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: 01.04.2026 – 30.04.2026 г.

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

Оглавление

1. ОБЩАЯ ИНФОРМАЦИЯ 3

1.1. Ключевые показатели эффективности 3

2. ВВЕДЕНИЕ 3

2.1. Цель отчета 3

2.2. Область действия 4

3. АНАЛИЗ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 5

3.1. Состояние агентов 5

3.2 Настройка и актуализация представлений данных (Data Views) 6

3.3. Усиление мониторинга и анализа событий через SIEM-систему 7

4. МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 7

4.1. Статистика событий безопасности 10

4.2. Система уведомлений 16

4.3 Поиск угроз 16

4.4. Доступность веб-интерфейса 16

4.5. Автоматическое реагирование на угрозы 16

5. АНАЛИЗ УЯЗВИМОСТЕЙ 18

5.1 Инструментальное сканирование 18

5.2 Статистика управления уязвимости 19

6. ПЛАТФОРМА АНАЛИЗА УГРОЗ И ЗАЩИТА ОТ ТАРГЕТИРОВАННЫХ АТАК 21

6.1. OpenCTI — Платформа киберразведки 21

6.2. MISP — Обмен индикаторами компрометации 22

6.3. T-Lab Sandbox — Защита от таргетированных атак 23

6.4. DLP – Предотвращение утечек данных (safetica) 28

6.4.1. Анализ веб – активности 28

6.4.2. Передачи данных 33

6.4.3. Служебные операции через интернет и внутренние сервисы 35

6.5 Checkpoint - межсетевой экран 37

7. РЕАЛИЗОВАННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

БЕЗОПАСНОСТИ 40
8. ВЫВОДЫ И РЕКОМЕНДАЦИИ 41
8.1. Общие выводы 41
8.2. Приоритетные планы работ 41
8.3. Рекомендации 42

1. ОБЩАЯ ИНФОРМАЦИЯ

Настоящий отчет представляет результаты оказания услуг по обеспечению информационной безопасности для Акимата города Алматы (далее - Заказчик) за отчетный период 01.04.2026 – 30.04.2026 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 11742 событий безопасности, по которым обработано 11 кейсов. Защита конечных точек обеспечивалась на 267 узлах, средствами EDR предотвращено 96 вредоносных действий. Через T-Lab Sandbox проверено 9452 файлов/объектов, выявлено 142 угроз. По результатам сканирования Nessus обнаружено 41 критических и 81 высоких уязвимостей. В системе Safetica зафиксировано 329136 DLP-событий. Средствами Check Point выполнено 16127725 блокировок.

2. ВВЕДЕНИЕ

Настоящий отчет подготовлен в соответствии с пунктом 4.5 технической спецификации на услуги по обеспечению информационной безопасности и охватывает период 01.04.2026 – 30.04.2026 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 KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
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;
- 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.
Указанный объем используется как проектный контур обслуживания и сформирован на основании сведений и перечней активов, предоставленных Заказчиком на этапе реализации проекта. Фактическое подключение источников событий и объектов мониторинга выполняется поэтапно и зависит от предоставления доступов, сетевой доступности, согласования параметров подключения и актуальности реестра серверного, сетевого и пользовательского оборудования. При наличии дополнительных объектов, не включенных в ранее переданные перечни, требуется актуализация реестра активов с последующим подключением таких объектов к сервисам мониторинга.

DOC ID KZBW2Z120260000195576CDEC2
DOC ID KZBW2Z120260000195576CDEC2
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 отчётном периоде контроль состояния агентов EDR осуществлялся на 641 узлах, из которых защита была активна на 267 (41.65%). Выявлено 52 узлов с признаками некорректной работы агентов и 289 узлов, находившихся вне связи. Статусы агентов: healthy - 267, inactive - 52, offline - 289, unhealthy - 33. Наиболее затронутые хосты: sprt-pc-0014, fins-pc-0042, desktop-h2ajt7e. Под мониторингом находилось 641 узлов; offline - 289, нестабильных/требующих проверки - 52.
Следует учитывать, что полное агентное покрытие всех рабочих станций ограничено рядом инфраструктурных факторов. В части подразделений эксплуатируются устаревшие операционные системы, на которых установка или стабильная работа EDR-агента невозможна либо требует отдельной модернизации. Также выявляется организационный фактор: после переустановки операционной системы отдельные рабочие станции не всегда своевременно вводятся в домен, вследствие чего они не попадают в централизованный контур управления и мониторинга. Указанные причины влияют на долю offline-узлов и требуют совместной отработки с ответственными системными администраторами.

