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

Акимат города Алматы

Отчетный период: 01.03.2026 – 31.03.2026 г.

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

Содержание

1. Общая информация 3
1.1. Ключевые показатели эффективности 3
2. Цель отчета 3
2.1. Область действия 3
3. Анализ системы мониторинга информационной безопасности 4
3.1. Состояние агентов 4
3.2 Настройка и актуализация представлений данных (Data Views) 4
3.3. Усиление мониторинга и анализа событий через SIEM-систему 5
4. Мониторинг и реагирование на инциденты информационной безопасности 6
4.1. Статистика событий безопасности 6
4.2. Система уведомлений 9
4.3 Поиск угроз 10
4.4. Доступность веб-интерфейса 10
4.5. Автоматическое реагирование на угрозы 10
5.1 Инструментальное сканирование 10
5.2 Статистика управления уязвимости 11
6.1. OpenCTI — Платформа киберразведки 13
6.2. MISP — Обмен индикаторами компрометации 14
6.3. T-Lab Sandbox — Защита от таргетированных атак 15
6.4. DLP – Предотвращение утечек данных (safetica) 17
6.4.1. Анализ веб – активности 17
6.4.2. Передачи данных 18
6.4.3. Служебные операции через интернет и внутренние сервисы 20
6.5 Checkpoint - межсетевой экран 22
7. Реализованные системы информационной безопасности 24
8. Выводы и рекомендации 24
8.1. Общие выводы 24
8.2. Приоритетные планы работ 25
8.3. Рекомендации 25

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

1. Общая информация

Настоящий отчет подготовлен в соответствии с пунктом 4.5 технической спецификации на услуги по обеспечению информационной безопасности и представляет результаты оказания услуг по обеспечению информационной безопасности для Акимата города Алматы (далее - Заказчик) за отчетный период 01.03.2026 – 31.03.2026 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 в SIEM зарегистрировано 9292 событий безопасности, по которым обработано 21 кейсов. Защита конечных точек обеспечивалась на 21 узлах, средствами EDR предотвращено 96 вредоносных действий. Через T-Lab Sandbox проверено 1879 файлов/объектов, выявлено 77 угроз. По результатам сканирования Nessus обнаружено 108 критических и 178 высоких уязвимостей. В системе Safetica зафиксировано 840367 DLP-событий. Средствами Check Point выполнено 26341892 блокировок.

2. 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.

2.1. 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).

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

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 отчётном периоде контроль состояния агентов EDR осуществлялся на 580 узлах, из которых защита была активна на 21 (3.62%). Выявлено 17 узлов с признаками некорректной работы агентов и 530 узлов, находившихся вне связи. Статусы агентов: healthy - 21, inactive - 17, offline - 530, unhealthy - 12. Наиболее затронутые хосты: nauz-pc-0004, fins-pc-0042, desktop-h2ajt7e. Под мониторингом находилось 580 узлов; offline - 530, нестабильных/требующих проверки - 17.

3.2 Настройка и актуализация представлений данных (Data Views)

Состояние источников данных и представлений в SIEM за отчётный период оценено как стабильное. В пространстве Elastic доступно 11 Data Views; ключевые представления: *case*, logs-elastic_agent-akimat_almaty, metrics-*, logs-windows.sysmon_operational-akimat, *akimat,.alerts-security.alerts-akimat*. В рамках мониторинга использовались правила корреляции, наиболее значимые из которых: *Privileged Account Brute Force, Malware Detection Alert, First Time Seen Removable Device*.

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

Рисунок 1. Data views

3.3. Усиление мониторинга и анализа событий через SIEM-систему

За отчётный период в системе мониторинга обработано 9292 событий безопасности, в том числе *critical - 1416, high - 673, medium - 3465, low - 3738*. Наиболее часто события фиксировались по правилам: *Privileged Account Brute Force, Malware Detection Alert, First Time Seen Removable Device*. Всего в отчётном периоде срабатывания пришлись на *45 правил, 558 хостов и 193 пользователей*. Наиболее затронутые хосты: *nauz-pc-0004, desktop-mlq5rlg, fins-pc-0042; пользователи: СИСТЕМА, administrator, LOCAL SERVICE*.

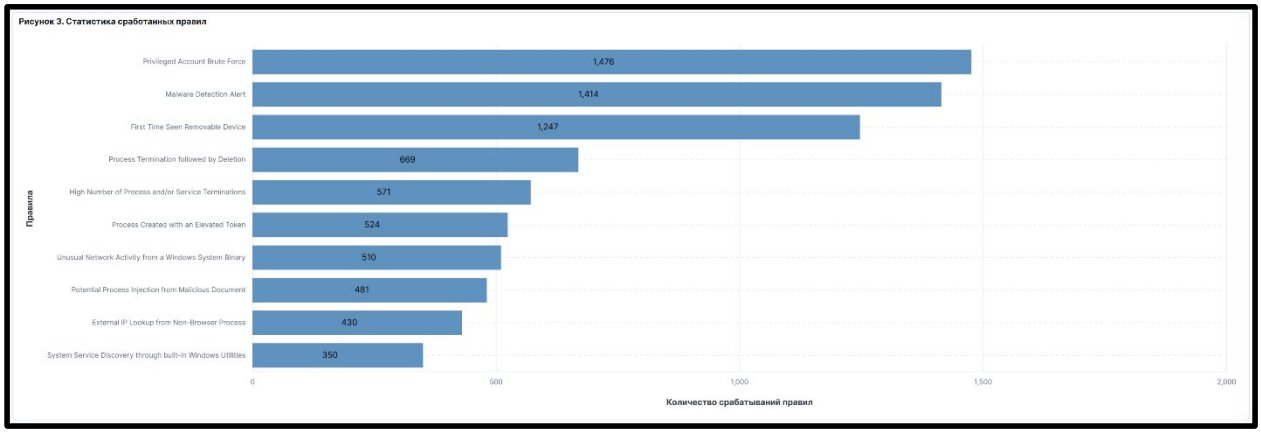

Рисунок 2. Статистика сработанных правил

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

На рисунке 3 отражено 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	1,476
Malware Detection Alert	1,414
First Time Seen Removable Device	1,247
Process Termination followed by Deletion	669
High Number of Process and/or Service Terminations	571
Process Created with an Elevated Token	524
Unusual Network Activity from a Windows System Binary	510
Potential Process Injection from Malicious Document	481
External IP Lookup from Non-Browser Process	430
System Service Discovery through built-in Windows Utilities	350

Рисунок 3. Правила корреляция

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. Подробнее смотрите рисунок 4.

