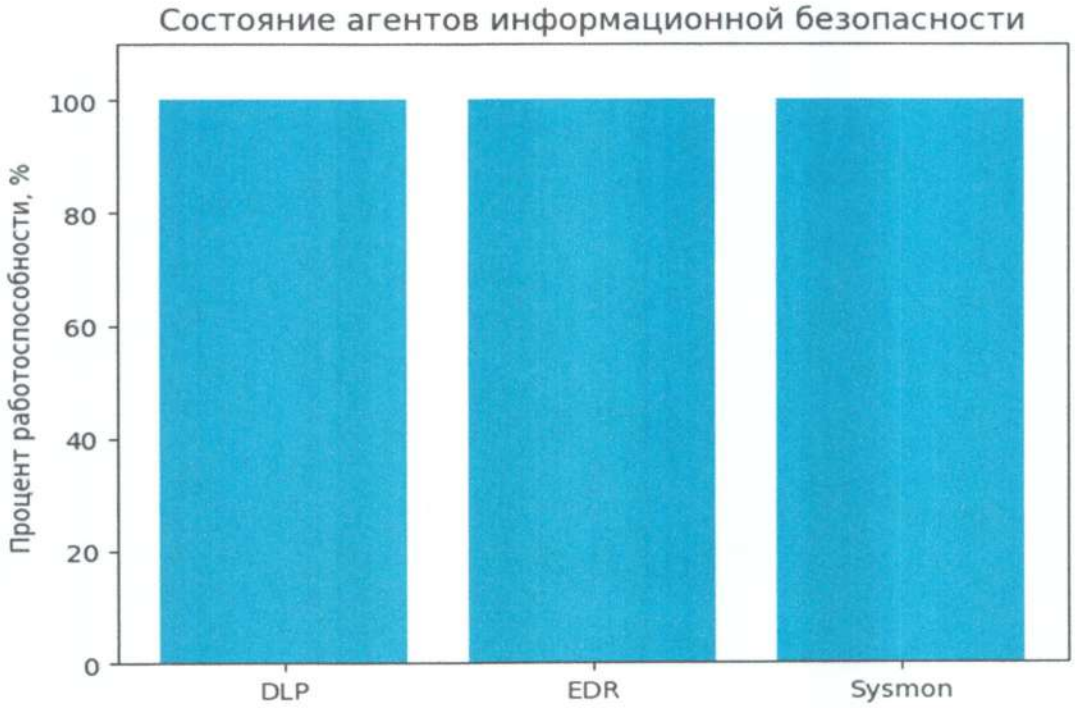

Рисунок 1. Агенты DLP, EDR и Sysmon

Рисунок 1 отражает текущее состояние агентов информационной безопасности, установленных на рабочих станциях Заказчика. По результатам проведённых работ все используемые агенты – DLP, EDR и Sysmon –

функционируют в штатном режиме. Отклонений в работе, сбоев или неактивных агентов не выявлено. Уровень работоспособности агентов по каждому типу средств защиты остаётся стабильно высоким, что подтверждает корректность внедрения и устойчивость функционирования задействованных компонентов в инфраструктуре Заказчика.

3.2 Настройка и актуализация представлений данных (Data Views)

В рамках работ по обеспечению корректного функционирования SIEM-системы были выполнены мероприятия по настройке и актуализации представлений данных (Data Views), используемых для централизованного сбора и анализа событий информационной безопасности. В системе настроены и актуализированы представления данных для обработки событий безопасности, системных журналов и метрик, включая отдельные Data Views для сработок правил информационной безопасности, логов, метрик, событий Sysmon и данных, поступающих от Elastic Agent. Обеспечена корректная привязка представлений данных к соответствующим индексам Elasticsearch, а также их использование в правилах корреляции, визуализациях и аналитических отчётах.

Рисунок 2. Data views

3.3. Усиление мониторинга и анализа событий через SIEM-систему

В соответствии с утверждённым планом осуществляется анализ полноты и качества поступающих событий от средств защиты информации. В рамках данных мероприятий выполняется корректировка и оптимизация интеграций, а также актуализация и обновление правил корреляции в SIEM-системе с

целью повышения эффективности выявления и обработки событий информационной безопасности.

В отчётном периоде SIEM-системой зафиксировано 8 416 срабатываний корреляционных и поведенческих правил безопасности. Наибольшее количество событий связано с попытками подбора привилегированных учётных записей (Privileged Account Brute Force — 3 912 событий), а также с аномальной сетевой активностью от системного бинарника Windows (Unusual Network Activity from a Windows System Binary — 810 событий) и признаками внедрения процесса из вредоносного документа (Potential Process Injection from Malicious Document — 625 событий). Подробная информация представлена в таблице 2.

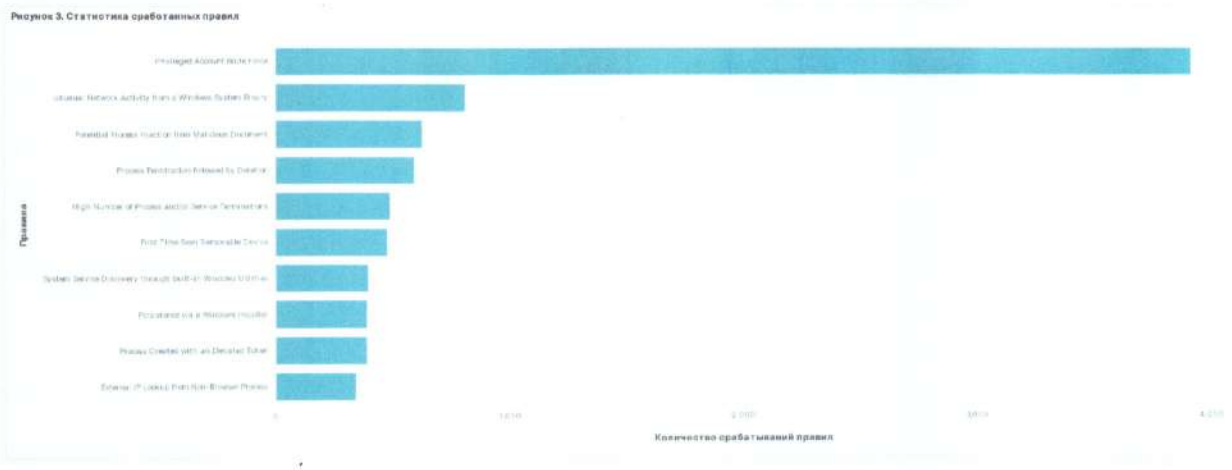

Рисунок 3. Статистика сработанных правил

Таблица 1 отражает количество срабатываний корреляционных правил информационной безопасности в SIEM-системе за отчётный период и используется для анализа наиболее актуальных типов угроз и аномальной активности в инфраструктуре.

Таблица 1. Правила корреляции

Наименование правила	Количество срабатываний
Privileged Account Brute Force	3,912
Unusual Network Activity from a Windows System Binary	810
Potential Process Injection from Malicious Document	625
Process Termination followed by Deletion	591
High Number of Process and/or Service Terminations	488
First Time Seen Removable Device	476
System Service Discovery through built-in Windows Utilities	395
Persistence via a Windows Installer	389
Process Created with an Elevated Token	389
External IP Lookup from Non-Browser Process	341

Таблица 1. Правила корреляции

Примечание: Полная таблица обработанных правил корреляции представлена в Приложении 1.

Стоит отметить, что распределение срабатываний корреляционных правил информационной безопасности в SIEM-системе в разрезе дней отчётного периода отражает динамику событийной активности в инфраструктуре. Подробная информация описана на рисунке 4.

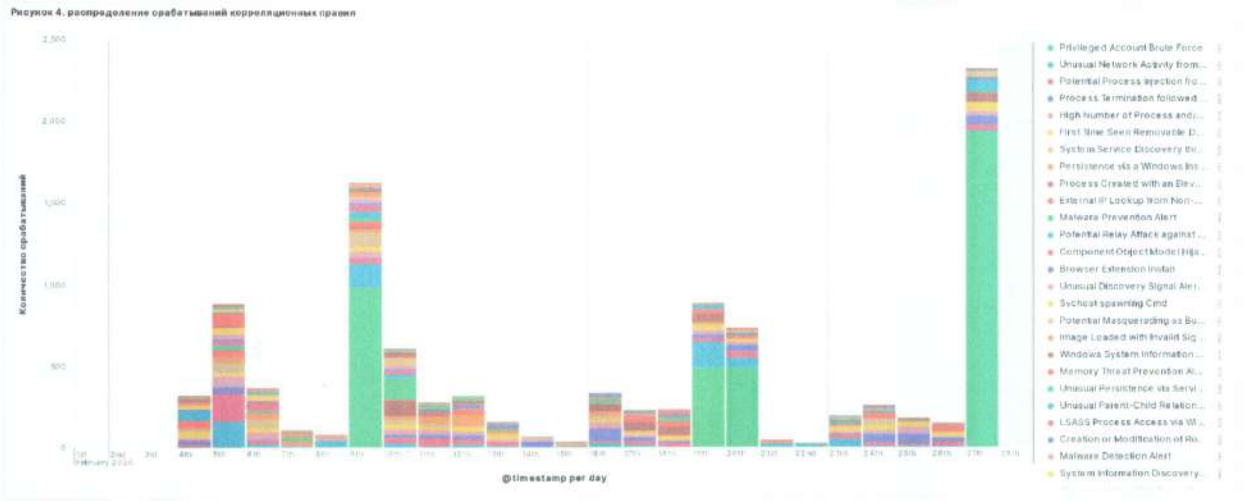

Рисунок 4. распределение срабатываний корреляционных правил

Проведен комплекс мероприятий по мониторингу, анализу и корреляции событий информационной безопасности. В ходе работ выполнен детальный анализ срабатываний средств защиты, включая события, требующие дополнительного рассмотрения, такие как аномальная активность процессов, изменения в системных компонентах и операции в доменной среде. Все выявленные события были проанализированы аналитиками в рамках установленного процесса мониторинга и реагирования; по итогам рассмотрения нарушений функционирования информационных систем не выявлено, однако посредством поиска угроз был выявлен подозрительный хост, который на текущий момент анализируется подробности в разделе Поиск угроз информационной безопасности.

4. МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Статистика событий безопасности

В рамках мониторинга системы обнаружения и предотвращения угроз за отчетный период было зарегистрировано **4551 событий (alerts)** различного уровня критичности.

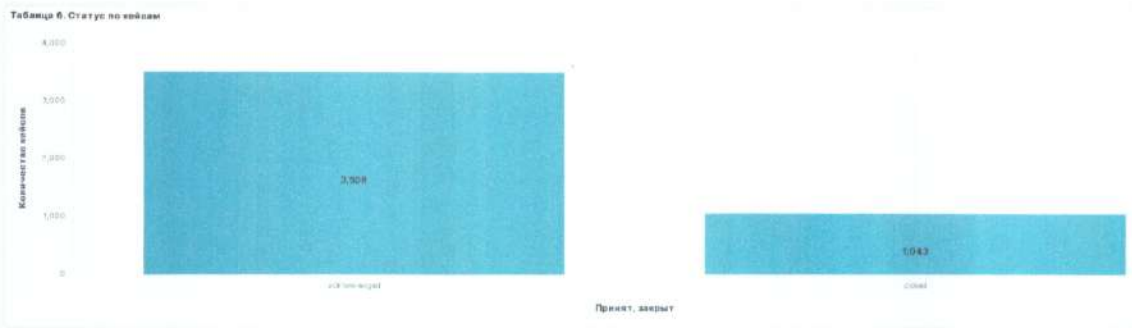

Рисунок 5. Статус по кейсам

Диаграмма отражает распределение кейсов по статусам обработки. Основная часть кейсов находится в статусе ***acknowledged***, что свидетельствует о принятии событий в работу, при этом часть кейсов успешно завершена и переведена в статус ***closed***.

За отчётный период в системе зарегистрированы и обработаны кейсы информационной безопасности, связанные со срабатываниями корреляционных правил. Основная часть событий относится к завершению процессов и служб, а также к фиксации подключений ранее не использовавшихся съёмных носителей. Все выявленные события были проанализированы в установленном порядке и по результатам рассмотрения переведены в статус *closed*. Признаков реализации инцидентов информационной безопасности или нарушения функционирования информационных систем за отчётный период не выявлено.

Таблица 3. Статус закрытых кейсов

Сработанные правила	Количество закрытых кейсов	Дата и время
High Number of Process and/or Service Terminations	486	Feb 4, 2026 @ 17:02:42.141
First Time Seen Removable Device	338	Feb 4, 2026 @ 15:35:51.981
Process Termination followed by Deletion	197	Feb 4, 2026 @ 20:01:59.312
Multiple Alerts involving a User [Duplicate]	9	Feb 6, 2026 @ 17:16:56.500
Disable Windows Firewall Rules via Netsh	8	Feb 24, 2026 @ 14:19:23.403
Persistence via a Windows Installer	2	Feb 14, 2026 @ 19:56:18.837
Unusual Persistence via Services Registry	2	Feb 6, 2026 @ 14:05:22.196
Unusual Discovery Signal Alert with Unusual Process Command Line	1	Feb 22, 2026 @ 04:19:52.930

Рисунок 6. Статус закрытых кейсов

Примечание: Полная таблица закрытых кейсов представлена в Приложении 2.

За отчетный период аналитиками зафиксировано распределение событий информационной безопасности по рабочим станциям, при котором на TOP-10 хостов приходится наибольшее количество срабатываний средств защиты. Повышенная событийная активность на указанных рабочих станциях обусловлена выявлением подозрительных и аномальных действий, а также повторяющимися срабатываниями, связанными с легитимной активностью и потенциально нежелательным программным обеспечением. Все выявленные события и случаи вредоносной активности своевременно анализируются и устраняются аналитиками в рамках установленного процесса мониторинга и реагирования.

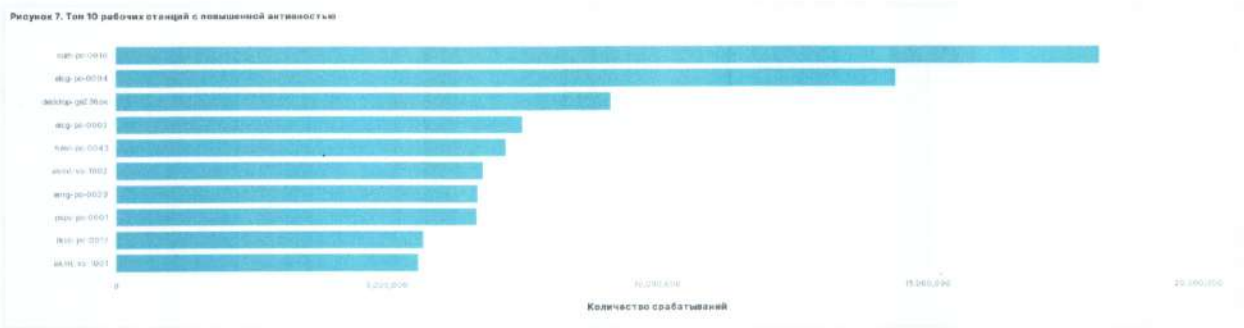

Рисунок 7. Топ 10 рабочих станций с повышенной активностью

В рамках мониторинга зафиксированы запуски преимущественно легитимных системных и пользовательских процессов, связанных со штатной работой операционной системы, администрированием, обслуживанием оборудования и установкой программного обеспечения. К таким процессам относятся стандартные компоненты Windows и прикладные приложения, использование которых не выходит за рамки допустимой и ожидаемой активности. По результатам анализа признаков нелегитимного или неконтролируемого выполнения процессов не выявлено.

Отдельные процессы (*cmd.exe, nslookup.exe, regsvr32.exe*) могут использоваться как в административных, так и в потенциально небезопасных сценариях, в связи с чем их запуск был подвергнут дополнительному анализу аналитиками. По результатам проведённого анализа все зафиксированные события признаны легитимными, подтверждённых случаев нелегитимного или вредоносного выполнения процессов за отчётный период не выявлено.

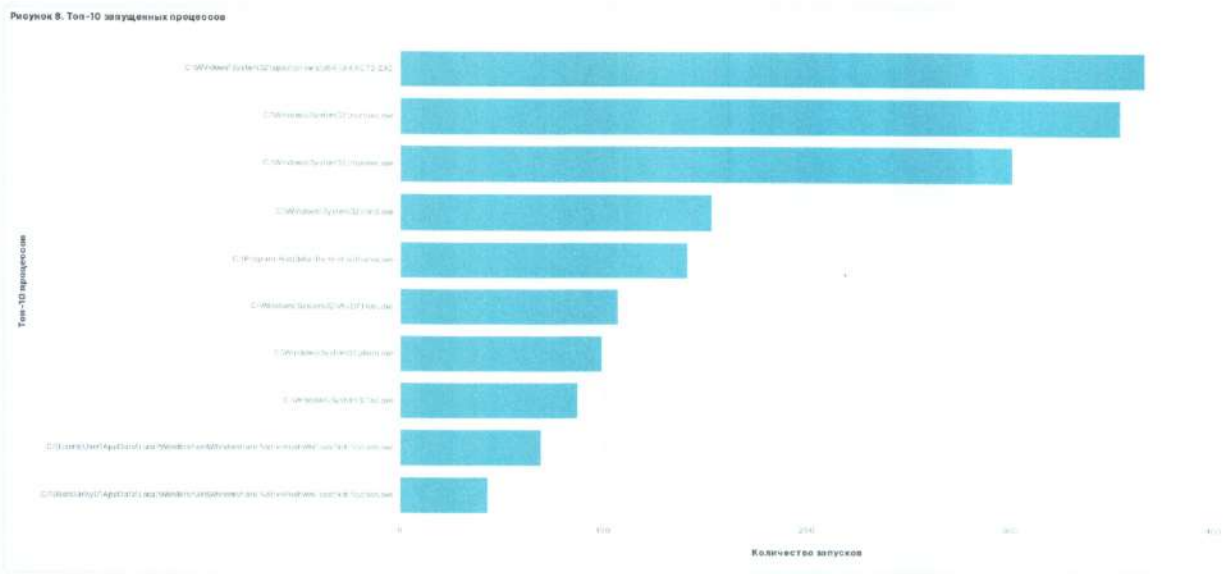

Рисунок 8. Топ-10 запущенных процессов

На рисунке 9 приведён перечень наиболее часто запускаемых процессов за отчётный период с указанием количества их запусков, зафиксированных средствами мониторинга информационной безопасности. Представленные данные отражают активность системных и пользовательских процессов, используемых в рамках штатной эксплуатации информационных систем.