Сведения о наличии объектов в статусе offline отражают текущее техническое состояние подключения источников событий на момент формирования отчета и не свидетельствуют об отсутствии выполнения Исполнителем мероприятий по мониторингу информационной безопасности. Мониторинг событий информационной безопасности осуществлялся по всем подключенным и передающим события источникам. Подключение дополнительных источников выполняется поэтапно и требует предоставления доступа к информационным системам, настройки сетевого взаимодействия и согласования параметров подключения с ответственными представителями Заказчика; работы по расширению охвата инфраструктуры продолжаются.

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

3.2 Настройка и актуализация представлений данных (Data Views)

В отчётном периоде представления данных Elastic использовались в штатном режиме; целевые изменения состава Data Views не выполнялись. Состояние источников данных и представлений в SIEM оценено как стабильное. В рабочем пространстве подтверждена доступность 11 Data Views; ключевые представления: case*, logs-elastic_agent-akimat_almaty, metrics-*, logs-windows.sysmon_operational-akimat, *akimat,.alerts-security.alerts-akimat, logs-*, logs-*, logs-*. Через указанные представления обеспечивался анализ событий по 44 правилам корреляции, 564 хостам и 222 учетным записям пользователей.

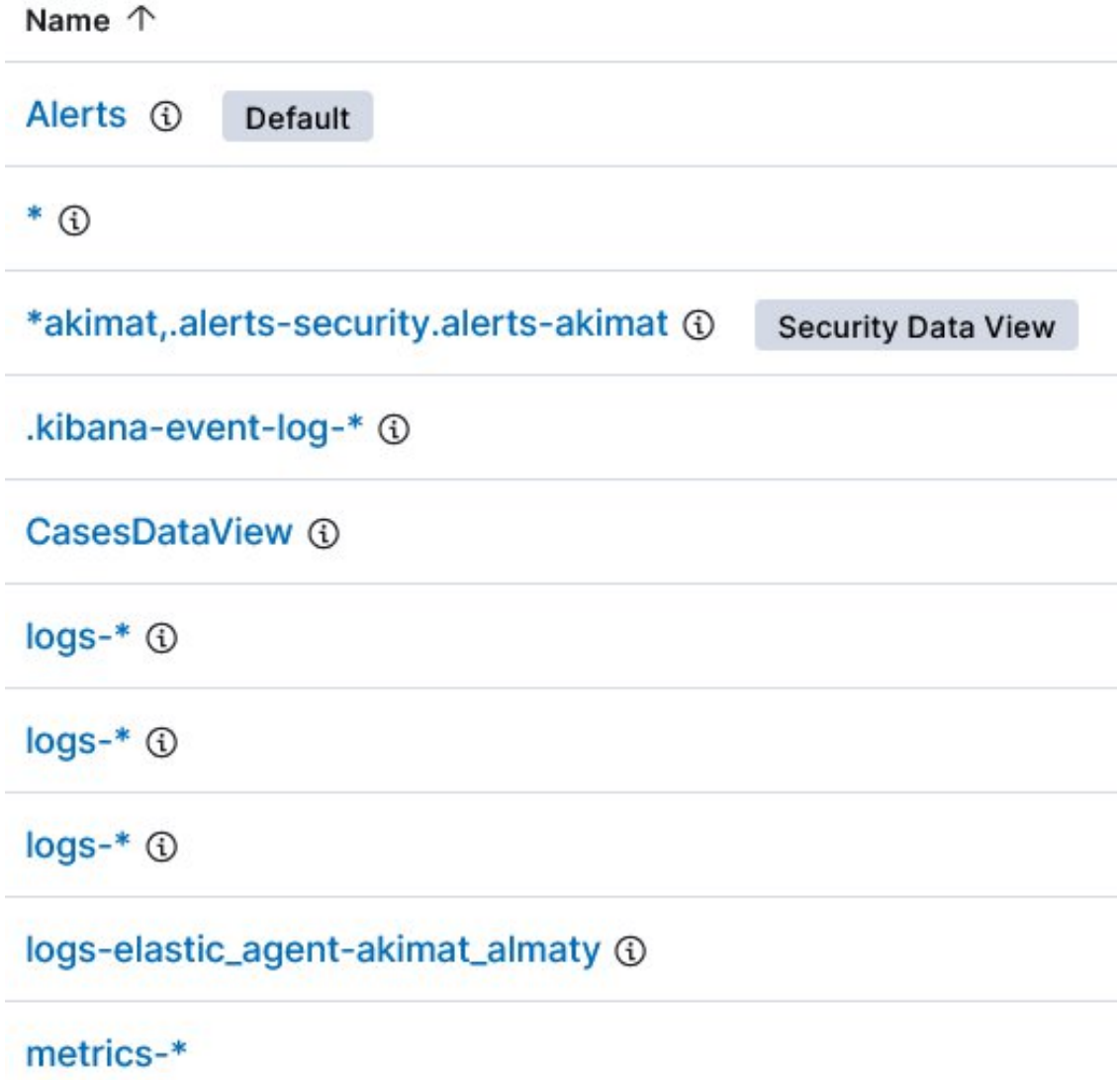

Рисунок 1. Состав представлений данных и рабочих источников Elastic

На рисунке показан состав представлений данных Elastic, задействованных в отчетном периоде. В сводном блоке указано количество Data Views - 11, а также состояние источников: стабильное. В правой части рисунка перечислены ключевые представления данных, включая: case*, logs-elastic_agent-akimat_almaty, metrics-*, logs-windows.sysmon_operational-akimat. Рисунок фиксирует, какие рабочие источники использовались для построения разделов SIEM, EDR, кейсов реагирования и аналитических выборок отчета.