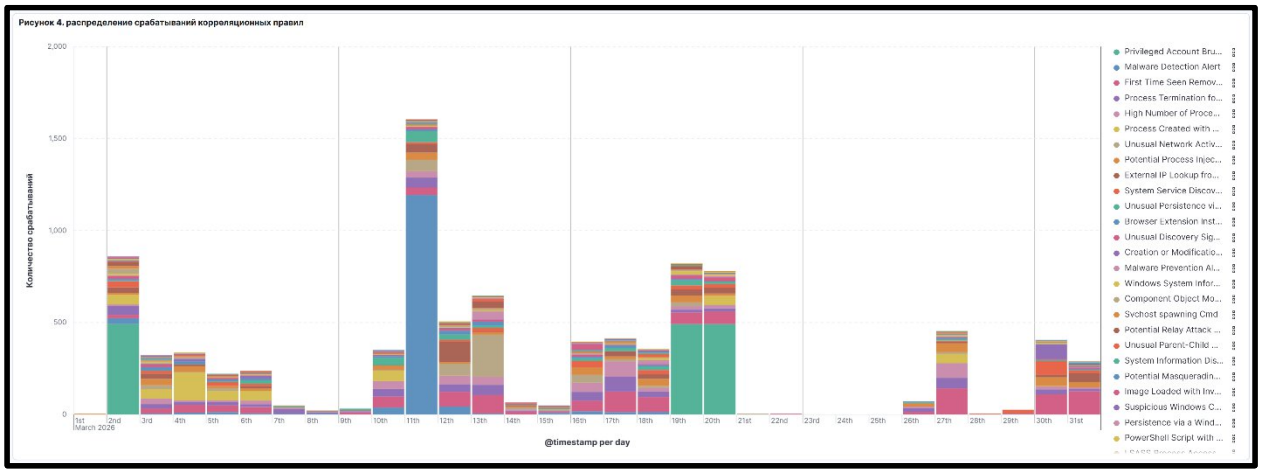

Рисунок 4. распределение срабатываний корреляционных правил

4. Мониторинг и реагирование на инциденты информационной безопасности

4.1. Статистика событий безопасности

В рамках мониторинга системы обнаружения и предотвращения угроз за отчётный период было зарегистрировано 9292 событий безопасности. Распределение по уровням критичности составило: critical - 1416, high - 673, medium - 3465, low - 3738. Наиболее заметная активность наблюдалась по правилам Privileged Account Brute Force, Malware Detection Alert, First Time

DOC ID KZBW2Z120260000018790AEE818
DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

Seen Removable Device, а также на узлах nauz-pc-0004, desktop-mlq5rlg, fins-pc-0042. Статусы кейсов за период: closed - 2, in-progress - 19.

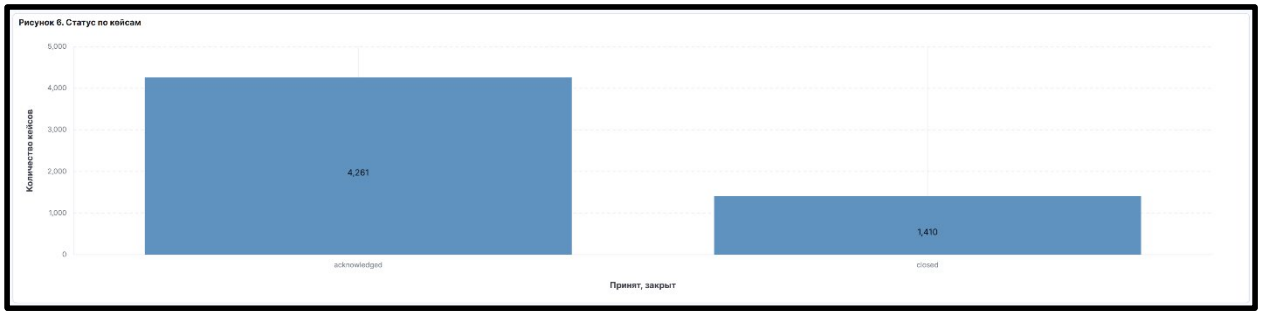

Рисунок 5. Статус по кейсам

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 2. Статус закрытых кейсов

Сработанные правила	Количество закрытых кейсов	Дата и время
High Number of Process and/or Service Terminations	563	Mar 2, 2026 @ 08:32:23.
First Time Seen Removable Device	435	Mar 2, 2026 @ 10:04:34.
Process Termination followed by Deletion	220	Mar 2, 2026 @ 08:47:58.
Unusual Persistence via Services Registry	78	Mar 2, 2026 @ 08:59:45.
Potential Relay Attack against a Domain Controller	24	Mar 2, 2026 @ 13:43:32.
Browser Extension Install	20	Mar 3, 2026 @ 19:19:42.
Unusual Discovery Signal Alert with Unusual Process Command Line	16	Mar 3, 2026 @ 16:30:14.
Svchost spawning Cmd	11	Mar 2, 2026 @ 08:27:15.

Рисунок 6. Статус закрытых кейсов

Примечание: Полная таблица закрытых кейсов представлена в Приложении 2.

За отчётный 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

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business
DOC ID KZBW2Z120260000018790AEE818

потенциально нежелательным программным обеспечением. Все выявленные события и случаи вредоносной активности своевременно анализируются и устраняются аналитиками в рамках установленного процесса мониторинга и реагирования.

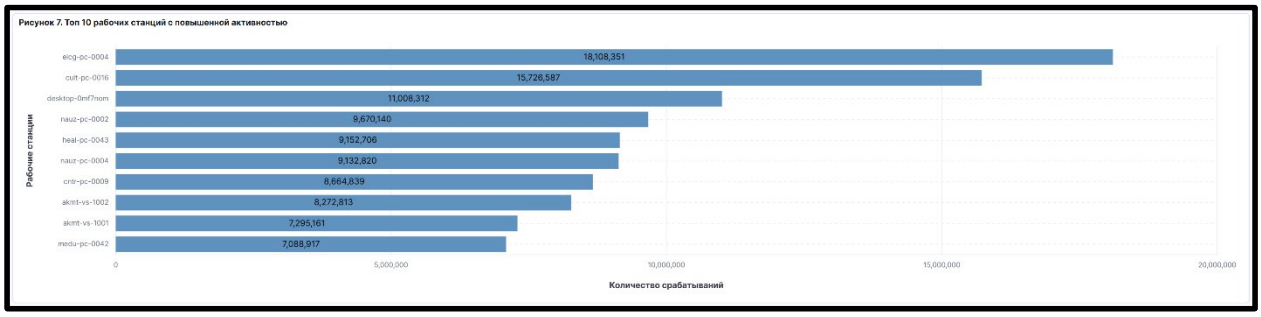

Рисунок 7. Топ 10 рабочих станций с повышенной активностью

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.

