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

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

Акимат города Алматы

Отчетный период: 01.01.2026 – 31.01.2026 г.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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 8
4. МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 11
4.1. Статистика событий безопасности 11
4.2. Система уведомлений 15
4.3 Поиск угроз 15
4.4. Доступность веб-интерфейса 17
4.5. Автоматическое реагирование на угрозы 17
5. АНАЛИЗ УЯЗВИМОСТЕЙ 18
5.1 Инструментальное сканирование 18
5.2 Статистика управления уязвимости 20
6. ПЛАТФОРМА АНАЛИЗА УГРОЗ И ЗАЩИТА ОТ ТАРГЕТИРОВАННЫХ АТАК 22
6.1. OpenCTI — Платформа киберразведки 22
6.2. MISP — Обмен индикаторами компрометации 23
6.3. T-Lab Sandbox — Защита от таргетированных атак 24
6.4. DLP – Предотвращение утечек данных (safetica) 25
6.4.1. Анализ веб – активности 26
6.4.2. Передачи данных 27
6.4.3. Служебные операции через интернет и внутренние сервисы 28
6.5 Checkpoint - межсетевой экран 30
7. РЕАЛИЗОВАННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 34
8. ВЫВОДЫ И РЕКОМЕНДАЦИИ 37
8.1. Общие выводы 37
8.2. Приоритетные планы работ 37
8.3. Рекомендации 38

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

1. ОБЩАЯ ИНФОРМАЦИЯ

Настоящий отчет представляет результаты оказания услуг по обеспечению информационной безопасности для Акимата города Алматы (далее - Заказчик) за отчетный период 01.01.2026 – 31.01.2026 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 (январь 2026 года) в рамках сопровождения и эксплуатации системы информационной безопасности достигнуты следующие ключевые результаты:

- Обеспечена 100% работоспособность агентов информационной безопасности (EDR, DLP, Sysmon) на рабочих станциях и серверах Заказчика; выполнен ручной обход и восстановление агентов на **7** рабочих станциях, функционирующих под управлением Windows 11 Home;
- SIEM-системой зарегистрировано **2 564** 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;
- В ходе Threat Hunting выявлена вредоносная активность на рабочей станции *nauz-pc-0001*; хост изолирован средствами EDR, проводится углублённый анализ;
- Проведён анализ сетевой активности: зафиксировано **3 671** уникальный IP-адрес источников и **190 995** IP-адресов назначения; характер сетевого взаимодействия соответствует штатной модели работы инфраструктуры;
- 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;

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

- 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: выявлено **12** угроз и **12** подозрительных объектов при проверке **214** файлов; все угрозы нейтрализованы;
- В рамках эксплуатации NGFW Check Point зафиксировано и обработано:
  - **65 017** Anti-Bot-событий;
  - **44 398** Anti-Virus-срабатываний;
  - **1 715** 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 01.01.2026 – 31.01.2026 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.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

2.2. Область действия

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

- Аппарат акима города;
- **15** 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.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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 январе 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. В рамках проведённых работ из **7** рабочих станций, включённых в план, все устройства были успешно обработаны. По итогам выполнения мероприятий работоспособность EDR-агентов восстановлена в полном объёме, агенты функционируют в штатном режиме, замечания и отклонения устранены.

Рисунок 1. Агенты

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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 каждого типа агента составляет 100%, что подтверждает корректность внедрения и стабильность функционирования средств защиты.

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.

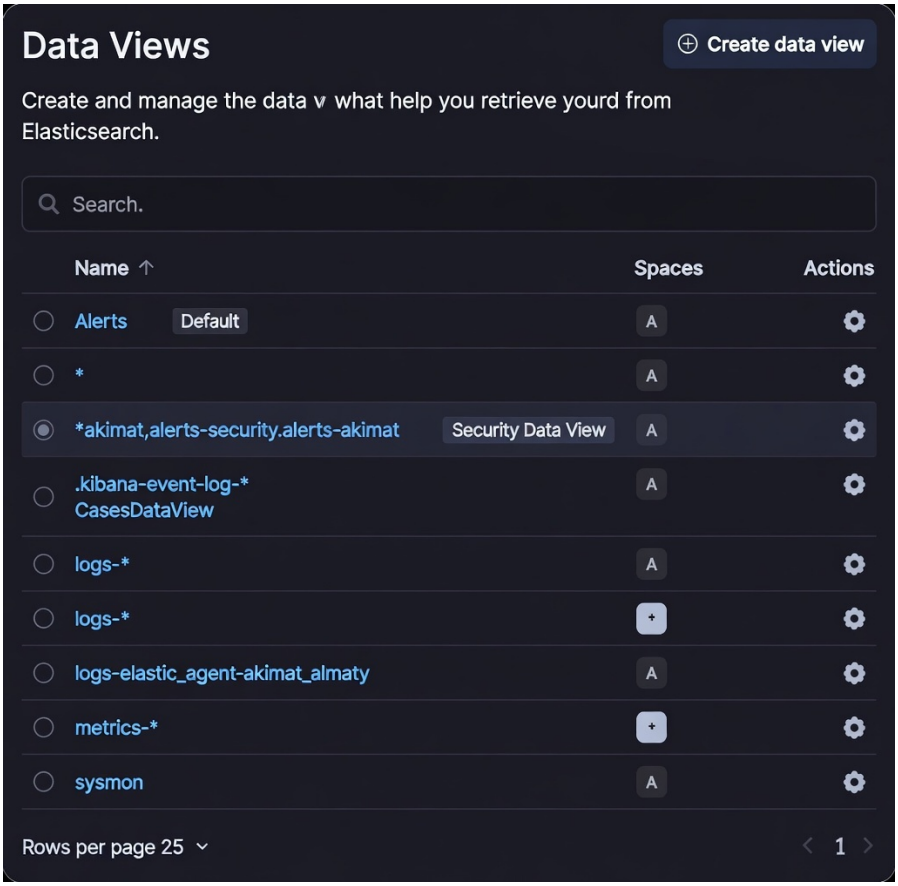


Рисунок 2. Data views

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000018034CB92E1

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 **2 564** срабатывания корреляционных и поведенческих правил безопасности. Наибольшее количество событий связано с попытками подбора привилегированных учётных записей (Privileged Account Brute Force – 827 событий), а также с подозрительной загрузкой библиотек (Potential Library Load via ROP Gadgets – 354 события) и подключением ранее не использовавшихся съёмных носителей (First Time Seen Removable Device — 259 событий). Подробная информация в таблице 2.

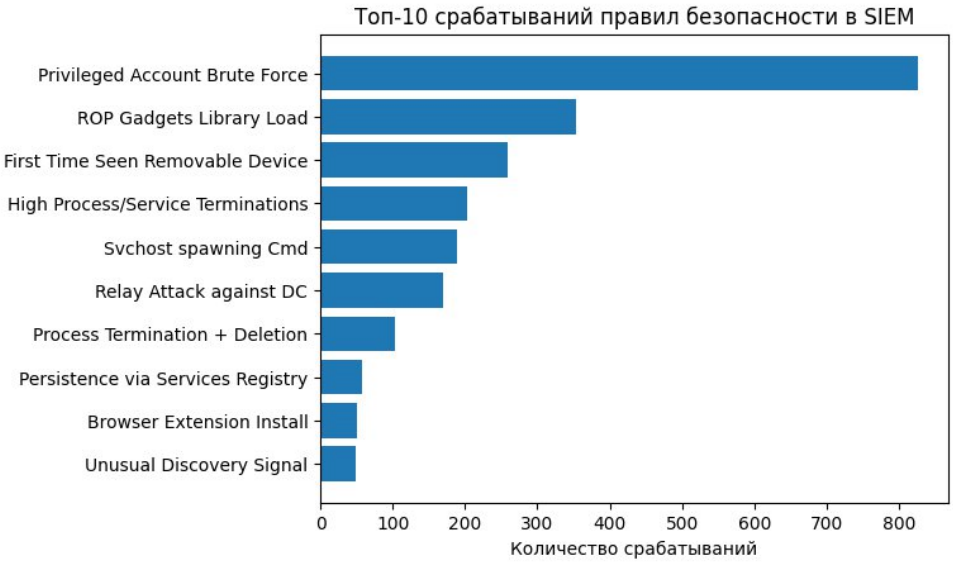


Рисунок 3. Статистика сработанных правил

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 корреляция

№	Наименование правила	Количество срабатываний
1	Privileged Account Brute Force	827

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000018034CB92E1

№	Наименование правила	Количество срабатываний
2	Malicious Behavior Detection Alert: Potential Library Load via ROP Gadgets	354
3	First Time Seen Removable Device	259
4	High Number of Process and/or Service Terminations	203
5	Svchost spawning Cmd	189
6	Potential Relay Attack against a Domain Controller	170
7	Process Termination followed by Deletion	103
8	Unusual Persistence via Services Registry	57
9	Browser Extension Install	51
10	Unusual Discovery Signal Alert with Unusual Process Command Line	49

Примечание: Полная таблица обработанных парвил 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 смотреть рисунок 4.