DOC ID KZBW2Z120260000195576CDEC2
DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

3.3. Усиление мониторинга и анализа событий через SIEM-систему

За отчётный период в системе мониторинга обработано 11742 событий безопасности, в том числе critical - 855, high - 632, medium - 4593, low - 5662. Наиболее часто события фиксировались по правилам: First Time Seen Removable Device, Privileged Account Brute Force, Process Termination followed by Deletion. Всего в отчётном периоде срабатывания пришлись на 44 правил, 564 хостов и 222 пользователей. Наиболее затронутые хосты: asst-pc-0011, sprt-pc-0014, economy3; пользователи: СИСТЕМА, LOCAL SERVICE, administrator. Детализация по ключевым правилам корреляции показывает следующее: «First Time Seen Removable Device» - 2 276 срабатываний (19.38%); Правило фиксирует подключение или первое обнаружение съемных носителей и применяется для контроля несанкционированного переноса данных. «Privileged Account Brute Force» - 1 452 срабатываний (12.37%); Правило выявляет повторяющиеся неуспешные попытки аутентификации и используется для раннего обнаружения перебора учетных данных. «Process Termination followed by Deletion» - 1 224 срабатываний (10.42%); Правило отражает попытки сокрытия следов или нарушения штатной работы защитных механизмов на конечной точке. «High Number of Process and/or Service Terminations» - 955 срабатываний (8.13%); Правило отражает попытки сокрытия следов или нарушения штатной работы защитных механизмов на конечной точке. «Malware Detection Alert» - 855 срабатываний (7.28%); Правило «Malware Detection Alert» используется для выявления событий, соответствующих его корреляционной логике; в отчете отражено количество таких срабатываний за период.

4. МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

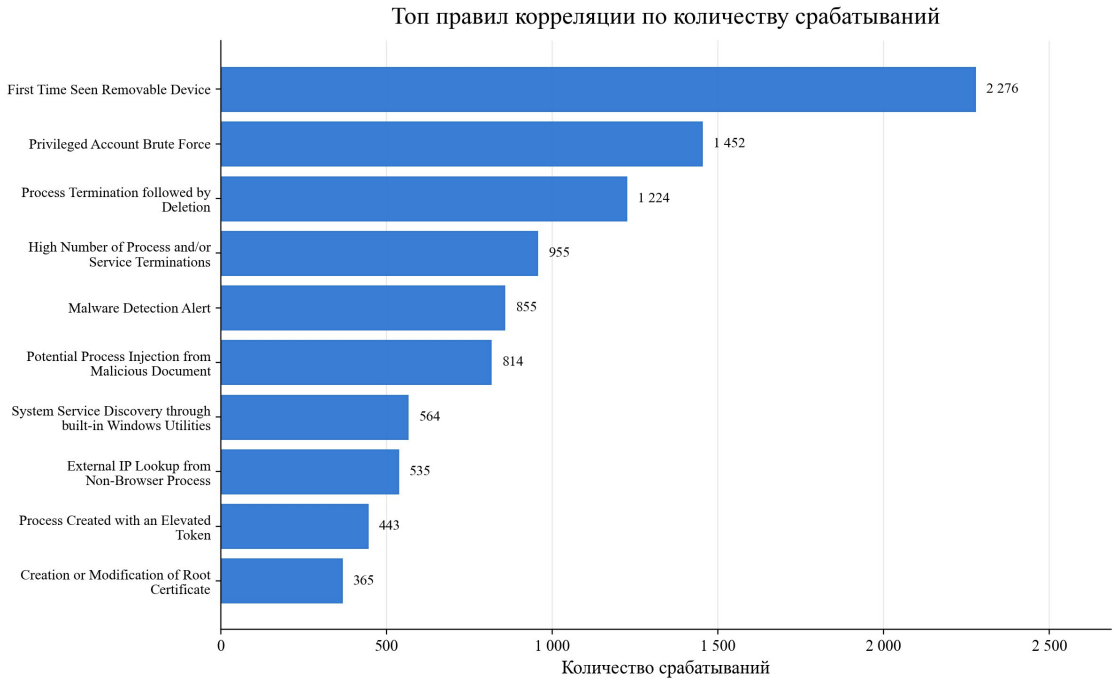

Рисунок 2. Топ правил корреляции по количеству срабатываний

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

На рисунке показаны корреляционные правила Elastic с наибольшим количеством срабатываний за отчетный период. Верхняя строка диаграммы соответствует правилу «First Time Seen Removable Device» с количеством срабатываний 2 276. Всего в периоде срабатывания пришлись на 44 правил, а на рисунке отображена верхняя часть выборки по количеству событий. Длина каждой полосы пропорциональна числу срабатываний соответствующего правила, поэтому диаграмма показывает распределение нагрузки между наиболее активными корреляционными сценариями.

Числовая расшифровка содержит правила корреляции, представленные в разделе статистики событий. В колонках указаны порядковый номер, название правила, количество срабатываний и доля от общего числа событий. Наибольшая доля в таблице относится к правилу «First Time Seen Removable Device» - 19.38%. Табличный формат дополняет диаграмму тем, что позволяет видеть точные значения и процентный вклад каждого правила без визуальной оценки длины полос.

Таблица 1. Правила корреляции

№	Название правила	Количество	Доля
1	First Time Seen Removable Device	2 276	19.38%
2	Privileged Account Brute Force	1 452	12.37%
3	Process Termination followed by Deletion	1 224	10.42%
4	High Number of Process and/or Service Terminations	955	8.13%
5	Malware Detection Alert	855	7.28%
6	Potential Process Injection from Malicious	814	6.93%

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

	Document		
7	System Service Discovery through built-in Windows Utilities	564	4.80%
8	External IP Lookup from Non-Browser Process	535	4.56%
9	Process Created with an Elevated Token	443	3.77%
10	Creation or Modification of Root Certificate	365	3.11%
11	Component Object Model Hijacking	342	2.91%
12	Suspicious WMI Image Load from MS Office	233	1.98%
13	Persistence via a Windows Installer	209	1.78%
14	Browser Extension Install	191	1.63%
15	Unusual Parent-Child Relationship	160	1.36%