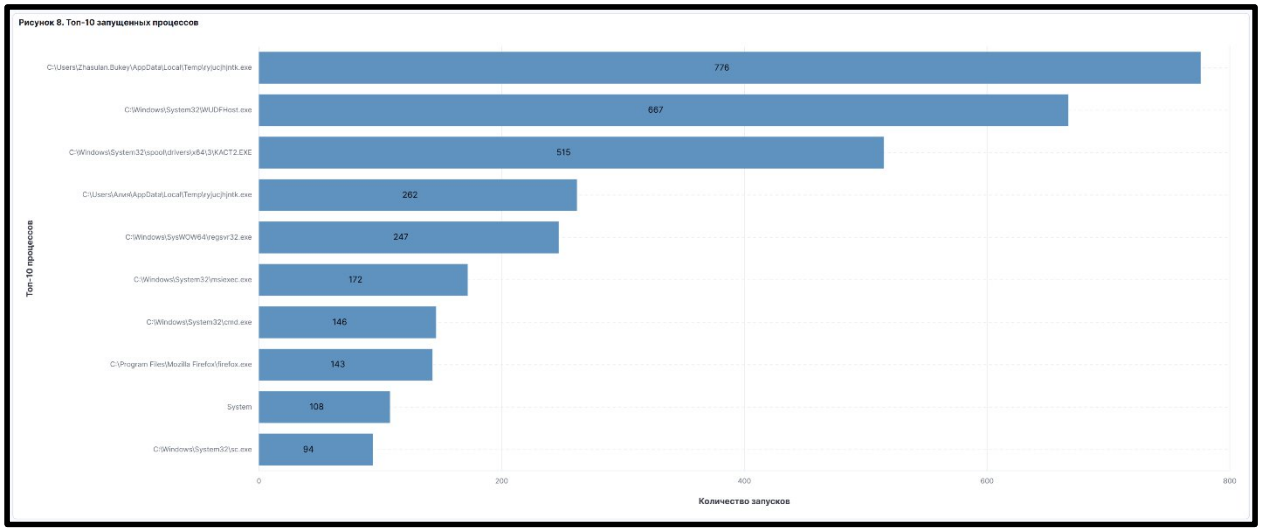

Рисунок 8. Топ-10 запущенных процессов

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000018790AEE818

На рисунке 10 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.

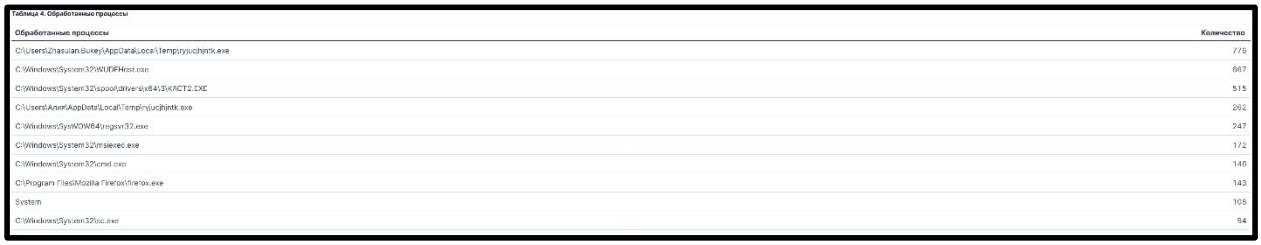

Таблица 4. Обработанные процессы

Обработанные процессы	Количество
C:\Users\Zhasulan.Sukey\AppData\Local\Temp\ryjucjhintk.exe	776
C:\Windows\System32\WUDFHost.exe	667
C:\Windows\System32\spool\drivers\x64\3\KACT2.EXE	515
C:\Users\Aneri\AppData\Local\Temp\ryjucjhintk.exe	262
C:\Windows\SysWOW64\regsvr32.exe	247
C:\Windows\System32\vmslevec.exe	172
C:\Windows\System32\cmd.exe	146
C:\Program Files\Mozilla Firefox\firefox.exe	143
System	105
C:\Windows\System32\sc.exe	94

Рисунок 9. Обработанные процессы

Примечание: Полная таблица обработанных процессов описаны в Приложении 3.

4.2. Система уведомлений

По событиям безопасности за отчётный период заведено и обработано 21 кейсов. Количество направленных уведомлений составило 2. Распределение кейсов по статусам: closed - 2, in-progress - 19. Наиболее характерные заголовки кейсов: HPCEE.exe, STCService.exe, Anomalous Process. За отчетный период зарегистрировано 2089 событий уровня high/critical; основной вклад внесло правило «Privileged Account Brute Force».

4.3 Поиск угроз

В рамках проактивного поиска угроз отдельные находки Threat Hunting по выделенному признаку не зафиксированы. При этом в отчётном периоде аналитическая обработка выполнялась на фоне 2089 событий уровня high/critical с основной концентрацией по правилам Privileged Account Brute Force, Malware Detection Alert, First Time Seen Removable Device. За отчетный период зарегистрировано 2089 событий уровня high/critical; основной вклад внесло правило «Privileged Account Brute Force».

4.4. Доступность веб-интерфейса

В отчетном периоде выполнена дополнительная проверка веб-сайта electorat.almaty.kz. В ходе анализа выявлены критичные недостатки безопасности: хранение учетных данных API в клиентском коде и отсутствие ограничений частоты запросов, что создает риск массового перебора ИИН и несанкционированного получения сведений через API. Подробная техническая информация приведена в Приложении 4.

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

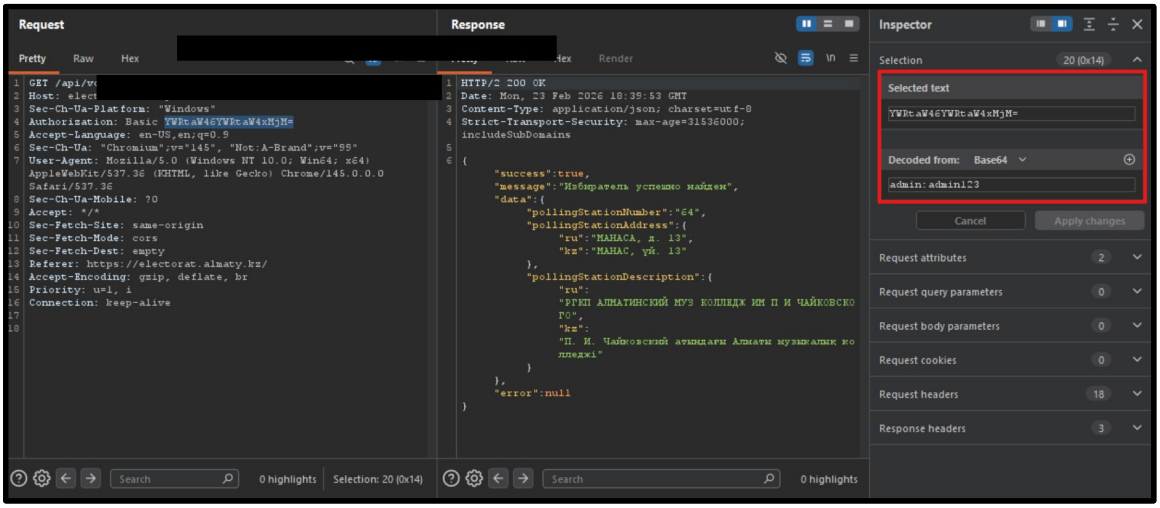

Рисунок 10. Проверка сайта electorat.almaty.kz

4.5. Автоматическое реагирование на угрозы

Средствами EDR за отчётный период заблокировано 96 вредоносных действий и 635 запусков подозрительных объектов. Изоляция была применена к 0 узлам.

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. По результатам текущего цикла во внутреннем периметре выявлено Critical - 107, High - 177, Medium - 590; во внешнем периметре выявлено Critical - 1, High - 1, Medium - 18. Наибольшая событийная активность зафиксирована в подразделениях Упр. по делам религий, Упр. градостроительного контроля, Зам. рукапы, Упр. Предприн. и инвестиций (*см. Таблицу 1*).