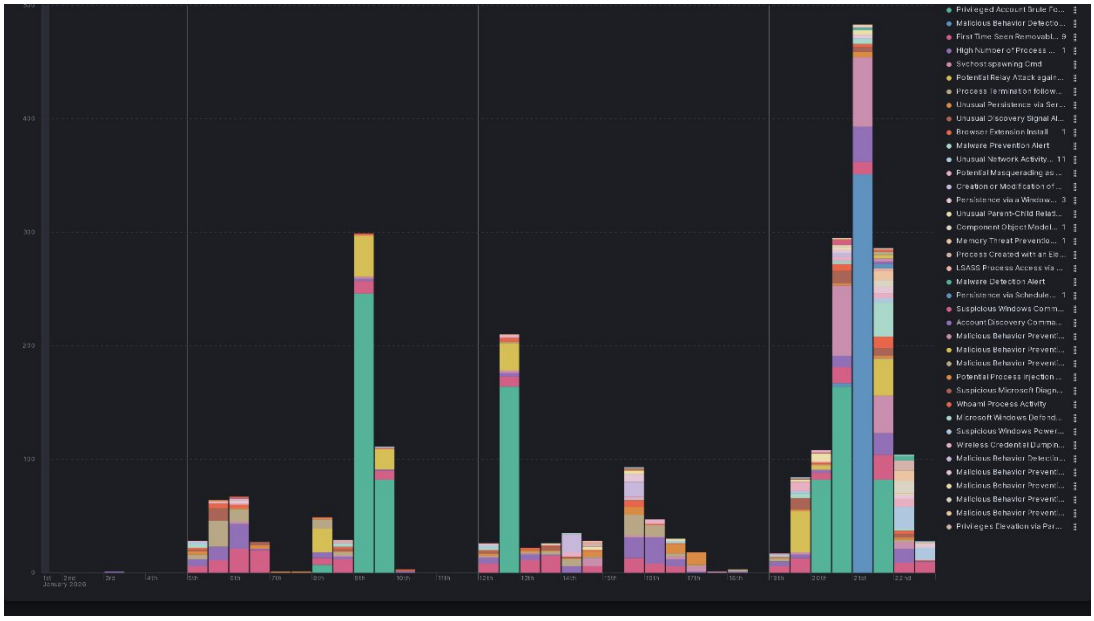


Рисунок 4. распределение срабатываний корреляционных правил

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

Проведён 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.

В рамках анализа сетевой активности за отчётный период зафиксировано **3 671** уникальный IP-адрес источников и **190 995** уникальных IP-адресов назначения, что соответствует типовой модели взаимодействия рабочих станций и серверных ресурсов с внешними сетевыми сервисами. Динамика сетевой активности носила контролируемый и предсказуемый характер, признаков массовых распределённых атак или аномальных отклонений не выявлено.

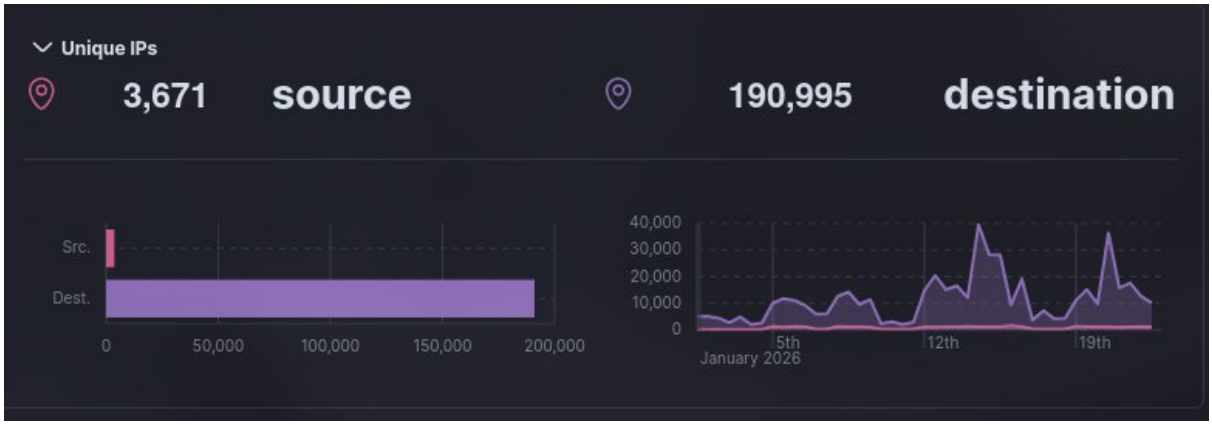


Рисунок 5. Сетевая активность

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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 **2564 событий (alerts)** различного уровня критичности.

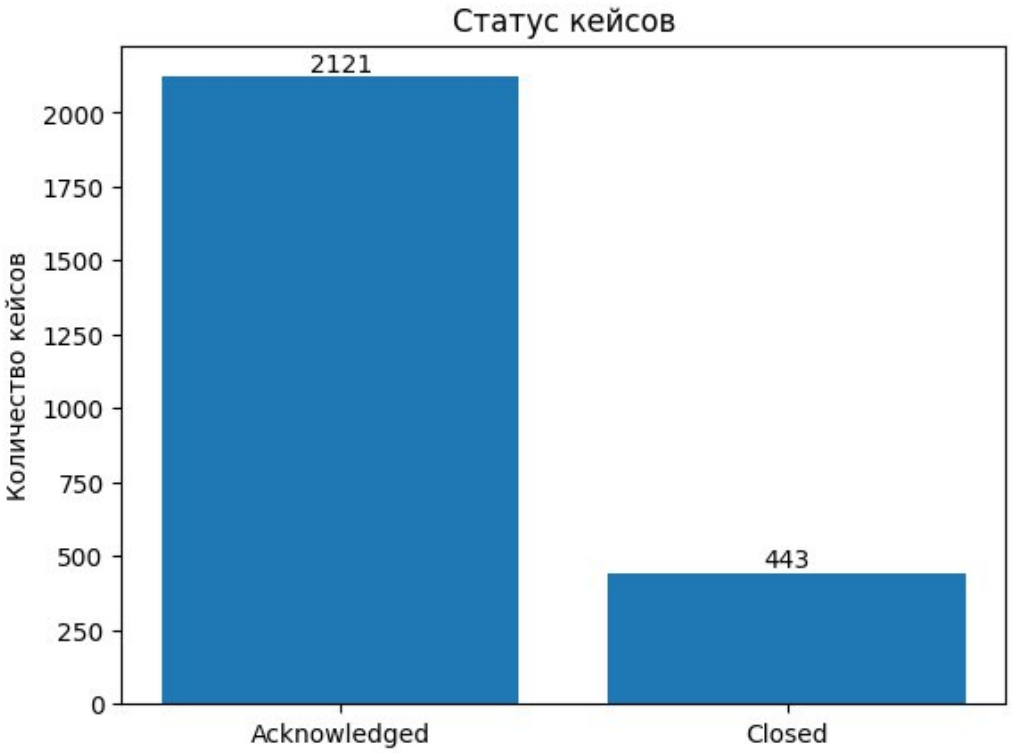


Таблица 6. Статус по кейсам

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, однако на одним их хосте акимата Наурызбаевского района зафиксирован подозрение на

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

инцидент информационной безопасности, подробнее в разделе *4.3 Поиск Угроз*, который на текущий момент анализируется.