Таблица 4. Обработанные процессы

Обработанные процессы	Количество
C:\Windows\System32\spool\drivers\x64\3\KACT.2.EXE	366
C:\Windows\System32\svchost.exe	354
C:\Windows\System32\msiexec.exe	301
C:\Windows\System32\cmd.exe	153
C:\Program Files\Mozilla Firefox\firefox.exe	141
C:\Windows\System32\WUDFHost.exe	107
C:\Windows\System32\dwm.exe	99
C:\Windows\System32\sc.exe	67
C:\Users\User\AppData\Local\Wondershare\Wondershare NativePush\WsToastNotification.exe	69
C:\Users\aray0\AppData\Local\Wondershare\Wondershare NativePush\WsToastNotification.exe	43

Рисунок 9. Обработанные процессы

Примечание: Полная таблица обработанных процессов описаны в Приложении 3.

4.2. Сопровождение и реагирование на инциденты информационной безопасности

В рамках операционной деятельности Поставщик осуществляет непрерывное сопровождение выявленных инцидентов информационной безопасности на всех этапах их жизненного цикла — от первичной регистрации до полного закрытия. Каждый зафиксированный инцидент проходит через установленный процесс обработки: первичную классификацию и верификацию аналитиками первой линии, углублённый

анализ аналитиками второй линии при необходимости, формирование карточки инцидента в системе IRP с фиксацией всех значимых атрибутов, а также подготовку рекомендаций по реагированию и устранению последствий.

4.3 Поиск угроз информационной безопасности (Threat Hunting)

В отчетном периоде специалистами Поставщика проведены мероприятия по проактивному поиску угроз (Threat Hunting) в информационно-коммуникационной инфраструктуре Заказчика. Работы выполнялись в рамках постоянного анализа событий безопасности, накопленных SIEM-системой, с применением гипотез о возможных векторах атак, техник и тактик, описанных в матрице MITRE ATT&CK, а также актуальных данных об угрозах, поступающих из источников Threat Intelligence.

В ходе проверки анализировались поведенческие паттерны пользователей и процессов, сетевые взаимодействия, активность на конечных устройствах, попытки горизонтального перемещения и аномалии в работе доменной инфраструктуры. По результатам проведённых мероприятий признаков компрометации (IoC), скрытого присутствия злоумышленника, несанкционированного доступа к ресурсам Заказчика, а также подозрительной активности, требующей эскалации, не обнаружено. Инфраструктура Заказчика в рамках зоны мониторинга оценивается как не скомпрометированная на дату составления настоящего отчёта.

4.4. Проверка безопасности веб-ресурса

В ходе проверки веб-сервиса electorat.almaty.kz выявлены критичные проблемы, связанные с доступом к API и возможностью массового сбора данных. В клиентском JavaScript обнаружено хранение учетных данных для Basic Auth, из-за чего любой посетитель может извлечь секрет из кода страницы и использовать его для обращения к API. Дополнительно отмечено отсутствие ограничений частоты запросов к методу поиска по ИИН, что создает риск автоматизированного перебора и массового извлечения сведений об избирательных участках, а также повышает вероятность злоупотреблений и перегрузки сервиса.

Также зафиксированы дефекты маршрутизации/валидации входных данных: параметр пути в `/api/voter/search/{iin}` принимает traversal-последовательности, позволяя получать непредусмотренные ресурсы (статические файлы и ответы других роутов), что нарушает границы между API и веб-контентом. Отдельно отмечено отсутствие защиты от clickjacking (нет `X-Frame-Options` и/или `Content-Security-Policy frame-ancestors`).

Рекомендуемые меры включают удаление секретов из клиентского кода и ротацию скомпрометированных данных, внедрение rate limiting и мониторинга аномалий, строгую серверную валидацию формата ИИН и нормализацию пути, разделение обработки `/api/*` и статики, а также добавление антифреймингових заголовков.

Рисунок 10. hardcoded credentials в клиентском коде и декодирование Basic Auth

Полная информация по анализу и проверке безопасности веб-сервиса electorat.almaty.kz описаны в Приложении 4.

4.5. Автоматическое реагирование на угрозы

В соответствии с пунктом 1.1.6 технической спецификации, в системе обнаружения и реагирования на угрозы реализованы меры автоматического реагирования на инциденты информационной безопасности. Данные меры включают:

- Автоматический анализ поступающих событий с использованием искусственного интеллекта;
- Блокировку подозрительных объектов и сетевых соединений;
- Изоляцию вредоносных процессов и помещение файлов в карантин;
- Применение обновлённых политик безопасности для предотвращения повторных инцидентов.

4.5. Проанализированные программы в рамках мониторинга

В рамках мониторинга выполнен анализ подозрительного образца **LevelDB.bat**, который фактически является **PE32 GUI (x86)** и используется как **лоадер/стейджер** с маскировкой под .bat. Установлено, что лоадер содержит

два зашифрованных PE-компонента, расшифровывает их и дропает на диск, после чего запускает второй этап (EXE); при обнаружении процессов защитного ПО дополнительно дропается и подгружается DLL-модуль, предназначенный для противодействия средствам защиты (anti-defense/anti-AV).

Функциональность второго этапа ориентирована на распространение и сбор данных: модуль подключается к **Skype Desktop API**, получает сведения о контактах/чатах и выполняет рассылку сообщений, что используется как основной канал распространения. Также выявлена сетевая логика **SSDP/UPnP** (включая M-SEARCH и AddPortMapping) для попыток проброса порта (NAT traversal), функции снятия скриншотов и упаковки данных в архив через установленный **WinRAR**. В качестве IoC отмечаются дроп EXE/DLL в **%TEMP%**, характерные строки (в т.ч. SkypeControlAPI*, WinRAR\rar.exe, M-SEARCH * HTTP/1.1) и SSDP-трафик на **239.255.255.250:1900**; в рекомендациях указаны изоляция хоста, сбор артефактов из %TEMP%, проверка активности Skype и проверка роутера на подозрительные UPnP-порт-маппинги, а также охота по указанным строковым индикаторам.

5. АНАЛИЗ УЯЗВИМОСТЕЙ

5.1 Инструментальное сканирование

Ежемесячно проводится комплексное инструментальное сканирование внутреннего и внешнего периметра сети. Работы выполняются в строгом соответствии с технической спецификацией Акимата города Алматы и включают анализ на наличие уязвимостей, отклонений в конфигурациях и потенциальных точек компрометации. Проведение регулярного сканирования позволяет поддерживать высокий уровень защищённости инфраструктуры, своевременно выявлять риски и обеспечивать их оперативную обработку.

По результатам сканирования за отчётный период установлено, что основная часть выявленных уязвимостей относится к уровню *Medium*, при этом уязвимости уровней *High* и *Critical* выявлены в ограниченном количестве и сосредоточены в отдельных подразделениях.

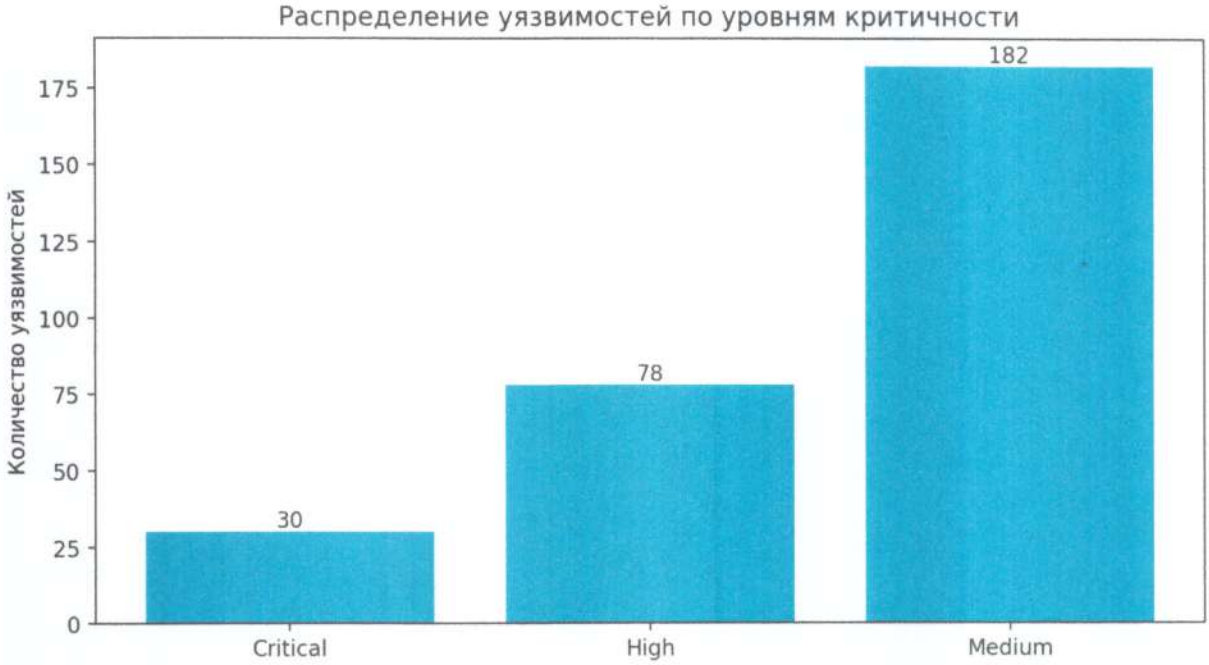

Рисунок 11. Уровень критичности

Наибольшая событийная активность зафиксирована в управлении энергетики, строительстве, общественном развитии и городской мобильности. Ряд подразделений по результатам сканирования уязвимостей не выявил, что свидетельствует о корректном уровне защищённости. Выявленные уязвимости приняты в работу в рамках установленного процесса управления уязвимостями.