Таблица 1. Сканирование сети

№	Подразделение (объект сканирования)	Critical	High	Medium
1	Упр. по делам религий	40	9	9
2	Упр. градостроительного контроля	8	2	24
3	Зам. рукапы	7	6	19

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000018790AEE818

4	Упр. Предприн. и инвестиций	4	62	158
5	Аппарат Акима	4	6	6
6	Упр. цифровизации 1	4	4	5
7	Упр. молодежной политики	3	11	17
8	Аппарат Алатауского района	3	8	27
9	Упр. экологии	3	6	12
10	Упр. гор. мобильности	3	5	11

Примечание: Подробная информация по сканированиям сети указана в Приложениях 5, 6 и 7.

5.2 Статистика управления уязвимости

Сравнение результатов текущего и предыдущего запусков сканирования отражает динамику уязвимостей по уровням Critical, High и Medium. Последний учитываемый запуск завершен 2026-03-31T19:39:36Z, предыдущий - 2026-03-26T12:00:57Z. Изменение профиля рисков составило: ΔCritical = +50, ΔHigh = +62, ΔMedium = +178. Новых критических уязвимостей зарегистрировано 50, устранено 0 (*см. Таблицу 2*).

Таблица 2. Статистика управлений по уязвимостям

Наименование	**СЕЙЧАС К/В/С**	**БЫЛО К/В/С**	**ΔК/ΔВ/ΔС**	**Новые**	**Устранены**	**Без изм.**	**Крит.↑**	**Крит.↓**	**ΔХостов**
Упр. по делам религий	40/9/9	2/5/11	+38/+4/-2	3 044	56	57	38	0	+251
Упр. градостроительного контроля	8/2/24	1/1/4	+7/+1/+20	142	2 728	175	7	0	-246
Зам. рукапы	7/6/19	7/5/16	+0/+1/+3	64	63	1 260	0	0	+0

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

Упр. Предприн. и инвестиций	4/62/158	0/0/0	+4/+62/+158	1 590	0	0	4	0	+44
Аппарат Акима	4/6/6	4/6/8	+0/+0/-2	1	601	921	0	0	+0
Упр. цифровизации 1	4/4/5	3/4/3	+1/+0/+2	213	10	431	1	0	+0
Упр. молодежной политики	3/11/17	3/11/17	+0/+0/+0	9	0	440	0	0	+0
Аппарат Алатауского района	3/8/27	4/5/55	-1/+3/-28	57	2 477	538	0	1	-212
Упр. экологии	3/6/12	3/7/11	+0/-1/+1	180	13	421	0	0	+0
Упр. гор. мобильности	3/5/11	3/5/11	+0/+0/+0	3	61	437	0	0	+0

Примечание: Подробная таблица по статистике управления уязвимостями приведена в Приложении 5.

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)**. 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**;

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

- 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.

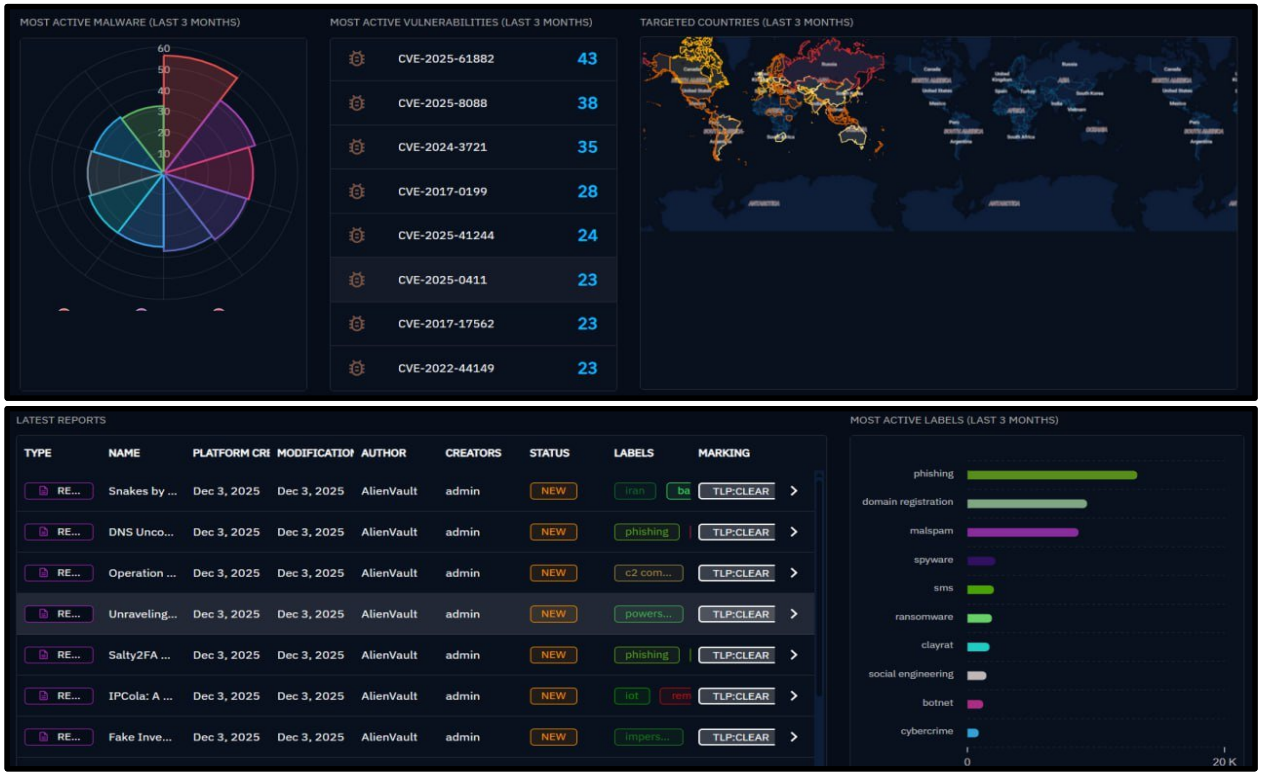

Рисунок 11. Данные OpenCTI

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

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

проверка источников угроз в соответствии с пунктом 1.1.27 технической спецификации.

За отчетный период угроз информационной безопасности не выявлено.