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

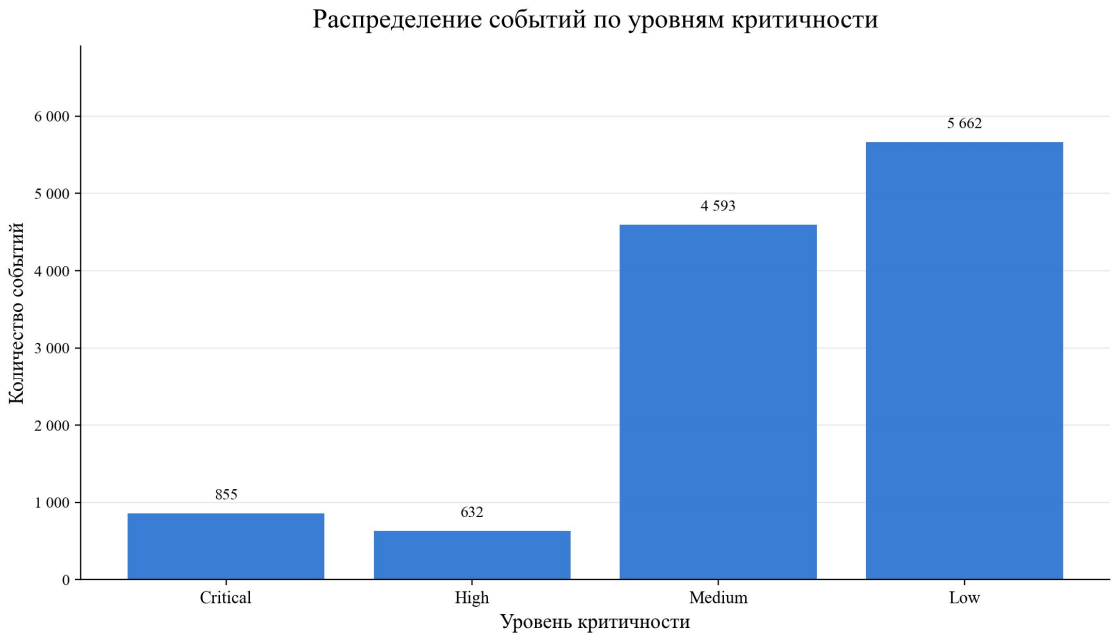

Рисунок 3. Распределение событий по уровням критичности

На рисунке показано распределение событий безопасности по уровням критичности: critical - 855, high - 632, medium - 4 593, low - 5 662. Суммарно по этим уровням отражено 11 742 событий. По горизонтальной оси указаны уровни критичности, по вертикальной - количество событий в каждой категории. Диаграмма используется как визуальная сводка структуры событий по severity и показывает, какие уровни сформировали основную часть зарегистрированной активности.

4.1. Статистика событий безопасности

В рамках мониторинга системы обнаружения и предотвращения угроз за отчётный период было зарегистрировано 11742 событий безопасности. Распределение по уровням критичности составило: critical - 855, high - 632, medium - 4593, low - 5662. Наиболее заметная активность наблюдалась по правилам First Time Seen Removable Device, Privileged Account Brute Force, Process Termination followed by Deletion, а также на узлах asst-pc-0011, sprt-pc-0014, economy3. Статусы кейсов за период: in-progress - 11. Основной объем срабатываний пришелся на сценарии, связанные с контролем внешних носителей, попытками перебора привилегированных учетных записей и разведывательной активностью внутри операционной системы.

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

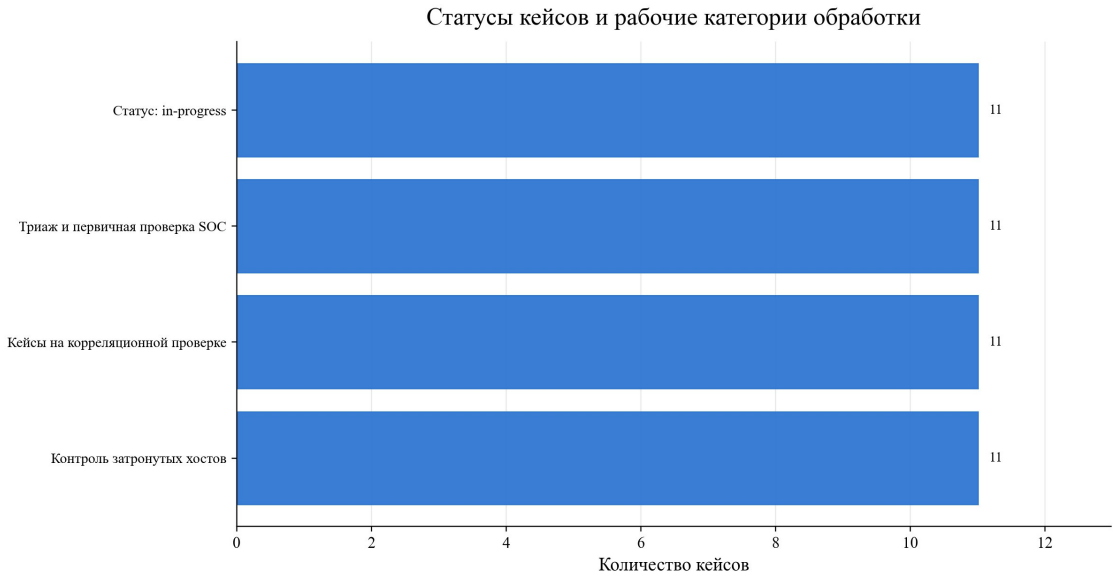

Рисунок 4. Статусы кейсов и уведомлений

На рисунке показано распределение кейсов и рабочих категорий обработки за отчетный период. Наиболее крупная категория на диаграмме: «Статус: in-progress» - 11. Общее количество кейсов в данных Elastic Cases составляет 11, количество направленных уведомлений - 11. Диаграмма объединяет фактические статусы кейсов и рабочие категории, использованные для отображения процесса обработки в отчете.

Строковая расшифровка раскрывает данные по кейсам и содержит 4 записей. В колонках указаны порядковый номер, статус или категория обработки, количество и текстовый комментарий. Строки со статусами отражают значения из Elastic Cases, а дополнительные рабочие категории показывают, как эти кейсы представлены в отчетном разделе. Таблица дополняет диаграмму тем, что фиксирует точные числа и пояснения к каждой категории.