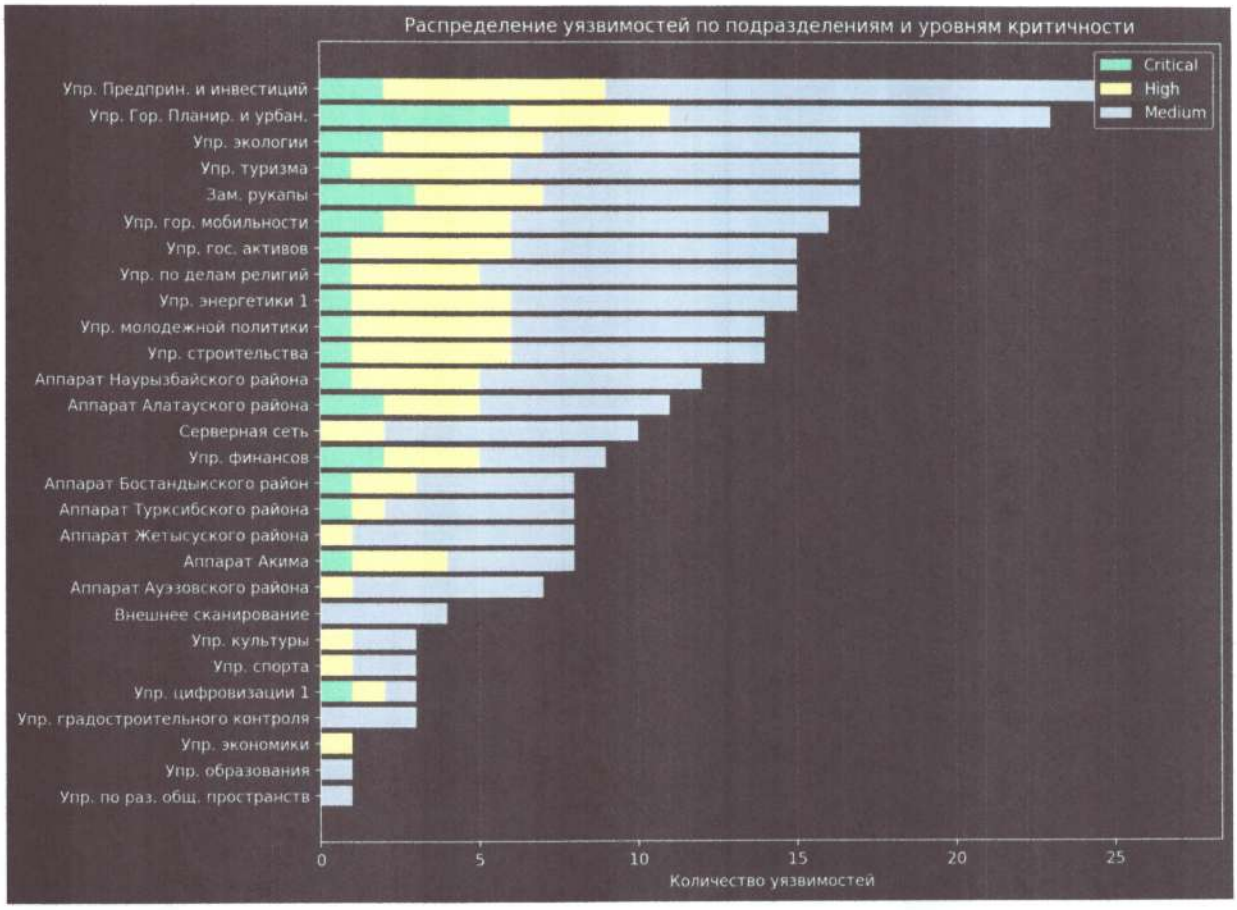

Рисунок 12. Распределение уязвимости по подразделениям

В целом результаты анализа свидетельствуют о контролируемом уровне рисков информационной безопасности и эффективности действующих процессов мониторинга и управления уязвимостями. Продолжение регулярных сканирований и последующая корреляция результатов с данными SIEM и EDR позволят своевременно выявлять изменения в уровне защищённости и минимизировать потенциальные риски.

Таблица 2. Сканирование сети

№	Подразделение (объект сканирования)	Critical	High	Medium
1	Аппарат Акима	1	3	4
2	Аппарат Алатауского района	2	3	6
3	Аппарат Ауэзовского района	0	1	6
4	Аппарат Бостандыкского район	1	2	5
5	Аппарат Жетысуского района	0	1	7
6	Аппарат Медеуского района	0	0	0
7	Аппарат Наурызбайского района	1	4	7
8	Аппарат Турксибского района	1	1	6
9	Внешнее сканирование	0	0	4
10	Зам. рукапы	3	4	10

№	Подразделение (объект сканирования)	Critical	High	Medium
11	Серверная сеть	0	2	8
12	Упр. гор. мобильности	2	4	10
13	Упр. Гор. Планир. и урбан.	6	5	12
14	Упр. гос. активов	1	5	9
15	Упр. градостроительного контроля	0	0	3
16	Упр. занятости и соц. программ	0	0	0
17	Упр. здравоохранения	0	0	0
18	Упр. земельных отношений	0	0	0
19	Упр. культуры	0	1	2
20	Упр. молодежной политики	1	5	8
21	Упр. образования	0	0	1
22	Упр. общественного развития	0	0	0
23	Упр. по делам религий	1	4	10
24	Упр. по раз. общ. пространств	0	0	1
25	Упр. Предприн. и инвестиций	2	7	18
26	Упр. развития коммун. инфрстр.	0	0	0
27	Упр. Сейс. Безопас. и мобил. подготовки	0	0	0
28	Упр. спорта	0	1	2
29	Упр. строительства	1	5	8
30	Упр. туризма	1	5	11
31	Упр. финансов	2	3	4
32	Упр. цифровизации 1	1	1	1
33	Упр. цифровизации 2	0	0	0
34	Упр. экологии	2	5	10
35	Упр. экономики	0	1	0
36	Упр. энергетики 1	1	5	9
37	Упр. энергетики 2	0	0	0

Примечание: Подробная информация по сканированиям сети указаны в Приложении 5, 6 и 7.

5.2 Статистика управления уязвимости

Диаграмма отражает сравнение количества выявленных уязвимостей по уровням критичности между текущим и предыдущим запусками сканирования. Текущий запуск выполнен 2026-02-27 23:51:41, предыдущий – 2026-02-09 19:06:34

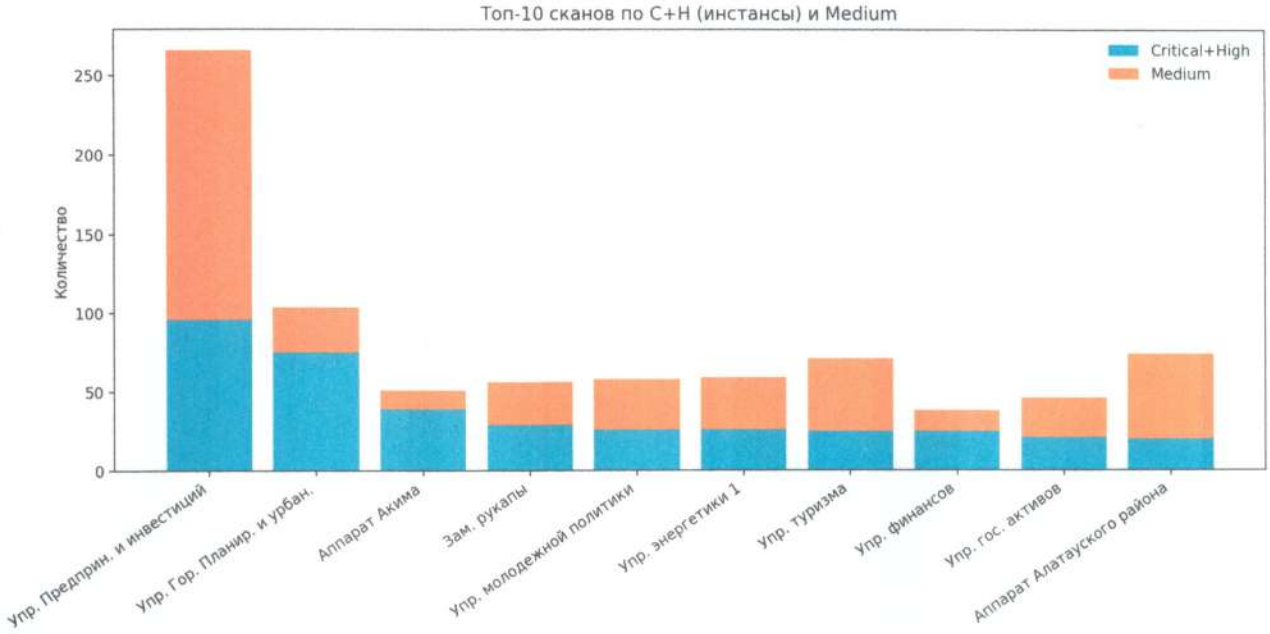

Рисунок 13. Топ-10 сканов

По результатам сравнения текущего и предыдущего запусков сканирования **изменений в количестве уязвимостей выявлено**. Новые уязвимости отсутствуют, устранённые уязвимости зафиксированы, рост или снижение критичных уязвимостей наблюдается. Состояние защищённости инфраструктуры характеризуется как **стабильное**.