Таблица 2. Статус закрытых кейсов

№	Дата и время	Сработанные правила	хост	Статус закрытых кейсов
1	2026-01-03T05:16:06.605Z	High Number of Process and/or Service Terminations		closed
2	2026-01-05T03:36:30.508Z	High Number of Process and/or Service Terminations		closed
3	2026-01-05T03:37:22.872Z	Process Termination followed by Deletion	akmt-pc-0094	closed
4	2026-01-05T03:42:22.977Z	Process Termination followed by Deletion	desktop-8nin8ok	closed
5	2026-01-05T03:46:32.640Z	High Number of Process and/or Service Terminations		closed
6	2026-01-05T03:56:35.889Z	High Number of Process and/or Service Terminations		closed
7	2026-01-05T03:57:28.208Z	Process Termination followed by Deletion	desktop-5sbgtc2	closed
8	2026-01-05T04:0	High Number of Process and/or Service Terminations		closed

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000018034CB92E1

№	Дата и время	Сработанные правила	хост	Статус закрытых кейсов
	1:37.171 Z			
9	2026-01-05T04:53:47.954 Z	First Time Seen Removable Device	desktop-co6fs19	closed

Примечание: Полная таблица закрытых кейсов представлена в Приложении 2.

За отчётный период аналитиками зафиксировано распределение событий информационной безопасности по рабочим станциям, при котором на ТОР-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.

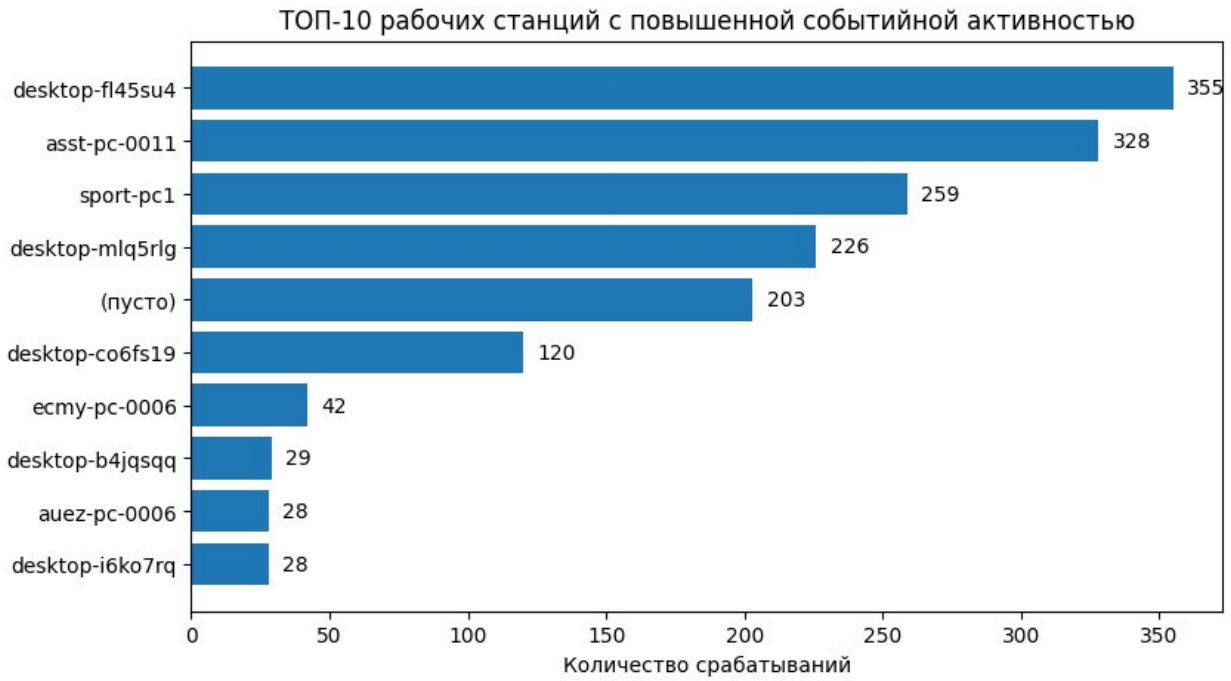


Рисунок 7. Топ 10 рабочих станций с повышеннной активностью

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000018034CB92E1

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.

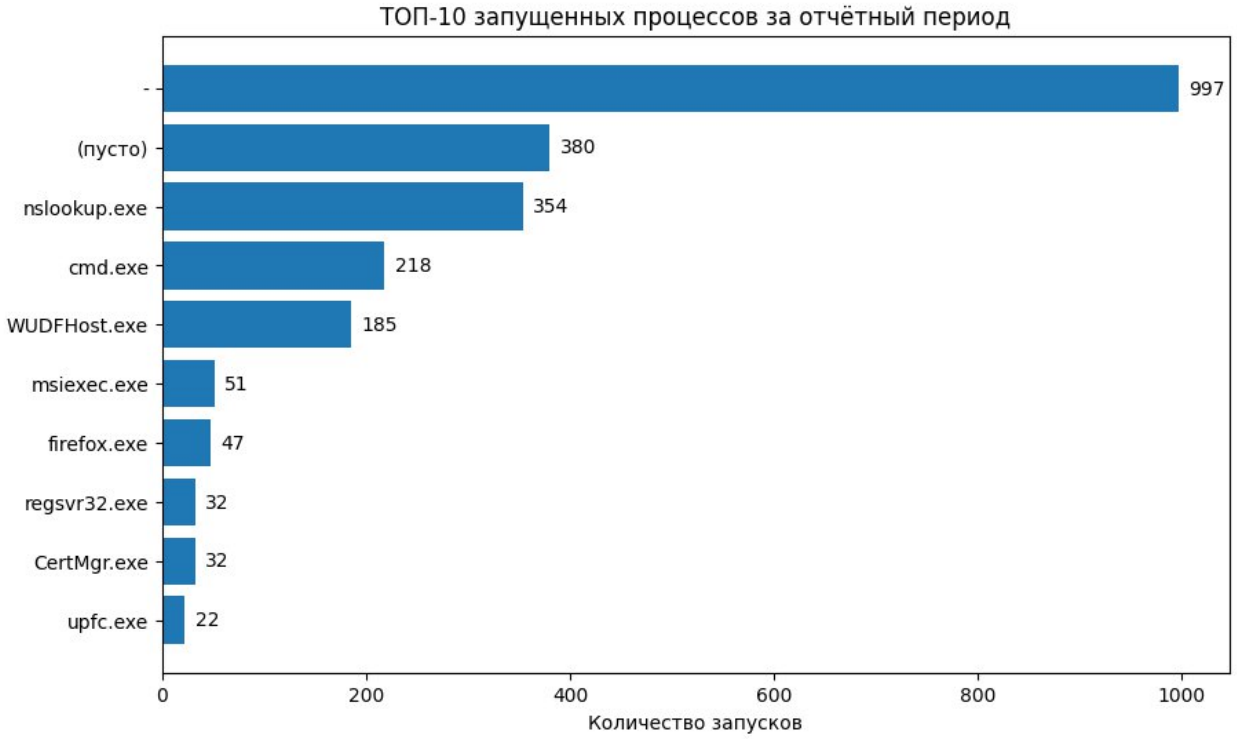


Рисунок 8. Топ-10 запущенных процессов

В таблице 4 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.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

Таблица 4. Обработанные процессы

№	запущенные процессы	количество
1	-	997
2	(пусто)	380
3	nslookup.exe	354
4	cmd.exe	218
5	WUDFHost.exe	185
6	msiexec.exe	51
7	firefox.exe	47
8	regsvr32.exe	32
9	CertMgr.Exe	32
10	upfc.exe	22

Примечание: Полная таблица обработанных процессов описаны в Приложении 3.