Таблица 2. Статусы и категории обработки кейсов

№	Статус/категория	Количество	Комментарий
1	Статус: in-progress	11	Фактический статус из Elastic Cases.
2	Триаж и первичная проверка SOC	11	Кейсы приняты в аналитическую обработку.
3	Кейсы на корреляционной проверке	11	Проверка связей с правилами корреляции и повторяющимися

DOC ID KZBW2Z120260000195576CDEC2
DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

			сценариями.
4	Контроль затронутых хостов	11	Сопоставление кейсов с endpoint- и host-телеметрией.

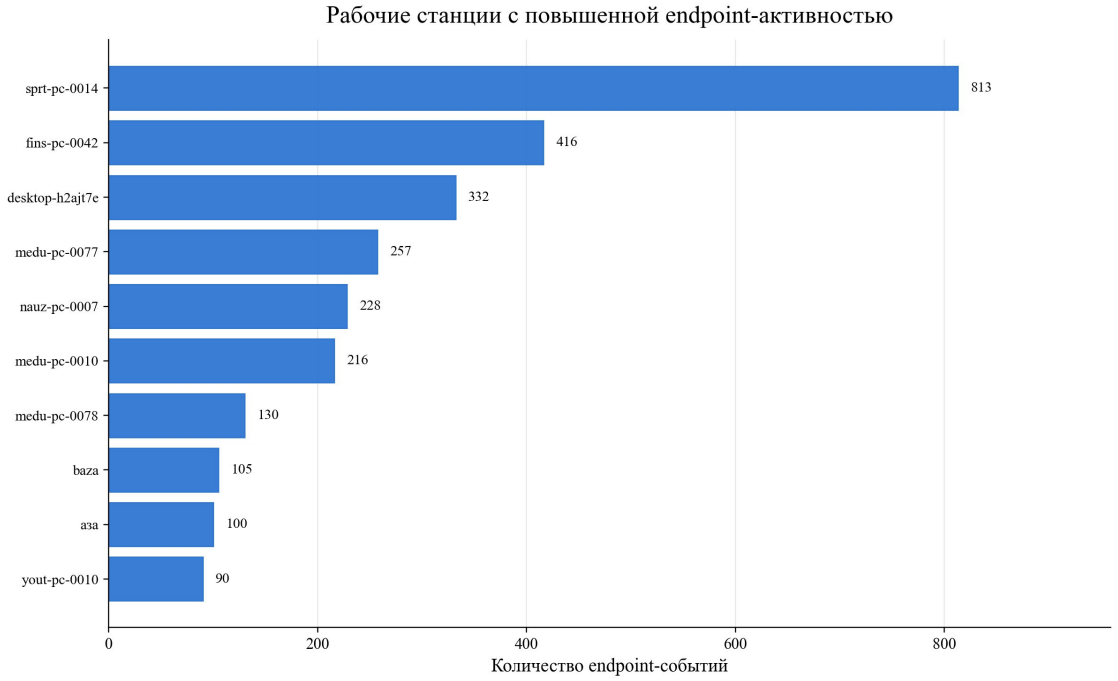

Рисунок 5. Рабочие станции с повышенной активностью

На рисунке показаны рабочие станции с наибольшим количеством endpoint-событий за отчетный период. Первое место в выборке занимает хост sprt-pc-0014 с количеством событий 813. Каждая полоса соответствует отдельной рабочей станции, а ее длина отражает количество зафиксированных endpoint-событий. Рисунок отображает верхнюю часть выборки по хостам и используется как визуальное дополнение к разделу обработки кейсов и активности конечных точек.

DOC ID KZBW2Z120260000195576CDEC2
DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