6. ПЛАТФОРМА АНАЛИЗА УГРОЗ И ЗАЩИТА ОТ ТАРГЕТИРОВАННЫХ АТАК

6.1. OpenCTI - Платформа киберразведки

Для обеспечения проактивного подхода к выявлению и предотвращению киберугроз в инфраструктуре Заказчика используется платформа анализа угроз **OpenCTI (Open Cyber Threat Intelligence Platform)**, развернутая по адресу **172.16.16.78:8080**. Данное решение обеспечивает централизованное хранение, корреляцию и визуализацию данных об угрозах, включая:

- индикаторы компрометации (IoC);
- тактики, техники и процедуры атак в соответствии с фреймворком **MITRE ATT&CK**;
- информацию о киберпреступных группировках, вредоносных кампаниях и используемых инструментах.

По результатам текущего анализа и расследования инцидентов выявленные индикаторы компрометации *(IP-адреса, хэши файлов, домены, URL, имена процессов и иные артефакты)* были проанализированы и добавлены в базу OpenCTI, что обеспечивает их последующее использование

при корреляции событий, threat hunting и автоматизированном выявлении схожих угроз в инфраструктуре.

Рисунок 14. OpenCTI

Актуализация базы IoC в OpenCTI позволяет повысить эффективность мониторинга, сократить время реагирования на повторяющиеся и схожие атаки, а также обеспечивает накопление аналитической базы для последующего прогнозирования и предотвращения потенциальных киберугроз.

6.2. MISP — Обмен индикаторами компрометации

На стороне Поставщика функционирует и поддерживается платформа MISP, посредством которой осуществляется обмен индикаторами компрометации с АО «ГТС». Поставщиком осуществляется постоянный мониторинг и отработка поступающих запросов в рамках действующих процедур реагирования. Все обращения, поступающие через MISP, анализируются на предмет наличия вредоносной активности, проводится проверка источников угроз в соответствии с пунктом 1.1.27 технической спецификации.

За отчетный период угроз информационной безопасности не выявлено.

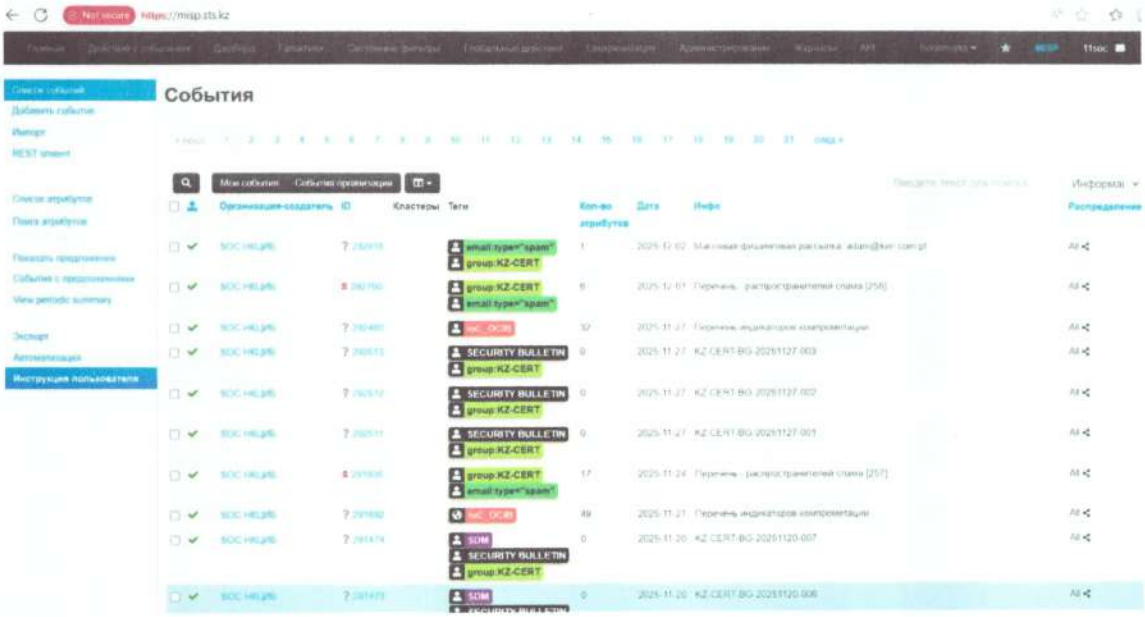

Рисунок 15. MISP

6.3. T-Lab Sandbox — Защита от таргетированных атак

Поставщиком реализованы меры защиты от таргетированных кибератак и угроз нулевого дня с использованием системы динамического и статического анализа T-Lab Sandbox, интегрированной с SIEM и EDR для централизованного мониторинга и реагирования. В отчётном периоде в системе анализа угроз в режиме реального времени проверено 320 объектов, из которых выявлено 3 угрозы и 57 подозрительных, что составляет незначительную долю от общего потока и не указывает на массовые инциденты; основная нагрузка носит неравномерный характер с пиковыми значениями в отдельные периоды (до ~150 загрузок), при этом в остальное время сохраняется низкий уровень активности; максимальные оценки угроз достигают порядка 100, что свидетельствует о наличии отдельных потенциально опасных объектов; в структуре файлов преобладают текстовые, далее следуют исполняемые, остальные типы (Java, PDF, MS Office, изображения) занимают малую долю; в разрезе недели наибольшая активность зафиксирована 26 февраля, после чего отмечается спад к концу периода, что в целом соответствует нормальному рабочему режиму системы без критических отклонений.

Рисунок 16. Статистика заблокированных ВПО

За период с 1 по 28 февраля 2026 года в систему T-Lab Anti-APT поступило 4997 отчетов; в течение месяца наблюдалась в целом стабильная динамика поступления с незначительными колебаниями и отдельными кратковременными снижениями, при этом к концу периода зафиксирован рост активности с достижением пиковых значений; основную долю составляют отчеты по текстовым файлам, далее следуют исполняемые файлы, тогда как

Java, PDF, изображения, MS Office и Android-пакеты представлены в значительно меньшем объеме; в целом поток отчетов носит стабильный характер без признаков аномальной или критической активности.

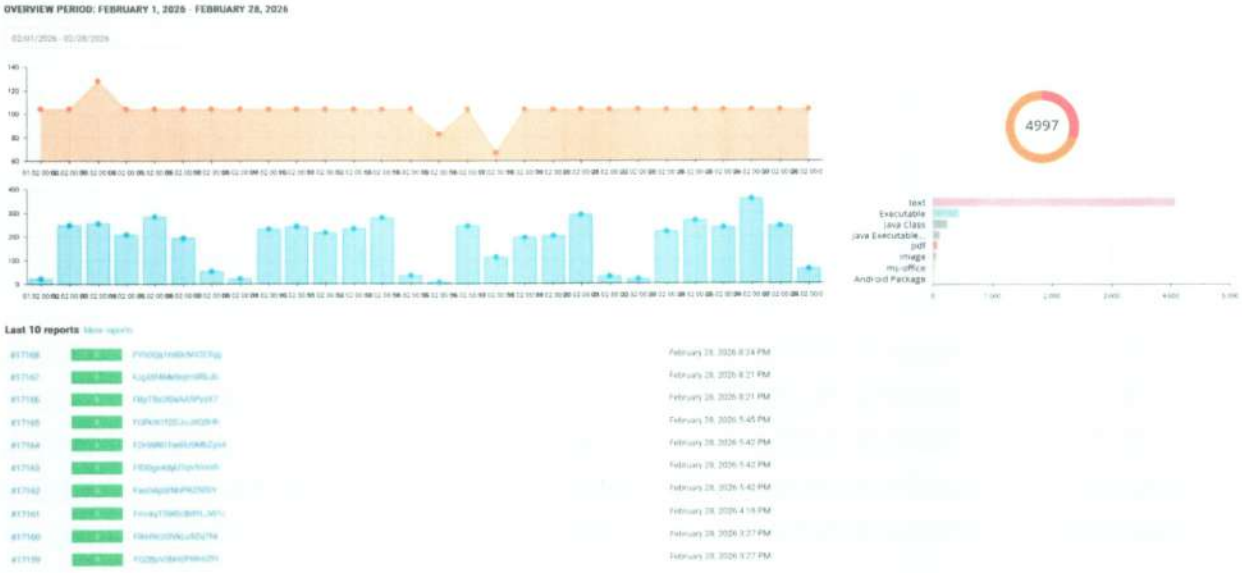

Рисунок 17. Статистика отчетов с системы T-Lab Anti-APT

В ходе анализа угроз были выявлены уникальные файловые хэши (SHA-256), ассоциированные с подозрительными и потенциально вредоносными объектами. Указанные индикаторы компрометации использовались для идентификации файлов, корреляции событий и оценки рисков. По результатам анализа выявленные IOC были внесены в платформу анализа угроз **OpenCTI** для централизованного хранения, последующего обогащения, корреляции с другими инцидентами и использования в дальнейших мероприятиях по мониторингу и предотвращению киберугроз.

Примечание: Подробный отчет T-Lab описан в Приложении 8.

6.4. DLP – Предотвращение утечек данных (safetica)

В ходе анализа телеметрии и, поступающей с рабочих станций в систему предотвращения утечек данных (DLP), установлено, что агенты функционируют в штатном режиме.

Все устройства регулярно передают данные в систему, что подтверждается колонками *«Записи отправлены»* и *«Последний ответ»*.

Обновления модулей защиты применяются своевременно - для всех станций отображается актуальная метка *«Защита обновлена»*. Фактов отключения агента, попыток его удаления или обхода не выявлено.