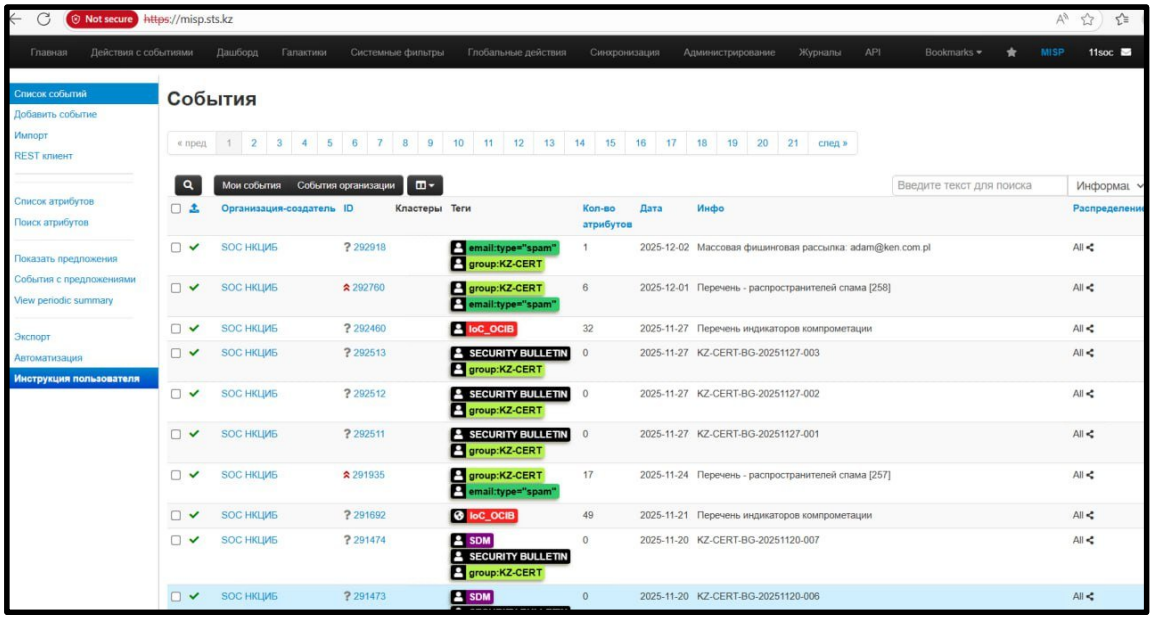

Рисунок 12 Данные MISP

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 система анализа угроз в режиме реального времени выявила 77 угроз и 396 подозрительных объектов, при общем количестве 1879 проверенных файлов/объектов. Активность носила равномерный характер в течение месяца. Основную долю проверяемых объектов составили текстовые файлы и исполняемые файлы. По результатам анализа все выявленные угрозы были обработаны средствами защиты, признаки массового заражения или распространения вредоносного программного обеспечения не зафиксировано.

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

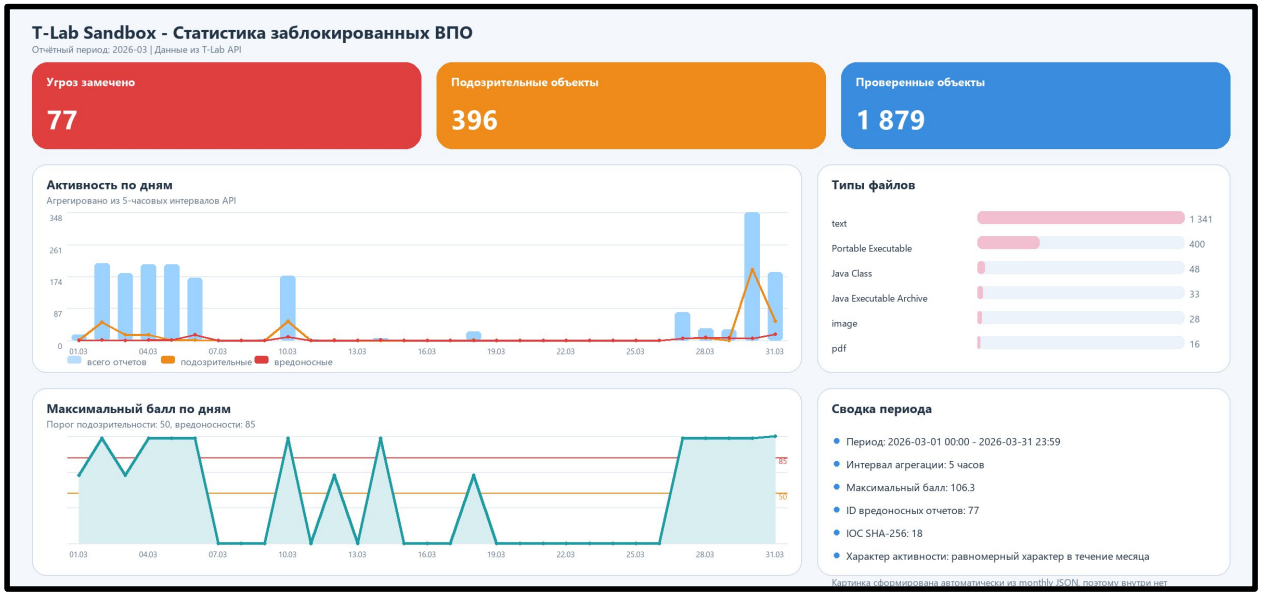

Рисунок 13. Статистика заблокированных ВПО

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 подготовлены для централизованного хранения, последующего обогащения, корреляции с другими инцидентами и использования в дальнейших мероприятиях по мониторингу и предотвращению киберугроз (*см. Таблицу 3*).

Таблица 3. IOC

№	Тип индикатора	Значение (SHA-256)
1	File Hash (SHA-256)	342bf1c60f243ce1ff65579d2808944c710491f020654216d7721a73be0727bf
2	File Hash (SHA-256)	c00575e6b362703f802bd4a7587e9e62e8f70c59ad1410855b85e54461ab328a
3	File Hash (SHA-256)	a5dc0ede3c790739680e7b7baa8e7dd3c14737f5e34ce0bdfce672c66da27cad
4	File Hash (SHA-256)	1bd413b5e840bebbcb58c1d7b85f531f26114da5c273cc12e2851333ffaa1dc7
5	File Hash (SHA-256)	97493887a39f9d02b44bd6dcbdfe0c294d747cd5b6471c85221ddfa0803b50a8
6	File Hash (SHA-256)	4a7680dcfa57277f3a5eb798b30d6729cd80e228f974f1743c705f051c567fc3
7	File Hash (SHA-256)	02974e4f8c7bbc71d30a53ddab1f2f0ce4e8f7a77dc5fa4f4e3ad64bf749b574

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

8	File Hash (SHA-256)	2d8f2401a8d303f8415ea49dd121377af273971466442efd6d3f40cd8cf2ba92
9	File Hash (SHA-256)	e9fd1e9491ae68d1ccd2d6f33f425f467dc056f01aeba565b71dca4db6e50b0a
10	File Hash (SHA-256)	269b2be0f7c32b6531a99c1846d015dba26316d9aedc07139d33ce0e70b9d5d4

Примечание: Смотреть подробный отчет T-Lab в Приложении 9

6.4. DLP – Предотвращение утечек данных (safetica)

В ходе анализа телеметрии, поступающей с рабочих станций в систему предотвращения утечек данных Safetica, за отчётный период зафиксировано 840367 событий контроля операций с данными. Наиболее активные пользователи: Guest TKSB, Guest JETS, Gaukhar Uskenova, UZE@ELCG-PC-0004, Aibar Saparhanov. Основные приложения: Google Chrome (chrome.exe), Microsoft Word (WINWORD.EXE), Проводник (explorer.exe), Microsoft Excel (EXCEL.EXE), Firefox (firefox.exe). Заметная часть DLP-активности пришлась на веб-направление: 30476 событий веб-активности. Передача данных преимущественно фиксировалась по каналам: Копировать, Переместить, Печать. По доступной выгрузке Safetica наблюдаемая активность покрывает диапазон 01.03.2026 03:04 - 31.03.2026 23:45. Подробная выгрузка Safetica приведена в Приложении 9.

6.4.1. Анализ веб – активности

В отчётном периоде по направлению веб-активности зарегистрировано 30476 событий. Преобладающие категории веб-ресурсов: Веб-приложения для мгновенных сообщений, Веб-порталы, Досуг, Внутренняя сеть, Не установлено. Отдельные события повышенного приоритета подлежат дополнительной проверке аналитиком.