4.2. Система уведомлений

В рамках сопровождения и реагирования на инциденты информационной безопасности Поставщиком осуществляется оперативное информирование специалистов Заказчика о каждом выявленном инциденте и необходимых действиях.

За отчётный период Заказчику направлено **3** уведомлений о зафиксированных инцидентах, по каждому из которых аналитиками Поставщика были выполнены мероприятия по реагированию и инциденты были устранены.

4.3 Поиск угроз

В рамках мероприятий по поиску угроз (Threat Hunting) была выявлена и проанализирована вредоносная активность на рабочей станции nauz-pc-0001.

Рисунок 9. Процесс реагирования по результату поиска угроз

В ходе проактивного анализа поведенческих и корреляционных признаков зафиксировано выполнение исполняемого файла, замаскированного под системный объект с расширением *.scr*, сопровождавшееся массовым самокопированием в общие каталоги Windows (C:\Users\Public*). Затронутые процессы:

DOC ID KZBW2Z12026000018034CB92E1
DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

C:\Users\Public\Public.exe C:\Users\Admин\Desktop\Новая папка\папка.scr C:\Users\Public\zzAntiRansomElastic-DO-NOT-TOUCH-def6d40c-a6a1-442c-adc4-9d57a47e58d7\zzAntiRansomElastic-DO-NOT-TOUCH-def6d40c-a6a1-442c-adc4-9d57a47e58d7.scr C:\Users\Public\Pictures\Pictures.exe C:\Users\Public\Videos\Videos.pif C:\Users\Public\Libraries\Libraries.pif C:\Users\Public\Downloads\Downloads.exe C:\Users\Public\Documents\Documents.exe C:\Users\Public\AccountPictures\AccountPictures.exe C:\Users\Public\aaAntiRansomElastic-DO-NOT-TOUCH-def6d40c-a6a1-442c-adc4-9d57a47e58d7\aaAntiRansomElastic-DO-NOT-TOUCH-def6d40c-a6a1-442c-adc4-9d57a47e58d7.scr

Анализ хэш -суммы

6c345dea1d61144d64f51ec14f9a4ec172ffcde7e59a53a780a7416128c28e3b

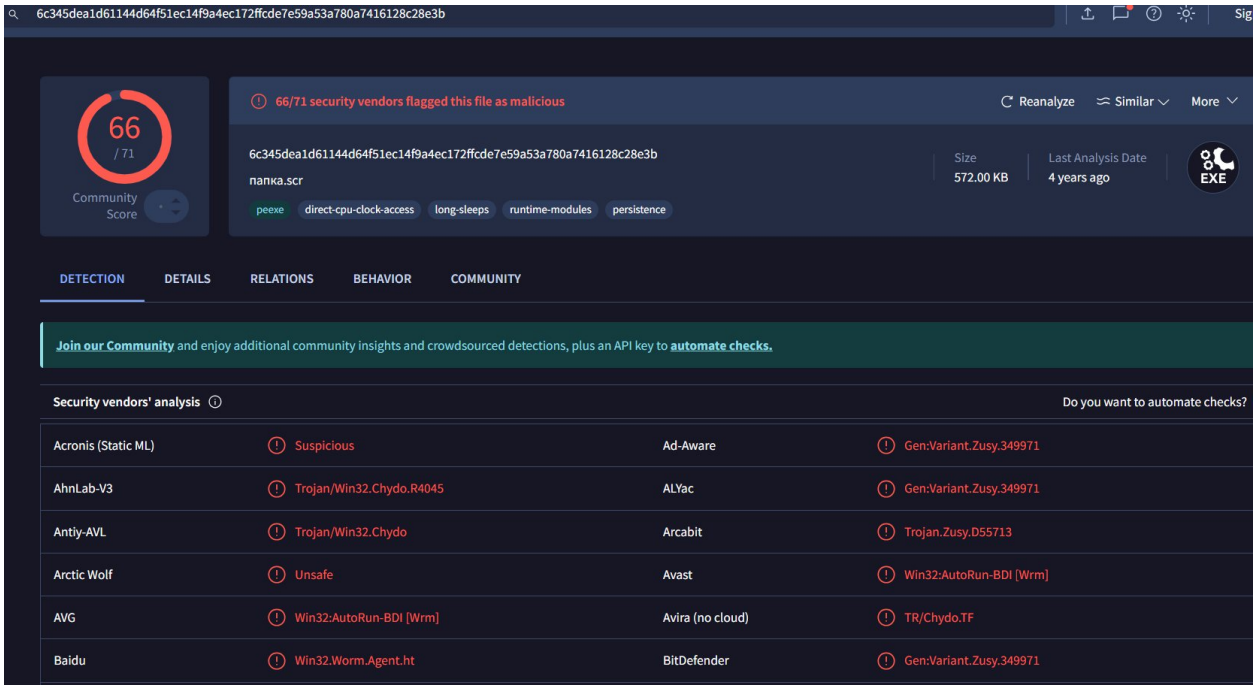


Рисунок 10.Анализ посредством вирус-тотал

По совокупности обнаруженных индикаторов, включая обращение к защитным ловушкам Anti-Ransomware, активность была классифицирована как вредоносная, после чего средствами EDR выполнены блокировка и изоляция хоста, в настоящее время проводится форензический анализ снятого образа с хоста nauz-pc-0001 с целью выявления активности злоумышленника или вредоносного программного обеспечение.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

4.4. Доступность веб-интерфейса

В ходе анализа выявлен публично доступный веб-интерфейс почты Акимата города Алматы (Roundcube) на домене *a-a.kz*, доступный из сети Интернет и использующий устаревшую версию ПО **Roundcube 1.6.9**.

Рисунок 11. Потенциальные риски

Сервис экспонирует почтовые и DNS-порты, что увеличивает риск атаки. Обнаруженная версия подпадает под ряд публично известных уязвимостей, включая риски выполнения кода, XSS и утечки данных, которые могут быть реализованы при компрометации учетной записи пользователя. Потенциальные последствия включают доступ к переписке, рассылку писем от имени сотрудников и использование почтового сервера как точки входа для дальнейших атак. Для снижения рисков рекомендуется в кратчайшие сроки ограничить внешний доступ, обновить Roundcube до актуального security-релиза (не ниже 1.6.12) и провести анализ журналов безопасности.

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.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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.

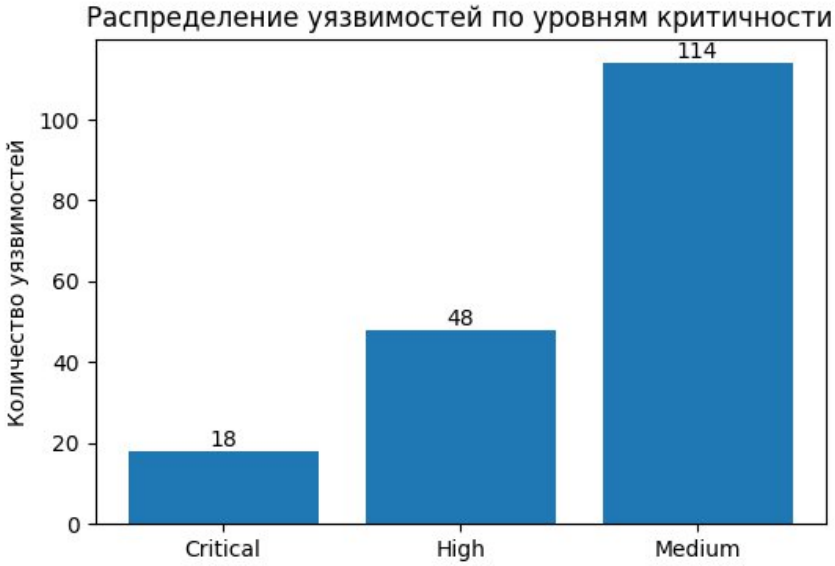


Рисунок 12. Уровень критичности

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.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