Времена входа пользователей соответствуют рабочему графику. Подозрительных логинов и активности, характерной для инсайдерских действий или компрометации учётных данных, не обнаружено.

Отражает общее число обращений по каждому подразделению. Высокие значения связаны с большим количеством пользователей и интенсивной работой систем.

6.4.1. Анализ веб – активности

В отчётном периоде с **1 по 28 февраля 2026 года** проведён анализ веб-активности пользователей в инфраструктуре Заказчика. Зафиксирован доступ к **5 022 проверенным веб-сайтам**, при этом **3 831 ресурс** отнесён к сайтам **без категории** и подлежит дополнительному анализу. **Заблокированных сайтов не выявлено (0), блокировки не применялись.**

При этом в разрезе веб-категорий зафиксированы единичные обращения к категориям Malware (3 сайта, суммарно 3 мин 54 с, 2 пользователя) и Pornography (2 сайта, суммарно 19 мин 3 с, 2 пользователя), что требует выборочной проверки контекста обращений и при необходимости актуализации политик фильтрации.

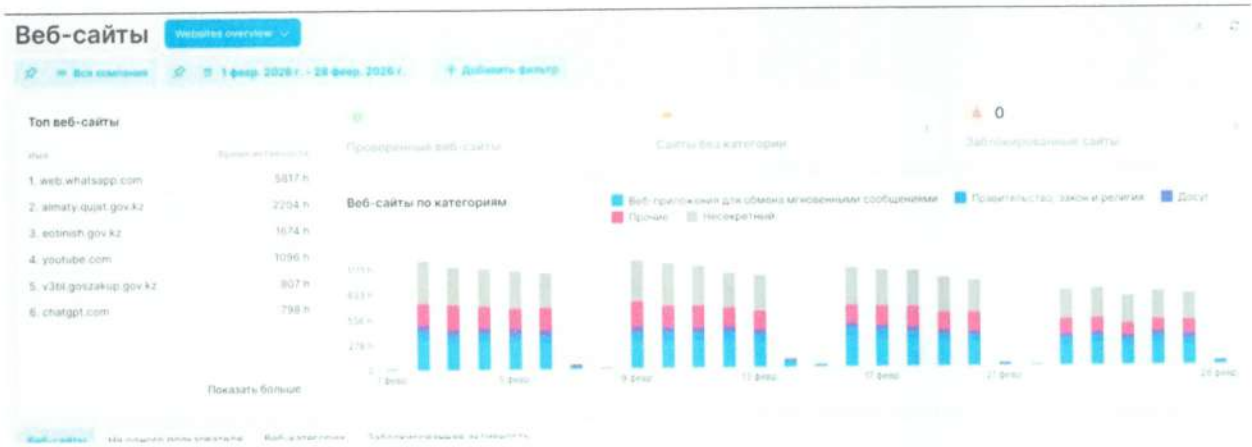

Рисунок 18. Веб-сайты

Примечание: Подробный отчет DLP описан в Приложении 9.

Дополнительно зафиксированы единичные события средней и высокой степени важности, связанные с обработкой и перемещением данных. Основная активность пользователей приходилась на работу с неклассифицированными данными и стандартные каналы передачи информации (USB-устройства, локальные ресурсы, веб-сервисы и почта). Все выявленные события были

проанализированы аналитиками в рамках установленного процесса контроля. Фактов утечки или несанкционированной передачи конфиденциальной информации не выявлено.

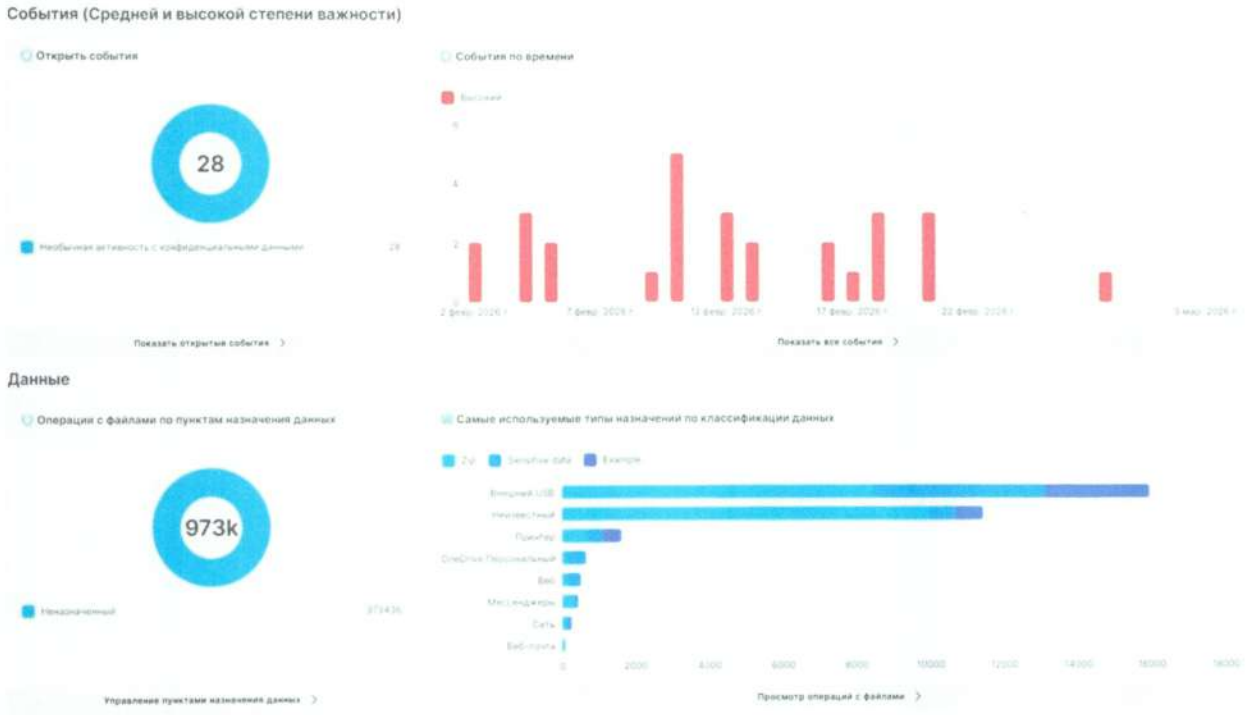

Рисунок 19. Средний и высокий степень важности

6.4.2. Передачи данных

Диаграмма «Топ-10 приложений» отражает распределение активности по наиболее используемым пользовательским и системным приложениям за отчётный период в разрезе суммарного времени использования. Наибольшая активность зафиксирована в веб-браузерах, прежде всего Google Chrome (16 483 ч), а также Microsoft Edge (1 151 ч) и Firefox (2 033 ч), что соответствует регулярной работе пользователей с веб-ресурсами и корпоративными сервисами. Существенная доля активности также приходится на системные и офисные приложения: Проводник Windows (4 342 ч), Microsoft Word (4 093 ч) и Microsoft Excel (2 362 ч), что отражает интенсивную работу с файлами и документами.

Дополнительно в топ входят WhatsApp (706 ч) как канал рабочей коммуникации, Microsoft PowerPoint (392 ч) и Adobe Acrobat (359 ч), используемые при подготовке и просмотре материалов, а также 1cv8 (357 ч), связанный с эксплуатацией прикладных информационных систем. В целом распределение активности соответствует типовой служебной деятельности

пользователей; признаков аномального или вредоносного использования приложений по представленным агрегированным данным не выявлено.

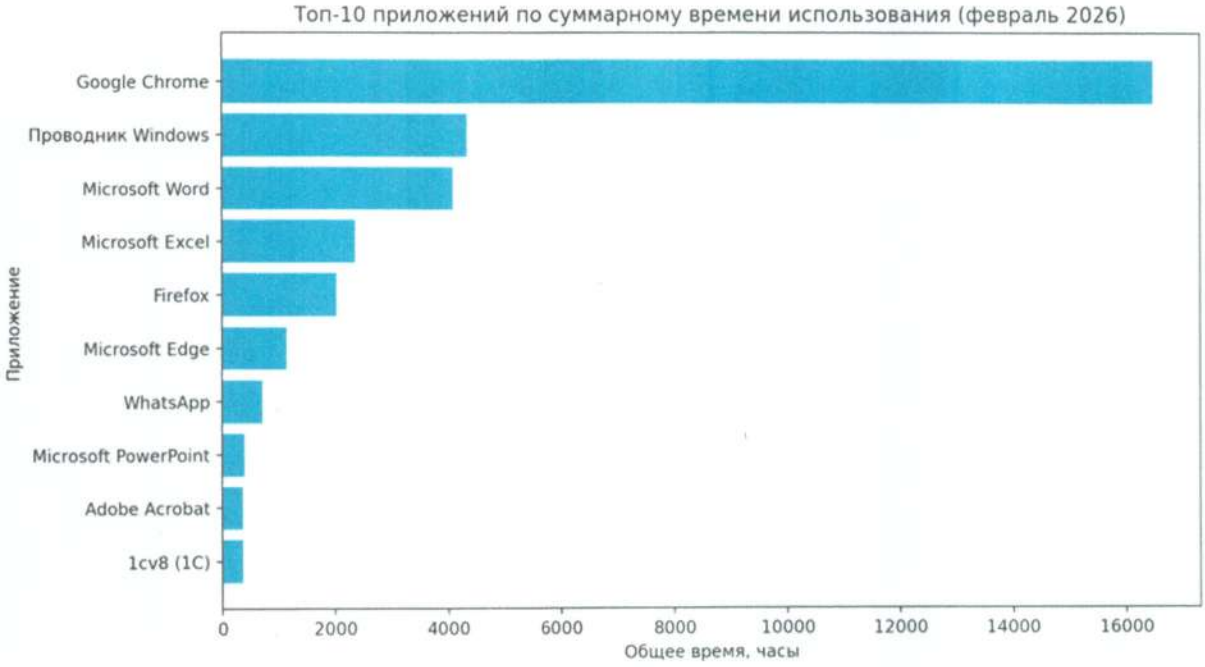

Рисунок 20. Топ-10 приложений

Таблица 3 отражает распределение активности по основным пользовательским и системным приложениям за отчётный период.