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

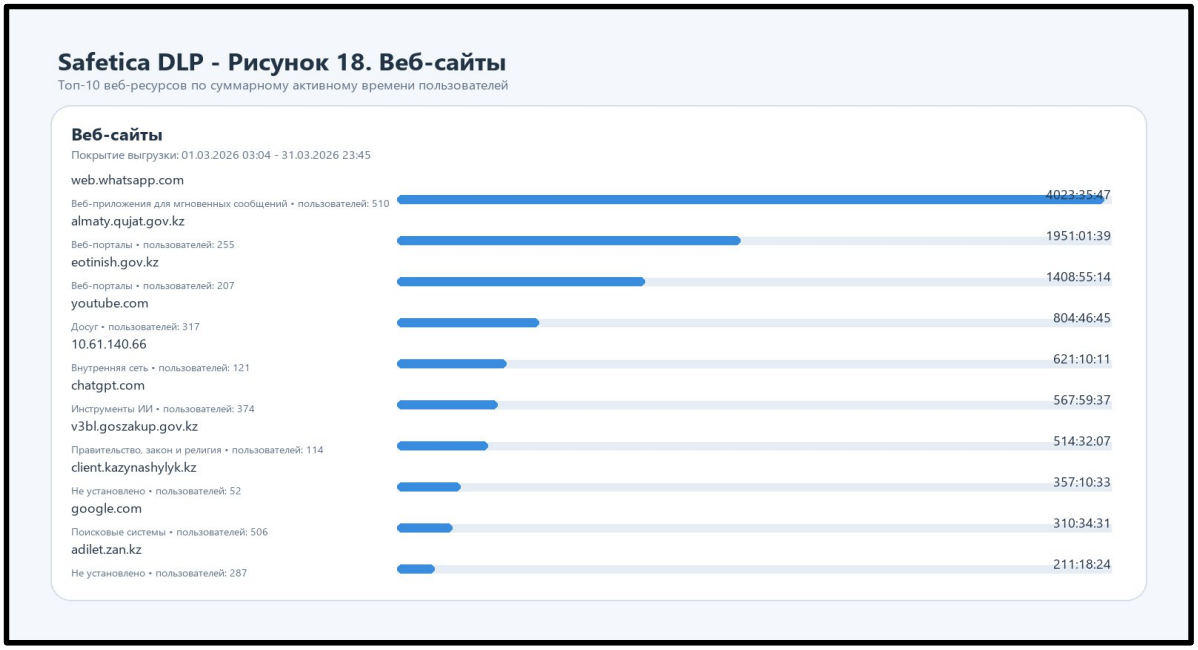

Рисунок 14. Веб-сайты

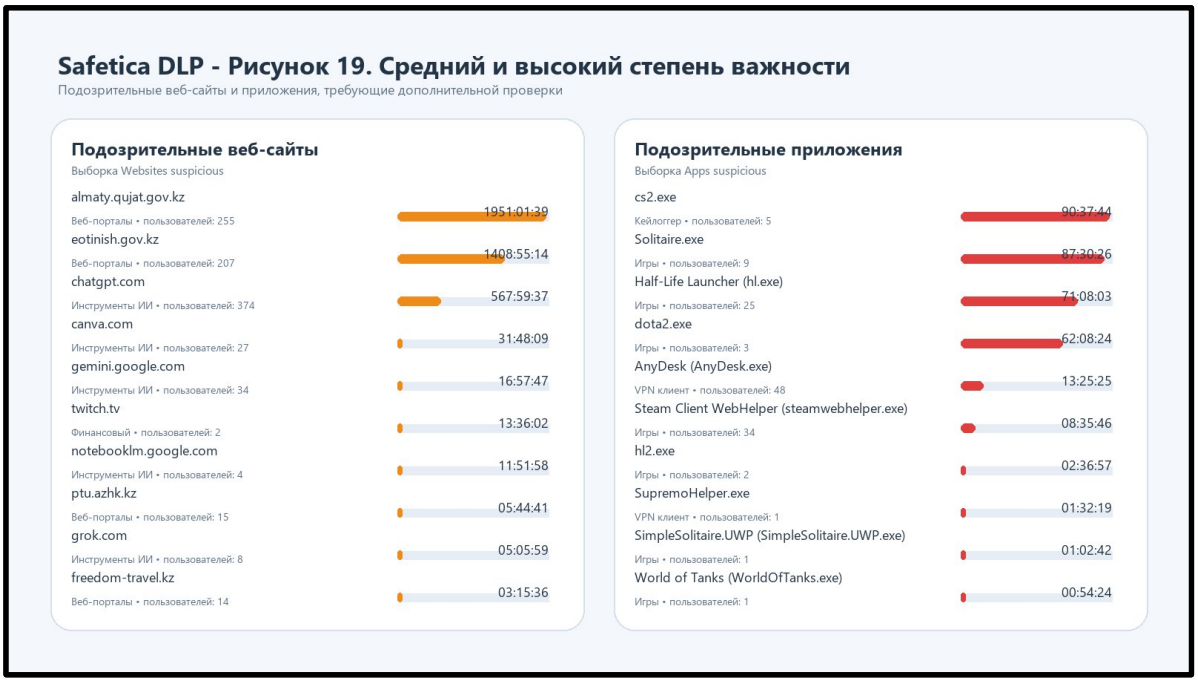

Рисунок 15. Средний и высокий степень важности

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 Проводник (explorer.exe) (≈1,6 ТБ), что обусловлено активной работой пользователей с файловой системой и сетевыми ресурсами. Существенную долю также занимают веб-браузеры (Google Chrome (chrome.exe), Microsoft Edge

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000018790AEE818

(msedge.exe) и Firefox (firefox.exe)) и офисные приложения (не представлены), что соответствует повседневной рабочей активности. Использование системных и прикладных процессов (WinRAR archiver (WinRAR.exe) и COM Surrogate (dllhost.exe)) 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.