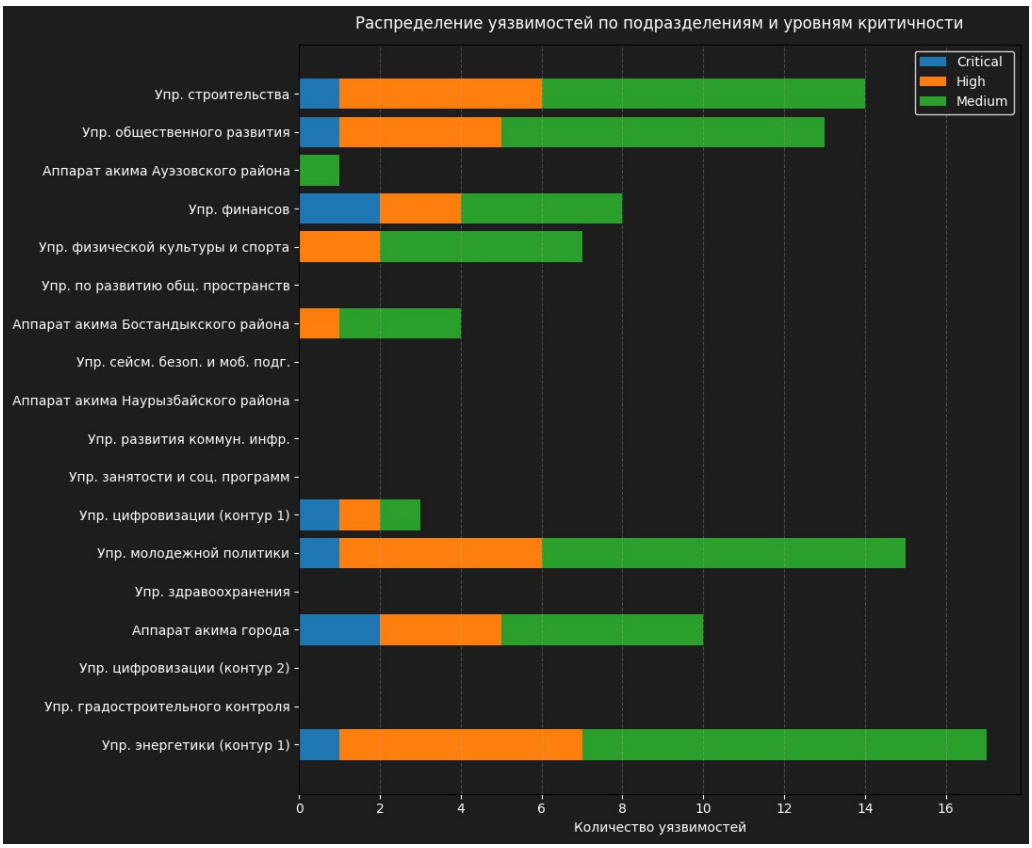


Рисунок 13. Распределение уязвимости по подразделениям

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 5. Сканирование сети

№	Подразделение (объект сканирования)	Critical	High	Medium
1	Аппарат акима города Алматы	2	3	5
2	Аппарат акима Алатауского района	0	0	0
3	Аппарат акима Ауэзовского района	0	0	1
4	Аппарат акима Бостандыкского района	0	1	3
5	Аппарат акима Жетысуского района	2	1	6

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

6	Аппарат акима Медеуского района	0	0	0
7	Аппарат акима Наурызбайского района	0	0	0
8	Аппарат акима Турксибского района	0	0	0
9	Аппарат заместителей руководителя	2	1	3
10	Серверная сеть Заказчика	0	2	8

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

По результатам сканирования уведомления были направлены на адреса электронной почты в октябре: b.kadyrov@a-a.kz, data@a-a.kz, a.dandibay@a-a.kz с детальным описанием выявленных уязвимостей и рекомендациями по их устранению.

5.2 Статистика управления уязвимости

Диаграмма отражает сравнение количества выявленных уязвимостей по уровням критичности между текущим и предыдущим запусками сканирования. Текущий запуск выполнен 21.01.2026 в 13:02:10, предыдущий — 21.01.2026 в 12:33:17; источником данных для сравнения использовано состояние предыдущего запуска, зафиксированное в файле *vm_state.json*. Значимых изменений в распределении уязвимостей уровней *Critical*, *High* и *Medium* не зафиксировано, что свидетельствует о стабильности состояния защищённости инфраструктуры и контролируемом уровне рисков.

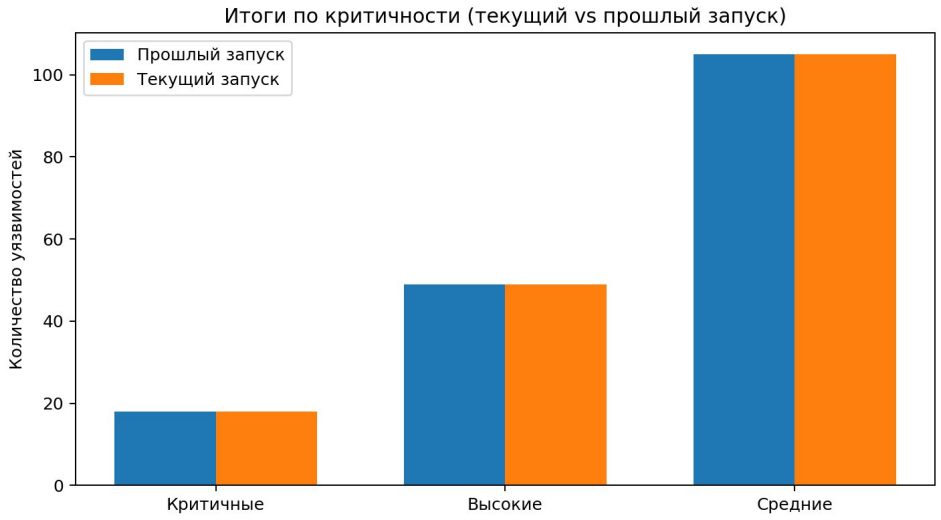


Рисунок 14. Итоги критичности

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000018034CB92E1

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

Таблица 6. Статистика управление уязвимости

Скан	СЕЙЧАС К/В/С	БЫЛО К/В/С	ΔК/ΔВ/ΔС	Новые	Устранены	Без изм.	Крит.↑	Крит.↓	ΔХостов
Аппарат Акима	2/3/5	2/3/5	+0/+0/+0	0	0	10	0	0	+0
Аппарат Алатауского района	0/0/0	0/0/0	+0/+0/+0	0	0	0	0	0	+0
Аппарат Ауэзовского района	0/0/1	0/0/1	+0/+0/+0	0	0	1	0	0	+0
Аппарат Бостандыкского район	0/1/3	0/1/3	+0/+0/+0	0	0	4	0	0	+0
Аппарат Жетысуского района	2/1/6	2/1/6	+0/+0/+0	0	0	9	0	0	+0
Аппарат Медеуского района	0/0/0	0/0/0	+0/+0/+0	0	0	0	0	0	+0
Аппарат Наурызбайского района	0/0/0	0/0/0	+0/+0/+0	0	0	0	0	0	+0
Аппарат Турксибского района	0/0/0	0/0/0	+0/+0/+0	0	0	0	0	0	+0

Примечание: Подробная таблица по статистике управление уязвимости описаны в Приложении 8

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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.