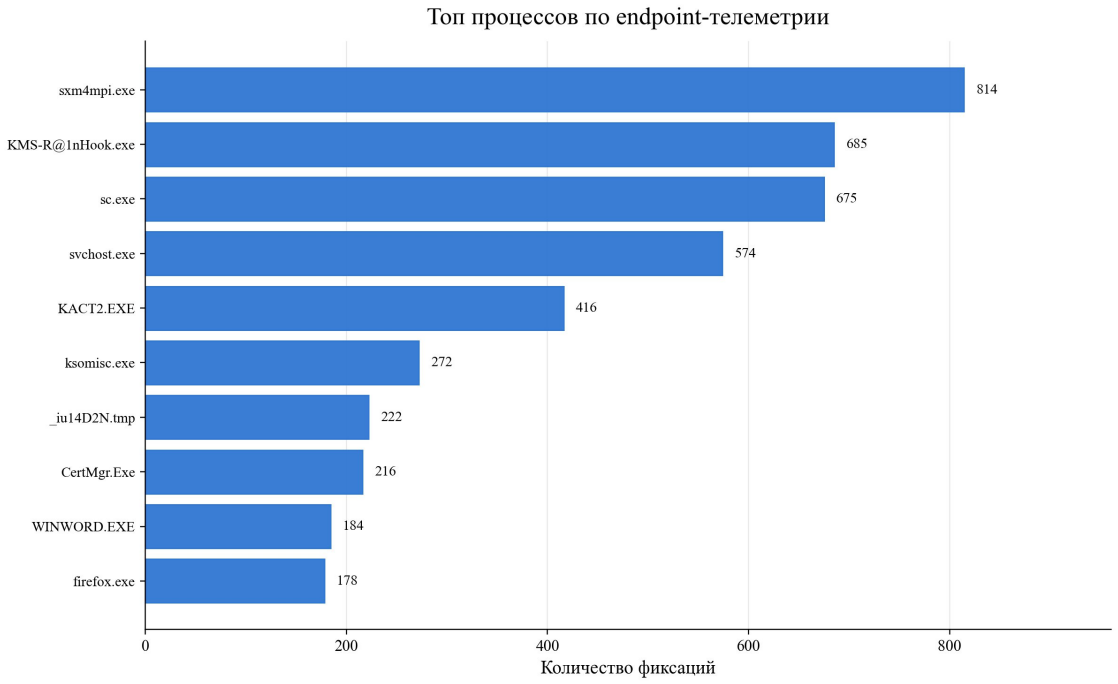

Рисунок 6. Топ процессов по endpoint-телеметрии

На рисунке показаны процессы, которые чаще всего встречались в endpoint-телеметрии за отчетный период. Верхняя строка диаграммы соответствует процессу sxm4mpi.exe с количеством фиксаций 814. По вертикальной оси перечислены имена процессов, по горизонтальной - количество фиксаций. Диаграмма показывает частотное распределение процессов и связана с таблицей ниже, где дополнительно приведено сравнение текущего и прошлого периодов.

Строковая детализация содержит процессы с изменением профиля активности относительно прошлого периода. В колонках указаны имя процесса, количество фиксаций в текущем периоде, значение прошлого периода, абсолютное изменение и комментарий из нормализованной выгрузки. Первая строка таблицы относится к процессу KMS-R@1nHook.exe. Таблица дополняет диаграмму процессов тем, что показывает не только текущую частоту, но и изменение относительно предыдущего отчетного периода.

Таблица 3. Процессы с изменением профиля активности

№	Процесс	Текущий период	Прошлый период	Δ	Комментарий

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

1	KMS-R@1nHook.exe	685	0	+685	новый или единичный в прошлом периоде
2	sxm4mpi.exe	814	481	+333	рост активности относительно прошлого периода
3	ksomisc.exe	272	0	+272	новый или единичный в прошлом периоде
4	svchost.exe	574	351	+223	рост активности относительно прошлого периода
5	sc.exe	675	453	+222	рост активности относительно прошлого периода
6	WINWORD.EXE	184	0	+184	новый или единичный в прошлом периоде
7	_iu14D2N.tmp	222	57	+165	рост активности относительно прошлого периода
8	CertMgr.Exe	216	112	+104	рост активности относительно

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

					прошлого периода
9	neunative-m.exe	105	5	+100	рост активности относительно прошлого периода
10	updroots.exe	100	0	+100	новый или единичный в прошлом периоде
11	NCALayer.exe	100	17	+83	рост активности относительно прошлого периода
12	unins000.exe	75	25	+50	рост активности относительно прошлого периода
13	taskhost.exe	50	0	+50	новый или единичный в прошлом периоде
14	unins001.exe	54	16	+38	рост активности относительно прошлого периода
15	HPCEE.exe	41	6	+35	рост активности относительно прошлого периода

DOC ID KZBW2Z120260000195576CDEC2
DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

4.2. Система уведомлений

По событиям безопасности за отчётный период заведено и обработано 11 кейсов. Количество направленных уведомлений составило 11. Распределение кейсов по статусам: in-progress - 11. Дополнительно кейсы рассматривались через рабочие категории обработки: первичный триаж SOC, корреляционная проверка сработавших правил и контроль затронутых хостов по endpoint-телеметрии. Наиболее характерные заголовки кейсов: CCleaner64.exe, KACT2.EXE, utweb.exe. За отчетный период зарегистрировано 1487 событий уровня high/critical; основной вклад внесло правило «First Time Seen Removable Device».