Таблица 3. Распределение активности

№	Приложение	Категория	Общее время
1	Google Chrome	Веб-браузер	16 483 ч
2	Проводник Windows	Windows	4 342 ч
3	Microsoft Word	Офисный пакет	4 093 ч
4	Microsoft Excel	Офисный пакет	2 362 ч
5	Firefox	Веб-браузер	2 033 ч
6	Microsoft Edge	Веб-браузер	1 151 ч
7	WhatsApp	Мессенджер / VOIP	706 ч

8	Microsoft PowerPoint	Офисный пакет	392 ч
9	Adobe Acrobat	PDF-ридер	359 ч
10	1cv8 (1C)	CRM-система	357 ч

6.4.3. Служебные операции через интернет и внутренние сервисы

Диаграмма отражает распределение суммарного времени нахождения пользователей в интернете и корпоративной сети Заказчика. Наибольшая сетевая активность зафиксирована у пользователей **Guest TKSB** и **Guest JETS**, что обусловлено спецификой выполняемых служебных задач. В целом характер интернет-активности пользователей носит рабочий и равномерный характер, отклонений и аномального поведения не выявлено.

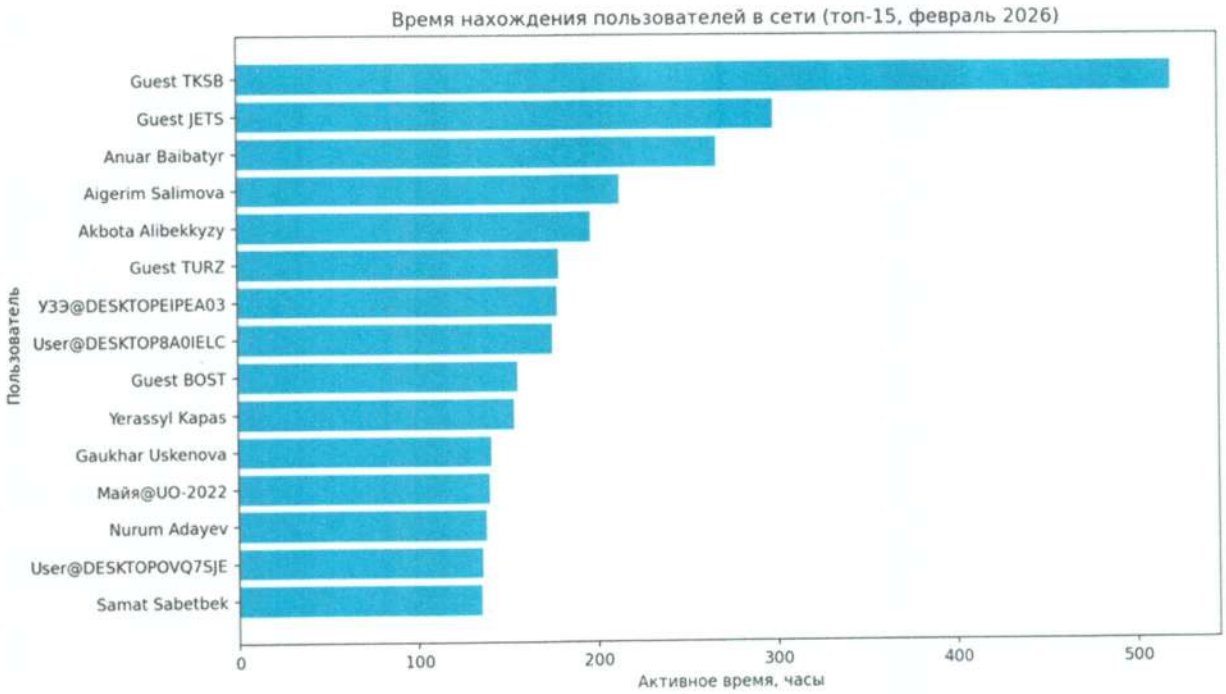

Рисунок 21. Время нахождения пользователя в сети

Представленные данные отражают **сетевую активность пользователей в интернете и корпоративной сети Заказчика** за отчётный период. Активное время показывает, сколько времени пользователи находились в сети, взаимодействовали с веб-ресурсами и приложениями, а также выполняли служебные операции через интернет и внутренние сервисы.

Таблица 4. Сетевая активность пользователя

№	Пользователь	Кол-во сессий	Кол-во пользователей	Активное время (суммарно)	Среднее активное время в день
1	Guest TKSB	42	1	519 ч 35 мин 46 с	18 ч 33 мин 25 с
2	Guest JETS	53	1	298 ч 35 мин 12 с	10 ч 39 мин 49 с
3	Anuar Baibatyr	15	1	266 ч 49 мин 23 с	9 ч 31 мин 45 с
4	Aigerim Salimova	31	1	212 ч 42 мин 50 с	7 ч 35 мин 48 с
5	Akbota Alibekkyzy	24	1	196 ч 43 мин 19 с	7 ч 1 мин 32 с
6	Guest TURZ	29	1	178 ч 41 мин 56 с	6 ч 22 мин 55 с
7	УЗЭ@DESKTOPEIPEA03	23	1	178 ч 2 мин 43 с	6 ч 21 мин 31 с
8	User@DESKTOP8A0IELC	24	1	174 ч 54 мин 27 с	6 ч 14 мин 48 с
9	Guest BOST	30	1	155 ч 19 мин 39 с	5 ч 32 мин 50 с
10	Yerassyl Kapas	22	1	153 ч 29 мин 53 с	5 ч 28 мин 55 с
11	Gaukhar Uskenova	21	1	140 ч 45 мин 22 с	5 ч 1 мин 37 с

№	Пользователь	Кол-во сессий	Кол-во пользователей	Активное время (суммарно)	Среднее активное время в день
12	Майя@UO-2022	29	1	139 ч 49 мин 23 с	4 ч 59 мин 37 с
13	Nurum Adayev	27	1	137 ч 53 мин 40 с	4 ч 55 мин 29 с
14	User@DESKTOPOVQ7SJE	20	1	135 ч 39 мин 4 с	4 ч 50 мин 40 с
15	Samat Sabetbek	19	1	135 ч 3 мин 19 с	4 ч 49 мин 24 с

6.5 Checkpoint - межсетевой экран

За отчётный период в инфраструктуре Заказчика осуществлялся непрерывный мониторинг событий информационной безопасности с использованием средств сетевой защиты, антивирусного контроля и предотвращения вторжений. В ходе анализа зафиксировано значительное количество событий, связанных с сетевой активностью и попытками взаимодействия с потенциально небезопасными внешними ресурсами, а также с загрузкой и распространением вредоносных объектов.

Таблица 5. Зафиксированный активность в Межсетевом экране

№	Категория	Показатель	Значение
1	**Общие события безопасности**	Anti-Bot события	**16 920 481**
		Anti-Virus события	**9 296 982**
		IPS-инциденты	1 153 090
		Threat Emulation	**0** (сканирование не выполнялось)
2	**Сетевой трафик**	Получено данных	**17,25 ТВ**

		Передано данных	**1,89 ТВ**
		Общий объём трафика	18,91 ТВ
3	**Инфицированные устройства**	Всего инфицированных	75
		High / Critical	**61**
		Скомпрометированные серверы	**0**
		Активные за последнюю неделю	55
4	**Приложения повышенного риска**	Всего сессий	**12 853 100**
5	**Версия шлюза**	Check Point	**R81.10.17**

В ходе анализа сетевой активности за отчётный период зафиксировано использование приложений и протоколов, потенциально представляющих риск с точки зрения информационной безопасности, в частности BitTorrent Protocol (~1 273 000 сессий, ~8,2 ГБ трафика), MediaGet, uTorrent, а также средств удалённого доступа и VPN-решений (AnyDesk, Thunder VPN, OpenVPN, TouchVPN, I2P). Наибольшая нагрузка приходится на пиринговые протоколы обмена файлами, что указывает на их активное использование в инфраструктуре.

Таблица 6. Сетевая активность

№	Приложение	Сессии	Трафик
1	BitTorrent Protocol	1 273 000	8,2 ГБ
2	MediaGet	5 500	5,4 МБ
3	Thunder VPN	3 600	57,8 КБ
4	AnyDesk	2 900	20,3 МБ
5	uTorrent	1 520	812 КБ

6	BitTorrent Sync	918	802 КБ

Наибольшую долю выявленных событий информационной безопасности составили вредоносные объекты семейства Phorpiex, варианты Infecting URL, а также PUA-объекты. Обнаруженные образцы использовали распространённые форматы исполняемых файлов и запускались из общедоступных директорий. Все выявленные вредоносные объекты были своевременно проанализированы и нейтрализованы.