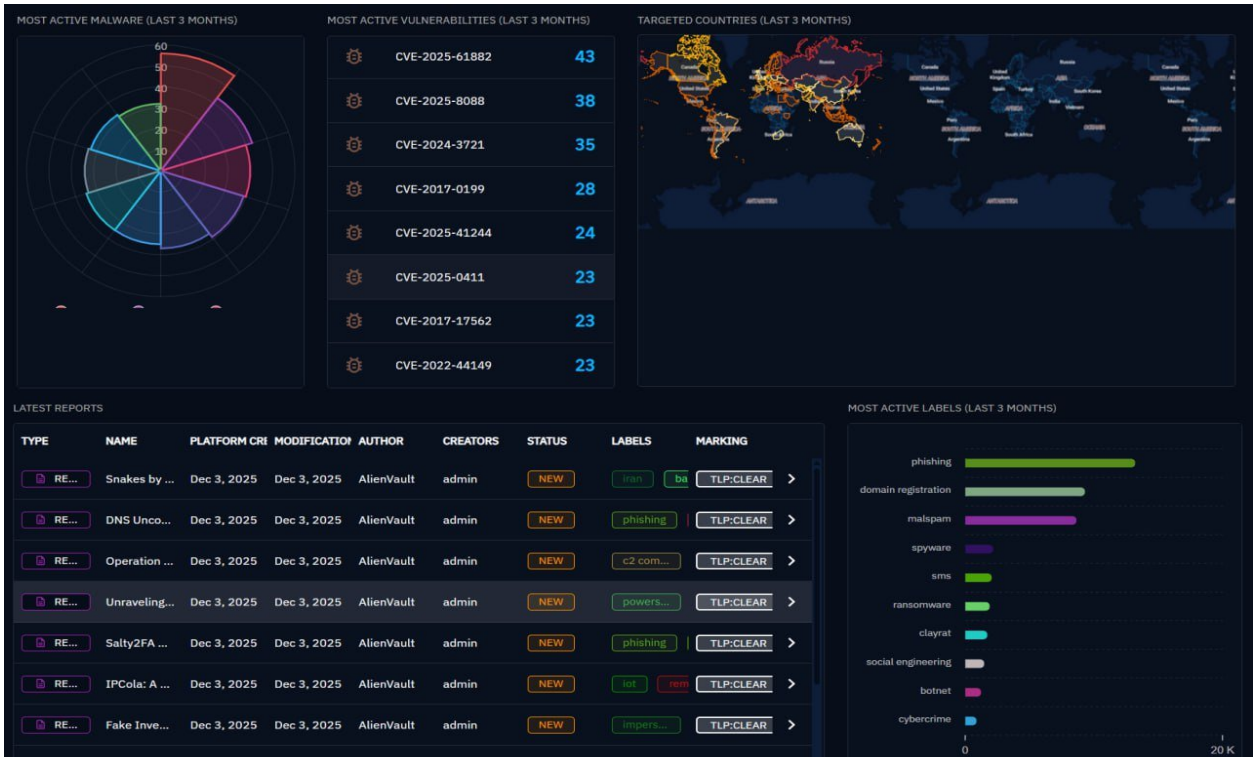


Рисунок 15. OpenCTI

Актуализация базы IoC в OpenCTI позволяет повысить эффективность мониторинга, сократить время реагирования на повторяющиеся и схожие

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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.

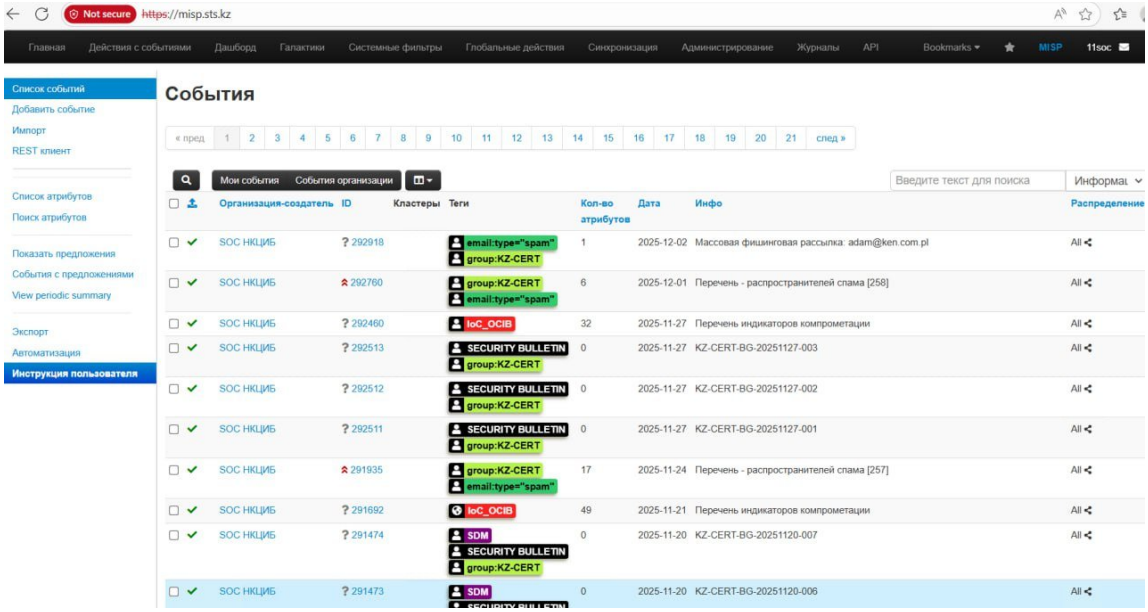


Рисунок 16. MISP

DOC ID KZBW2Z12026000018034CB92E1
DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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 система анализа угроз в режиме реального времени выявила **12 угроз и 12 подозрительных объектов**, при общем количестве **214 проверенных файлов/объектов**. Активность носила эпизодический характер и была сосредоточена в отдельные временные интервалы. Основную долю проверяемых объектов составили текстовые и исполняемые файлы. По результатам анализа все выявленные угрозы были обработаны средствами защиты, признаков массового заражения или распространения вредоносного программного обеспечения не зафиксировано.

Рисунок 17. Статистика заблокированных ВПО

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.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

Таблица 7. IOC

№	Тип индикатора	Значение (SHA-256)
1	File Hash (SHA-256)	8ee73db4e73f18913dc142c600145b2a7c4de007df55fab582318a882c2d5c02
2	File Hash (SHA-256)	0ed3cead9d59256a1f61dac12cd54255f5e7d6f360a2128167b16464b6b0ce43
3	File Hash (SHA-256)	e871549263d3f6a683e822535675830ab7737be37470bd948ee1858a9cdfab03
4	File Hash (SHA-256)	b7b7fc9fa8a002d4a0a9355470723a32fdf6d4d0e982ecdf32b17bd1bfaf4112
5	File Hash (SHA-256)	2ea1ed3a29ad5ffbe19f3c11fda18d6c8ee4c18c3a2c5971a7ace7b73bd91e22
6	File Hash (SHA-256)	d83d86ed5bfdb2bd795ff757231138d3c738b63e2bcea06085deeb4ac60d6
7	File Hash (SHA-256)	438ec817058a62042b0175326b12275c1b984dd97b607396a8ae24c692bb4616
8	File Hash (SHA-256)	1350480eebb363d006b785beb42e48e6b5fe723af0d1afbb9fe1e1c5400a9c3c
9	File Hash (SHA-256)	2348a3fe45c575cb033e3066143a8a1c457e850594fe766bdecf03f1e6c55318
10	File Hash (SHA-256)	f739669992c4a33919d143fb279ca5fd2c506528df5fbe7edd1f0af58a2b28e4

Примечание: Смотреть подробный отчет T-Lab в Приложении 9

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.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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

Примечание: Подробный отчет DLP в Приложении 10

6.4.1. Анализ веб – активности

В отчётном периоде **с 1 по 31 января 2026 года** проведён анализ веб-активности пользователей в инфраструктуре Заказчика. Зафиксирован доступ к **5 502 проверенным веб-сайтам**, при этом **4 230 ресурсов** отнесены к неклассифицированным и подлежат дополнительному анализу. Обращений к запрещённым или явно вредоносным сайтам не выявлено, блокировки не применялись.