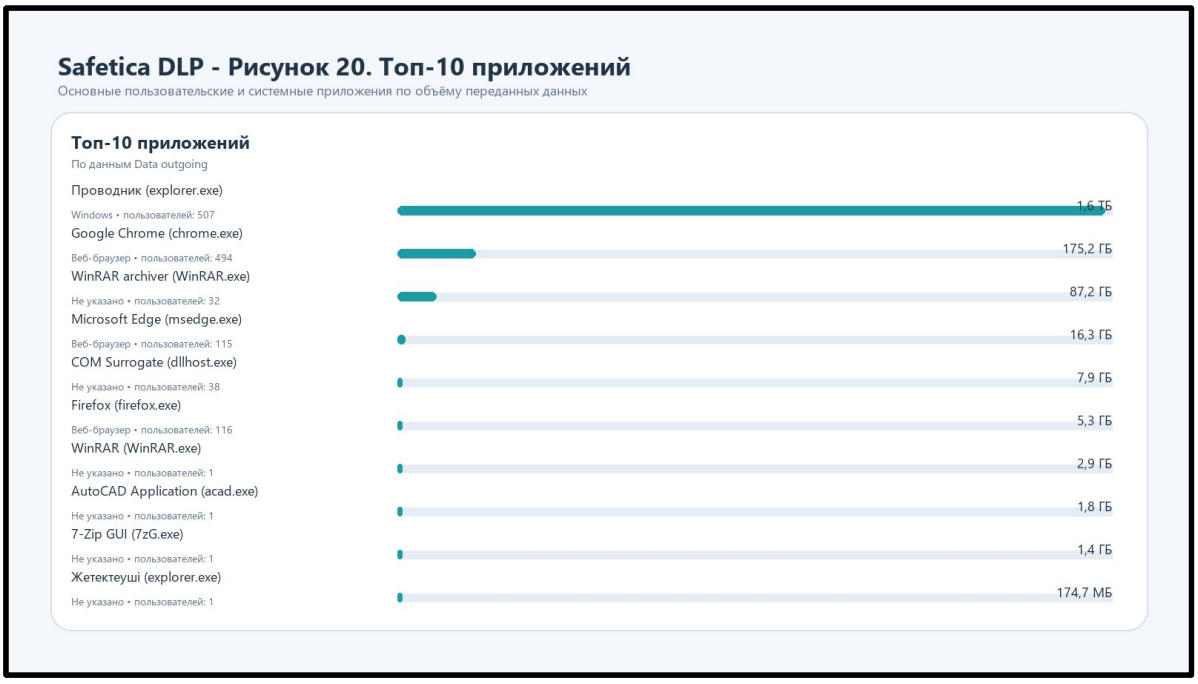

Рисунок 16. Топ-10 приложений

Таблица 5. Распределение объема переданных данных по основным пользовательским и системным приложениям.

№	Приложение	Категория	Объем переданных данных (итого)	Средний объем в активный день	Пользователи
1	Проводник (explorer.exe)	Windows	1,6 ТБ	51,4 ГБ	507
2	Google Chrome (chrome.exe)	Веб-браузер	175,2 ГБ	5,7 ГБ	494
3	WinRAR archiver (WinRAR.exe	Не указано	87,2 ГБ	4,2 ГБ	32

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business
DOC ID KZBW2Z120260000018790AEE818

	)				
4	Microsoft Edge (msedge.exe)	Веб-браузер	16,3 ГБ	576,4 МБ	115
5	COM Surrogate (dllhost.exe)	Не указано	7,9 ГБ	447,0 МБ	38
6	Firefox (firefox.exe)	Веб-браузер	5,3 ГБ	218,2 МБ	116
7	WinRAR (WinRAR.exe)	Не указано	2,9 ГБ	2,9 ГБ	1
8	AutoCAD Application (acad.exe)	Не указано	1,8 ГБ	943,4 МБ	1
9	7-Zip GUI (7zG.exe)	Не указано	1,4 ГБ	1,4 ГБ	1
10	Жетектеуші (explorer.exe)	Не указано	174,7 МБ	12,5 МБ	1

6.4.3. Служебные операции через интернет и внутренние сервисы

По служебным операциям и активности приложений зарегистрировано 1048000 событий. Наибольшая активность отмечалась в приложениях Google Chrome (chrome.exe), Microsoft Word (WINWORD.EXE), Проводник (explorer.exe), Microsoft Excel (EXCEL.EXE), Firefox (firefox.exe).

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

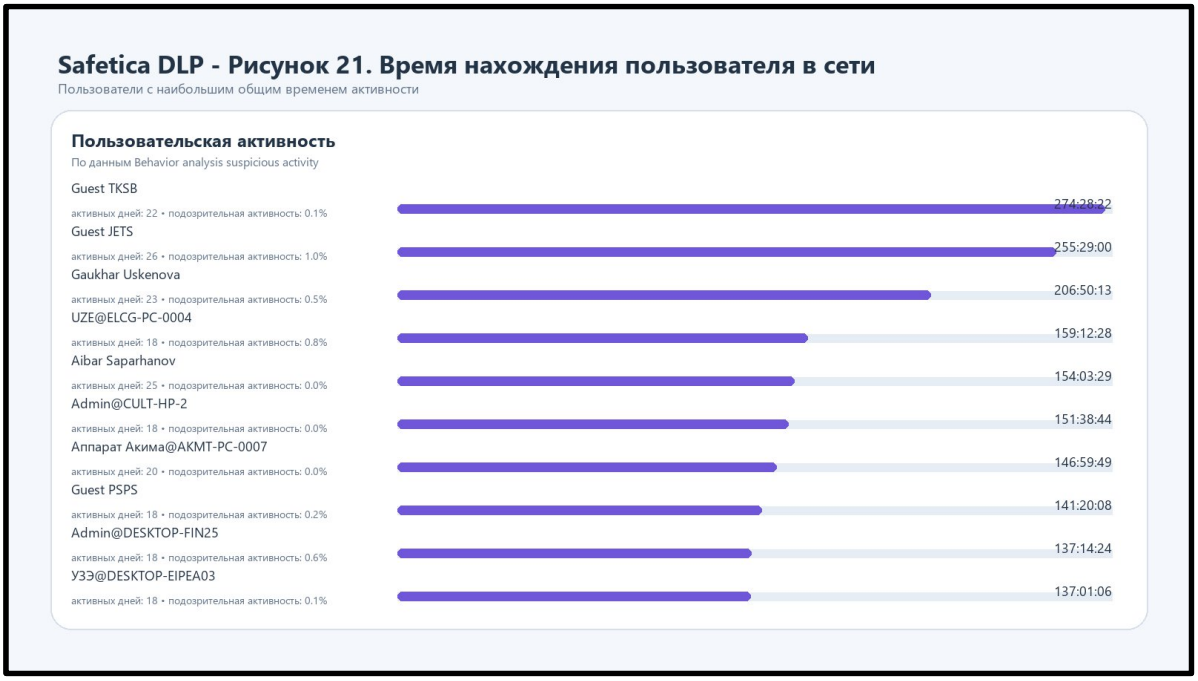

Рисунок 17. Время нахождения пользователя в сети

Таблица 6. Сетевая активность пользователя

№	Пользователь	Активные дни	Общее активное время	Подозрительная активность	Доля подозрительной активности
1	Guest TKSB	22	274:28:22	00:21:57	0.1%
2	Guest JETS	26	255:29:00	02:31:02	1.0%
3	Gaukhar Uskenova	23	206:50:13	00:57:57	0.5%
4	UZE@ELCG-PC-0004	18	159:12:28	01:17:53	0.8%
5	Aibar Saparhanov	25	154:03:29	00:00:52	0.0%
6	Admin@CULT-HP-2	18	151:38:44	00:00:23	0.0%
7	Аппарат Акима@AKMT-PC-0007	20	146:59:49	00:00:25	0.0%
8	Guest PSPS	18	141:20:08	00:13:46	0.2%

DOC ID KZBW2Z120260000018790AEE818
DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

9	Admin@DESKTOP-FIN25	18	137:14:24	00:46:16	0.6%
10	УЗЭ@DESKTOP-EIPEA03	18	137:01:06	00:04:52	0.1%

6.5 Checkpoint - межсетевой экран

В отчётном периоде на шлюзах Check Point NGFW осуществлялся мониторинг сетевой активности, выявление вредоносного трафика и блокирование потенциально опасных соединений. Совокупно зарегистрировано 26 341 892 срабатываний защитных механизмов, в том числе Anti-Bot - 15 023 378, Anti-Virus - 9 859 789, IPS - 1 458 725. Наибольшая активность наблюдалась на шлюзе GW-NAURYZBAY.