Таблица 7. Заблокированный ВПО

№	Вредоносное ПО	События
1	Infecting_URL.RS.TC.bec6FhkZ	92
2	KmsdBot.TC.1f22sSpv	40
3	PUA.TC.3626Wodp	40
4	Infecting_URL.VUP.RS.TC.2e44lRqn	23
5	Adware.TC.d7f6NLGo	18
6	Phorpiex.TC.5681FtDa	17
7	dga-PSunA.TC.746b0FzU	17
8	Phorpiex.TC.ee3Smoqo	15

Системой предотвращения вторжений (IPS) были зафиксированы отдельные попытки сетевого воздействия и срабатывания защитных сигнатур, соответствующие типовым сценариям сканирования, эксплуатации уязвимостей и подозрительной сетевой активности. Все выявленные срабатывания были автоматически обработаны средствами защиты и дополнительно проанализированы аналитиками. Признаков успешной эксплуатации, нарушения доступности сервисов либо компрометации информационных систем по результатам рассмотрения не выявлено. Работа IPS обеспечила своевременное обнаружение и блокирование потенциально опасных сетевых воздействий в штатном режиме.

Таблица 8. Система предотвращения вторжений

№	Тип события	Сессии
1	Microsoft Windows NT Null CIFS Sessions	544 000
2	Max Ping Size	37 000
3	TCP Segment Limit Enforcement	19 800
4	TCP Invalid Retransmission	6 237
5	Command Injection	2 124
6	Non Compliant IKE	216
7	Resource Records Enforcement	166

7. РЕАЛИЗОВАННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В соответствии с техническим заданием Поставщиком обеспечено внедрение, сопровождение и поддержка комплексной системы защиты информационной инфраструктуры Заказчика. Ниже представлен статус реализации основных компонентов системы информационной безопасности.

Таблица 9. Статус реализации систем информационной безопасности

№	Система	Назначение	Статус реализации
1	**Система контроля привилегированного доступа (PAM)**	Защищенные доступы администраторов через бастион безопасности, аудит действий	✓ Реализовано. Доступ к инфраструктуре через бастион, ведется аудит действий администраторов
2	**Система сканирования уязвимостей (Nessus)**	Сканирование инфраструктуры, управление уязвимостями, формирование отчетов CVSS	✓ Реализовано. Регулярное сканирование, интеграция с SIEM, контроль устранения критичных уязвимостей
3	**Система обнаружения и реагирования (EDR)**	Защита серверов и PC от вредоносных действий, поведенческий анализ	✓ Реализовано. Elastic EDR интегрирован с T-Lab Sandbox и SIEM, обеспечивает автоматическую изоляцию угроз

№	Система	Назначение	Статус реализации
4	**Система предотвращения утечек (DLP)**	Защита от утечек конфиденциальной информации, контроль каналов передачи	✓ Реализовано. Контроль почтовых, USB и веб-каналов, интеграция с SIEM
5	**Межсетевые экраны нового поколения (Check Point NGFW)**	Защита сетевого периметра от внешних атак, IPS, URL-фильтрация, SSL-инспекция	✓ Реализовано. 15 шлюзов Check Point с активными политиками безопасности, централизованное управление
6	**Система мониторинга событий (SIEM)**	Централизованный сбор и корреляция событий безопасности, формирование отчетов	✓ Реализовано. Интеграция с NGFW, DLP, EDR, PAM, Nessus. Круглосуточный мониторинг
7	**Система оркестрации SOAR**	централизованное управление, автоматизации и координации процессов реагирования на инциденты информационной безопасности.	✓ Реализовано. Интеграция с SIEM, Nessus. Круглосуточный мониторинг, корреляция и playbook
8	**Система регистрации инцидентов**	Централизованного учёта, обработки, классификации и управления инцидентами	✓ Реализовано. Интеграция с SIEM, Nessus. Круглосуточный мониторинг,

№	Система	Назначение	Статус реализации
	информационной безопасности	информационной безопасности	регистрация карточек инцидента информационной безопасности

Примечание: Полная таблица с описанием 17 систем представлена в Приложении 10.

8. ВЫВОДЫ И РЕКОМЕНДАЦИИ

8.1. Общие выводы

1. По итогам мониторинга и анализа событий информационной безопасности за февраль отчётного года установлено, что инфраструктура Заказчика функционировала в штатном и контролируемом режиме.
2. Обеспечен высокий уровень покрытия инфраструктуры средствами защиты информации — в системе мониторинга задействованы агенты SIEM, EDR, DLP и Sysmon на рабочих станциях и серверах Заказчика.
3. В течение отчётного периода проводился круглосуточный (24/7) мониторинг событий информационной безопасности с использованием SIEM, а также дежурной смены аналитиков Поставщик.
4. Все выявленные срабатывания средств защиты, включая события сетевой активности, активности процессов и изменений системных компонентов, своевременно проанализированы и обработаны в рамках установленного процесса реагирования.
5. Фактов нарушения доступности, целостности или конфиденциальности информационных ресурсов Заказчика не зафиксировано.
6. Выявленные вредоносные и подозрительные объекты блокировались средствами EDR, Check Point NGFW и T-Lab Sandbox; подтверждённых случаев распространения вредоносного программного обеспечения в инфраструктуре не выявлено.
7. Сетевая активность пользователей и узлов инфраструктуры соответствовала типовой модели эксплуатации, резких всплесков, признаков DDoS-атак или массовых распределённых воздействий не обнаружено.
8. По результатам анализа инцидентов и событий индикаторы компрометации (IOC) были проанализированы и использованы для актуализации механизмов обнаружения угроз, в том числе с применением платформы Threat Intelligence.

8.2. Приоритетные планы работ

1. Продолжить актуализацию и оптимизацию правил корреляции в SIEM с учётом выявленных сценариев и особенностей инфраструктуры Заказчика.
2. Усилить автоматизацию процессов реагирования за счёт развития сценариев SOAR и контроля полноты телеметрии от агентов.
3. Обеспечить дальнейшую актуализацию политик безопасности EDR, DLP и сетевых средств защиты с учётом выявленных рисков.
4. Продолжится регулярный анализ пользовательской и сетевой активности с целью своевременного выявления поведенческих аномалий, нетипичных паттернов доступа и ранних признаков потенциальных угроз, в том числе с применением инструментов UEBA.
5. Расширять использование Threat Intelligence и платформы OpenCTI для проактивного выявления и предотвращения киберугроз.

8.3. Рекомендации

1) По результатам анализа событий и инцидентов информационной безопасности за отчётный период Поставщиком сформированы следующие рекомендации.

2) Рекомендуется продолжить эксплуатацию внедрённого комплекса средств защиты информации с проведением регулярной актуализации правил, сигнатур и политик безопасности во всех задействованных подсистемах. Своевременное обновление конфигураций является ключевым условием поддержания актуальности защитных механизмов в условиях постоянно меняющегося ландшафта угроз.

3) Необходимо обеспечить постоянный контроль полноты и качества поступающих событий от всех подключённых источников — SIEM, EDR, DLP, Check Point и T-Lab Sandbox. Перебои в передаче телеметрии или неполнота журналов событий могут приводить к пропускам при обнаружении угроз, в связи с чем данный аспект требует систематического контроля.

4) Рекомендуется активно использовать результаты анализа IoC и данные T-Lab Sandbox для планомерного пополнения базы знаний угроз и совершенствования механизмов корреляции. Накопленная аналитика позволяет повышать точность детектирования и сокращать среднее время обнаружения новых угроз.

5) Заказчику рекомендуется продолжить проведение мероприятий по повышению осведомлённости пользователей в области информационной безопасности, включая обучение правилам безопасной работы с интернет-ресурсами, электронной почтой и съемными носителями. Человеческий фактор остаётся одним из наиболее значимых векторов реализации атак социальной инженерии и фишинга.

6) Рекомендуется обеспечить неукоснительное соблюдение требований технической документации, регламентирующей эксплуатацию информационно-коммуникационной инфраструктуры Заказчика. Эксплуатация программного обеспечения, средств защиты информации и сетевых компонентов должна осуществляться строго в соответствии с утверждёнными техническими регламентами, инструкциями по эксплуатации и руководящими документами по информационной безопасности. Отступление от установленных технических требований, самостоятельная модификация конфигураций без согласования с ответственными специалистами, а также эксплуатация компонентов инфраструктуры в режимах, не предусмотренных документацией производителя, создают

дополнительные риски нарушения целостности и безопасности инфраструктуры в целом.

В целях минимизации рисков, связанных с использованием неавторизованного и потенциально вредоносного программного обеспечения, настоятельно рекомендуется внедрить и последовательно применять на всех рабочих станциях и серверах Заказчика реестр разрешённого программного обеспечения (Allowlist / White List). Использование исключительно верифицированного и официально разрешённого ПО из утверждённого реестра существенно сокращает поверхность атаки, исключает возможность несанкционированной установки стороннего программного обеспечения пользователями и снижает вероятность проникновения вредоносных программ под видом легитимных приложений. Контроль соответствия установленного ПО реестру разрешённых программ рекомендуется осуществлять на постоянной основе средствами EDR и политиками групповых объектов (GPO) с фиксацией выявленных отклонений в SIEM-системе для последующего анализа аналитиками Поставщика.

7) Мониторинг и реагирование на инциденты информационной безопасности необходимо поддерживать в строгом соответствии с требованиями действующих нормативных документов Республики Казахстан, в том числе Постановления Правительства № 832 от 20 декабря 2016 года и Приказа Министра оборонной и аэрокосмической промышленности № 52-НҚ от 28 марта 2018 года. Соблюдение установленных регламентов обеспечивает не только надлежащий уровень защищённости, но и готовность Заказчика к прохождению контрольных проверок со стороны уполномоченных органов.