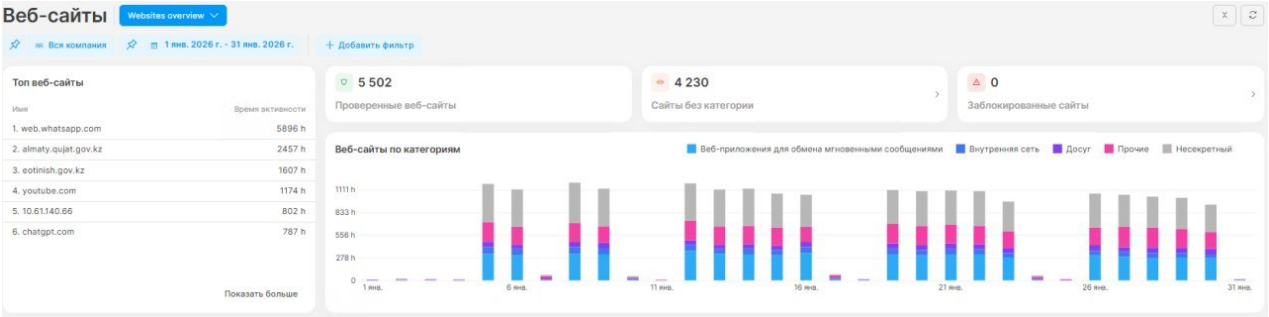
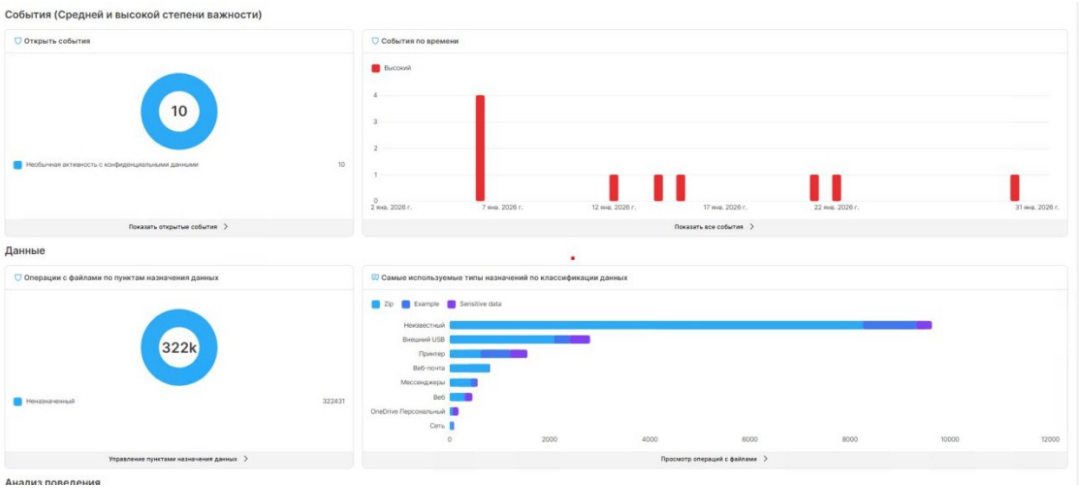


Рисунок 18. Веб-сайты

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.



DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000018034CB92E1

Рисунок 19. Средний и высокий степень важности

6.4.2. Передачи данных

Диаграмма «Топ-10 приложений по объёму переданных данных» отражает распределение сетевого трафика между наиболее активно используемыми пользовательскими и системными приложениями за отчётный период. Наибольший объём трафика сформирован процессом *explorer.exe* (≈1,3 ТБ), что обусловлено активной работой пользователей с файловой системой и сетевыми ресурсами. Существенную долю также занимают веб-браузеры (*Google Chrome*, *Microsoft Edge*, *Firefox*) и офисные приложения (*Microsoft Word*, *Excel*, *PowerPoint*), что соответствует повседневной рабочей активности. Использование архиваторов и PDF-просмотрщиков (*WinRAR*, *Adobe Acrobat*) связано с обработкой и передачей документов. В целом распределение трафика носит легитимный характер и соответствует функциональным задачам пользователей, признаков аномальной или вредоносной активности не выявлено.

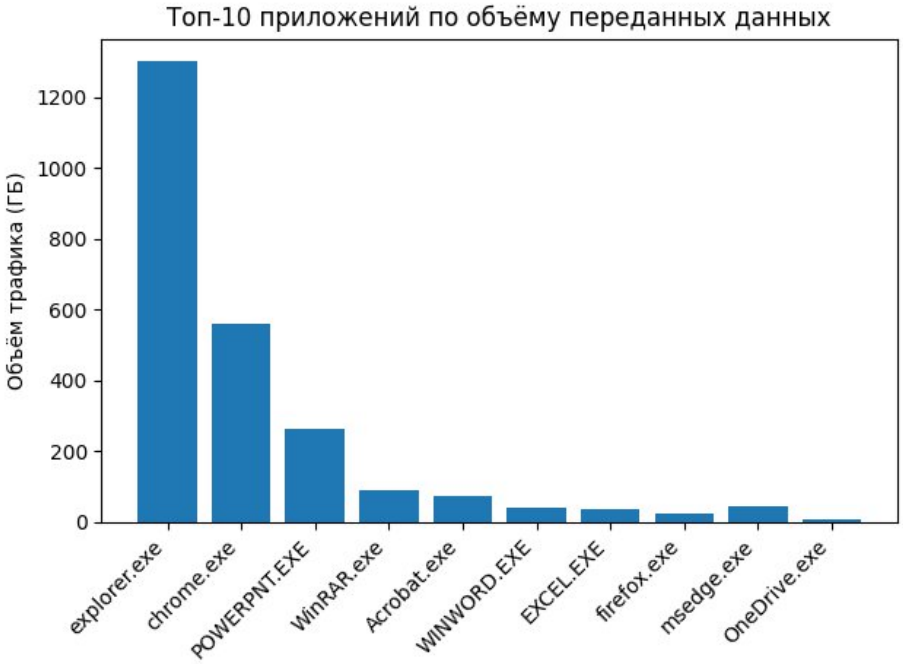


Рисунок 20. Топ-10 приложений

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000018034CB92E1

Таблица 8 отражает распределение активности по основным пользовательским и системным приложениям за отчётный период.

Таблица 8. Распределение активности по основным пользовательским и системным приложениям

№	Приложение	Количество операций	Объём переданных данных
1	Проводник Windows (explorer.exe)	444 097	1,3 ТБ
2	Microsoft Word (WINWORD.EXE)	119 605	38,8 ГБ
3	Google Chrome (chrome.exe)	113 381	559,5 ГБ.
4	Microsoft Excel (EXCEL.EXE)	45 949	34 ГБ
5	Mozilla Firefox (firefox.exe)	15 397	24,3 ГБ
6	Adobe Acrobat (Acrobat.exe)	13 111	47,5 ГБ
7	Microsoft PowerPoint (POWERPNT.EXE)	9 346	261,9 ГБ
8	Microsoft Edge (msedge.exe)	8 840	43,4 ГБ
9	WinRAR (WinRAR.exe)	8 756	90,4 ГБ
10	Canon PageComposer Despooler (CPC10D.EXE)	5 932	0 Б

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 подразделений **энергетики** и **УОР**, что обусловлено спецификой выполняемых служебных задач. В целом характер интернет-активности пользователей носит рабочий и равномерный характер, отклонений и аномального поведения не выявлено.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

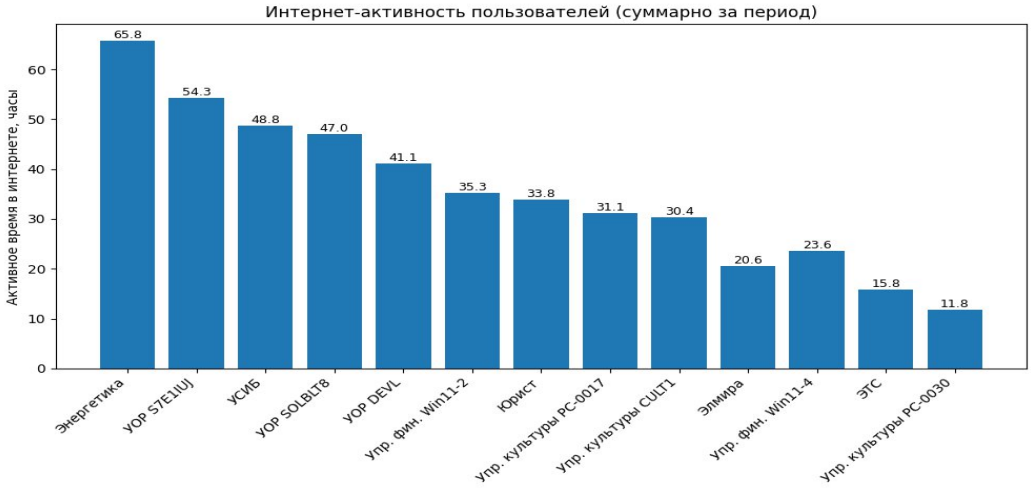


Рисунок 21. Время нахождения пользователя в сети

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 9. Сетевая активность пользователя