Таблица 7. Зафиксированный активность в Межсетевом экране

№	Категория	Показатель	Значение
1	Общие события безопасности	Anti-Bot события	15 023 378
2	Общие события безопасности	Anti-Virus события	9 859 789
3	Общие события безопасности	IPS-инциденты	1 458 725

Анализ сетевой активности показывает преобладание приложений удалённого доступа, обмена файлами и проксирующих сервисов. Наиболее заметная нагрузка пришлась на приложение BitTorrent Protocol (сессии - 11 562 454, трафик - 207,9 ГБ). Основные категории сетевой активности: P2P File Sharing, Remote Administration, Critical Risk, IPTV, Anonymizer. Указанные показатели требуют периодической проверки на предмет соответствия деловым задачам пользователей.

Таблица 8. Сетевая активность

№	Приложение	Сессии	Трафик
1	BitTorrent Protocol	11 562 454	207,9 ГБ
2	AnyDesk	126 477	632,4 МБ
3	uTorrent	43 378	73,5 МБ
4	MediaGet	39 662	3,4 ГБ
5	TeamViewer	9 247	593,3 МБ

DOC ID KZBW2Z120260000018790AEE818
DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

6	DotVPN	6 133	6,2 МБ
7	Perfect Dark	5 857	2,8 МБ
8	BitTorrent Sync	5 623	4,4 МБ
9	OpenVPN	1 441	1,1 МБ
10	TouchVPN	826	728,4 КБ

Средства Anti-Bot и Anti-Virus блокировали обращения к вредоносным ресурсам и попытки загрузки/исполнения вредоносных объектов. Наиболее часто детектировались сигнатуры PUA.TC.3626Wodp, Infecting_URL.ME.RS.TC.530drvMW, Cryptominer.TC.9e2clQgd, что указывает на постоянный фон сетевых угроз в адрес инфраструктуры. Признаков массового заражения по итогам отчётного периода не выявлено.

Таблица 9. Заблокированные ВПО

№	Вредоносное ПО	События
1	PUA.TC.3626Wodp	899
2	Infecting_URL.ME.RS.TC.530drvMW	662
3	Cryptominer.TC.9e2clQgd	620
4	Swift.TC.e7e0XsOZ	411
5	ModernLoader.TC.6161XCgU	288
6	Generic.TC.5d3djpnb	261
7	Trojan.Linux.RubyMiner.B	217
8	Infecting_URL.RS.TC.bec6KCYu	191
9	Adware.TC.d7f6NLGo	171
10	Infecting_URL.VUP.RS.TC.c5edmXPX	154

Система предотвращения вторжений (IPS) фиксировала и блокировала типовые сценарии сетевого воздействия и нарушений протоколов. Наиболее частыми типами событий стали Microsoft Windows NT Null CIFS Sessions, TCP Segment Limit Enforcement, Max Ping Size. Срабатывания носили превентивный характер и свидетельствуют о штатной работе защитных политик межсетевого экрана.

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

Таблица 10. Система предотвращения вторжений

№	Тип события	Сессии
1	Microsoft Windows NT Null CIFS Sessions	872 324
2	TCP Segment Limit Enforcement	325 763
3	Max Ping Size	219 819
4	IMAP Servers Long Token in LOGIN Command Buffer Overflow	10 710
5	TCP Invalid Retransmission	10 272
6	Command Injection	9 067
7	228	7 120
8	ZMap Security Scanner	599
9	RIP	456
10	Resource Records Enforcement	267

7. Реализованные системы информационной безопасности

В соответствии с техническим заданием обеспечено функционирование и сопровождение комплекса средств защиты информации, включающего: Elastic SIEM, Elastic Defend, Nessus, T-Lab Sandbox, Safetica DLP, Check Point NGFW. Состояние систем оценивается как работоспособное; детализированный статус по внедрению и сопровождению отражается в приложениях и служебной документации.

8. Выводы и рекомендации

8.1. Общие выводы

На отдельных шлюзах фиксировалось использование приложений удалённого доступа, VPN и P2P-обмена, включая BitTorrent Protocol, AnyDesk, uTorrent. Выявленные вредоносные объекты своевременно блокировались средствами Check Point; наиболее часто встречались PUA.TC.3626Wodp, Infecting_URL.ME.RS.TC.530drvMW, Cryptominer.TC.9e2clQgd. IPS фиксировала типовые сценарии сетевого воздействия, при этом признаков успешной эксплуатации уязвимостей не выявлено. Под мониторингом находилось 580 узлов; offline - 530, нестабильных/требующих проверки - 17. За отчетный период зарегистрировано 2089 событий уровня high/critical; основной вклад внесло правило «Privileged Account Brute Force». По данным

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

Nessus в отчётном периоде сохраняются 108 критических и 178 высоких уязвимостей.

8.2. Приоритетные планы работ

Продолжить актуализацию и оптимизацию правил корреляции в SIEM с учётом выявленных сценариев и особенностей инфраструктуры. Усилить контроль полноты телеметрии от агентов и качество интеграций между системами защиты. Продолжить устранение критических и высоких уязвимостей по данным сканирований и перепроверку проблемных узлов. Продолжить контроль и актуализацию политик Check Point NGFW с акцентом на risky applications, VPN и P2P-категории. Перепроверить необходимость использования приложений BitTorrent Protocol, AnyDesk, uTorrent в инфраструктуре Заказчика.

8.3. Рекомендации

Продолжить контроль и актуализацию политик Check Point NGFW с акцентом на risky applications, VPN и P2P-категории. Перепроверить необходимость использования приложений BitTorrent Protocol, AnyDesk, uTorrent в инфраструктуре Заказчика. Проводить дополнительную проверку узлов и пользователей, демонстрирующих устойчивую активность по BitTorrent, AnyDesk, OpenVPN и аналогичным приложениям. Сохранять мониторинг IPS/Anti-Bot/Anti-Virus в непрерывном режиме и пересматривать исключения на шлюзах с наибольшей активностью. Проверить offline/unhealthy агенты и сверить состояние политик на проблемных хостах. Провести ревизию логики и исключений для правила «Privileged Account Brute Force».

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z120260000018790AEE818
Тип документа	Исходящее письмо
Тема	Отчеты за март 2026 года
Статус	Отправлен
Рег. Номер:	01-01/127
Рег. Дата:	03.04.2026
Количество страниц	1237
Подписи	2

Информация об отправителе

Отправитель	ТОО "MSSP.GL"
IP-адрес	185.143.21.18

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	185.143.21.18
Email	d.salipov@mssp.global
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIXggYJ...n1KONDg==
Дата подписания	03.04.2026 13:11

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Генеральный директор
IP-адрес	185.143.21.18
Email	d.salipov@mssp.global
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIXuAYJ...YS1eOug==

Дата подписания 03.04.2026 13:12

DOC ID KZBW2Z120260000018790AEE818

DOC ID KZBW2Z120260000018790AEE818
Электронный документ подписан в Documentolog Business