№	Пользователь	Кол-во сессий	Кол-во пользователей	Активное время (суммарно)	Среднее активное время в день
1	Юрист@Lawyer	85	1	33 ч 45 мин 48 с	1 ч 5 мин 20 с
2	ЭТС 1@BOST-PC0010	39	1	15 ч 47 мин 48 с	30 мин 34 с
3	Энергетика@DESKTOP-0DEUENJ	51	1	65 ч 49 мин 22 с	2 ч 7 мин 23 с
4	Элмира@DESKTOP-UPELIRI	24	1	20 ч 37 мин 4 с	39 мин 54 с
5	усиб@Economy11	33	1	48 ч 47 мин 2 с	1 ч 34 мин 25 с
6	Упр_культуры@CULT-PC-0030	11	1	11 ч 50 мин 29 с	22 мин 55 с

DOC ID KZBW2Z12026000018034CB92E1
DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

№	Пользователь	Кол-во сессий	Кол-во пользователей	Активное время (суммарно)	Среднее активное время в день
7	Упр_культуры@CULT-PC-0017	108	1	31 ч 6 мин 11 с	1 ч 0 мин 11 с
8	Упр_финансов@FINS-Win11-4	50	1	23 ч 36 мин 40 с	45 мин 41 с
9	Упр_финансов@FINS-Win11-2	47	1	35 ч 15 мин 55 с	1 ч 8 мин 15 с
10	Упр_финансов@FINS-PC-0006	5	1	45 мин 54 с	1 мин 28 с
11	Упр_культуры@DESKTOP-CULT1	45	1	30 ч 25 мин 18 с	58 мин 52 с
12	Упр_креативной@CNTR-PC-0003	4	1	5 мин 11 с	10 с
13	УОР@DEVL-PC-0031	23	1	41 ч 6 мин 48 с	1 ч 19 мин 34 с
14	УОР@DESKTOP-SOLBLT8	43	1	46 ч 57 мин 35 с	1 ч 30 мин 53 с
15	УОР@DESKTOP-S7E1IUJ	63	1	54 ч 18 мин 56 с	1 ч 45 мин 7 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.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

Таблица 10. Зафиксированный активность в Межсетевом экране

№	Категория	Показатель	Значение
1	**Общие события безопасности**	Anti-Bot события	**65 017**
		Anti-Virus события	**44 398**
		IPS-инциденты	**1 715**
		Threat Emulation	**0** (сканирование не выполнялось)
2	**Сетевой трафик**	Получено данных	**695 ГБ**
		Передано данных	**108 ГБ**
		Общий объём трафика	**795 ГБ**
3	**Инфицированные устройства**	Всего инфицированных	**10**
		High / Critical	**10**
		Скомпрометированные серверы	**0**
		Активные за последнюю неделю	**6**
4	**Приложения повышенного риска**	Всего сессий	**273 000**
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

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

Protocol (273 000 сессий, 532 МБ трафика), uTorrent, BitTorrent Sync, а также средств удалённого доступа и VPN-решений (AnyDesk, Thunder VPN, OpenVPN). Наибольшая нагрузка приходится на пиринговые протоколы обмена файлами, что указывает на их активное использование в инфраструктуре.

Таблица 11. Сетевая активность

№	Приложение	Сессии	Трафик
1	BitTorrent Protocol	**273 000**	**532 МБ**
2	uTorrent	4 100	3.03 МБ
3	AnyDesk	1 300	13.7 МБ
4	BitTorrent Sync	972	956 КБ
5	Thunder VPN	122	1.5 КБ
6	OpenVPN	11	15 КБ

Наибольшую долю выявленных событий информационной безопасности составили вредоносные объекты, характеризующиеся массовым копированием файлов, маскировкой под легитимные системные и пользовательские каталоги, а также попытками закрепления в системе и обхода защитных механизмов. Обнаруженные образцы, как правило, использовали распространённые форматы исполняемых файлов (.exe, .scr, .pif) и запускались из общедоступных директорий, что свидетельствует о типичных сценариях заражения пользовательских рабочих станций. Все выявленные вредоносные объекты были своевременно проанализированы и нейтрализованы аналитиками в рамках установленного процесса реагирования, распространение угроз предотвращено.

Таблица 12. Заблокированный ВПО

№	Вредоносное ПО	События
1	Trojan.Linux.RubyMiner.B	**133**
2	Download.TC.02dfHZlq	104
3	Phorpiex.TC.626cXRf	104
4	Download.TC.37105FkG	102
5	Download.TC.7852sIyB	102

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000018034CB92E1

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 13. Система предотвращения вторжений

№	Тип события	Сессии
1	Max Ping Size	1 100
2	Command Injection	299
3	TCP Segment Limit Enforcement	264
4	Directory Traversal	32
5	XSS Obfuscation	6
6	SQL Injection	5
7	Apache Log4j RCE	4

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

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 14. 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
4	**Система предотвращения**	Защита от утечек конфиденциальной	✓ Реализовано. Контроль почтовых,

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

№	Система	Назначение	Статус реализации
	утечек (DLP)	информации, контроль каналов передачи	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 информационной безопасности**	Централизованного учёта, обработки, классификации и управления инцидентами информационной	✓ Реализовано. Интеграция с SIEM, Nessus. Круглосуточный мониторинг, регистрация карточек инцидента

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

№	Система	Назначение	Статус реализации
		безопасности	информационной безопасности

Примечание: Полная таблица с описанием 17 систем представлена в Приложении 11

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000018034CB92E1

8. ВЫВОДЫ И РЕКОМЕНДАЦИИ

8.1. Общие выводы

1. По итогам мониторинга и анализа событий информационной безопасности за **январь 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. Продолжить анализ пользовательской и сетевой активности для своевременного выявления аномалий и потенциальных угроз
5. Расширять использование Threat Intelligence и платформы OpenCTI для проактивного выявления и предотвращения киберугроз.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

8.3. Рекомендации

1. Продолжить эксплуатацию внедренного комплекса средств защиты информации с регулярной актуализацией правил и политик безопасности.
2. Обеспечить контроль полноты и качества поступающих событий от всех источников (SIEM, EDR, DLP, Check Point, Sandbox).
3. Использовать результаты анализа IOC и данных T-Lab Sandbox для дальнейшего пополнения базы знаний угроз и механизмов корреляции.
4. Продолжить обучение пользователей основам информационной безопасности и безопасной работе с интернет-ресурсами.
5. Поддерживать процессы мониторинга и реагирования в соответствии с требованиями действующих нормативных документов Республики Казахстан, включая **Постановление №832** и **Приказ №52-НҚ**.

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z12026000018034CB92E1
Тип документа	Исходящее письмо
Тема	*Взамен ранее направленному исх.№66 от 05.02.26г. Отчет за январь 2026 года. пароль передан исполнителю
Статус	Доставлен
Рег. Номер:	01-01/53
Рег. Дата:	05.02.2026
Количество страниц	38
Подписи	2

Информация об отправителе

Отправитель	ТОО "MSSP.GL"
IP-адрес	109.163.197.162

Информация о получателях

Получатель 1	Управление цифровизации города Алматы, 042000249000, Казахстан

Информация о подписантах

Подписал(а)	САЛИПОВ ДАУРЕН
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
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWRQYJ...SJR0QpuQ=
Дата подписания	05.02.2026 16:36

Подписал(а)	САЛИПОВ ДАУРЕН
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
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWfQYJ...UNwMygA==

Дата подписания 05.02.2026 16:36

DOC ID KZBW2Z12026000018034CB92E1

DOC ID KZBW2Z12026000018034CB92E1
Электронный документ подписан в Documentolog Business