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 1487 событий уровня high/critical с основной концентрацией по правилам First Time Seen Removable Device, Privileged Account Brute Force, Process Termination followed by Deletion. За отчетный период зарегистрировано 1487 событий уровня high/critical; основной вклад внесло правило «First Time Seen Removable Device».

4.4. Доступность веб-интерфейса

В отчётном периоде веб-интерфейс SIEM функционировал в штатном режиме и оставался доступным для выполнения задач мониторинга, анализа событий и сопровождения кейсов. Существенных перебоев, препятствующих работе операторов и аналитиков, не зафиксировано. Доступность интерфейса позволяла своевременно просматривать корреляционные события, контролировать статус инцидентов и выполнять необходимые действия по сопровождению расследований. Работа с панелями, представлениями данных и карточками событий осуществлялась в обычном рабочем порядке на протяжении отчётного периода.

4.5. Автоматическое реагирование на угрозы

Средствами EDR за отчётный период заблокировано 96 вредоносных действий и 869 запусков подозрительных объектов. Дополнительно по телеметрии конечных точек выделены процессы с аномальным ростом активности относительно прошлого периода: KMS-R@1nHook.exe - 685 запусков за текущий период против 0 ранее (Δ +685); новый или единичный в прошлом периоде. sxm4mpi.exe - 814 запусков за текущий период против 481 ранее (Δ +333); рост активности относительно прошлого периода. ksomisc.exe - 272 запусков за текущий период против 0 ранее (Δ +272); новый или единичный в прошлом периоде. svchost.exe - 574 запусков за текущий период против 351 ранее (Δ +223); рост активности относительно прошлого периода.

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

За апрель были произведены ручные действия реагирования с консоли Elastic Defend: временная изоляция отдельных хостов, постановка файлов в карантин, передача задач локальным администраторам, очистка рабочих станций и последующая разблокировка после подтверждения устранения.

Ключевые действия реагирования по операционным сообщениям за период: 01.04-16.04 отработаны повторные попытки запуска DriveMgr.exe и связанных маскирующихся файлов на nauz-pc-0052, medu-pc-0077, medu-pc-0035 и nauz-pc-0024; по nauz-pc-0024 зафиксирована цепочка cmd.exe -> DriveMgr.exe -> sihost.exe из нестандартного каталога, хост был изолирован и передан администраторам для очистки; 03.04-30.04 рассматривалась повторяющаяся активность AnyDesk.exe на medu-pc-0010, desktop-qp7t2ok, buh2, buh3, turz-pc-0013, tansu, cntr-pc-0005 и desktop-fl3rb84; проверялись исходящие соединения, persistence, источник загрузки и легитимность запуска с повышенными привилегиями; 03.04 и 11.04 вредоносные файлы acrobat-pro2026_id3048620ids1s.exe и Abcupdate.exe были помещены в карантин на desktop-2o3q61u и cntr-pc-0001, после чего рекомендована дополнительная проверка хостов на подозрительные файлы и автозагрузку; 13.04-24.04 по socp-pc-0056, asst-pc-0032, medu-pc-0078 и nauz-pc-0002 отработаны запуски uFiler.exe, sysnldcvmr.exe, DriveSecManager.exe и связанных процессов с внешних носителей; часть хостов изолировалась до очистки и подтверждения возможности разблокировки; 22.04 по medu-pc-0078 выявлена цепочка taskhostw.exe/taskhost.exe/audiodg.exe/MicrosoftHost.exe из каталогов C:\ProgramData\RealtekHD\ и C:\ProgramData\WindowsTask\ с попыткой соединения conhostservice.xyz:3333 по stratum+tcp; активность квалифицирована как признаки трояна/криптомайнера, хост был изолирован, после очистки выполнялся контроль повторных срабатываний; 21.04 по sprt-pc-0014 отработан многократный запуск KMS-R@1nHook.exe от имени NETWORK SERVICE; хост был изолирован, легитимность события передана на подтверждение ответственным администраторам; 24.04 по asst-pc-0032 выявлена цепочка запуска DriveSecManager.exe с USB-носителя, sysnldcvmr.exe и WerFault.exe с признаками clipper/downloader/backdoor/persistence и C2 185.215.113.66; хост был изолирован, администраторам переданы рекомендации по проверке автозагрузки, внешних носителей и дополнительной очистке.

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
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. По результатам текущего цикла во внутреннем периметре выявлено Critical - 41, High - 81, Medium - 192; во внешнем периметре выявлено Critical - 0, High - 0, Medium - 14. Наибольшая событийная активность зафиксирована в подразделениях Зам. рукапы, Упр. молодежной политики, Аппарат Ауэзовского района, Упр. экологии.

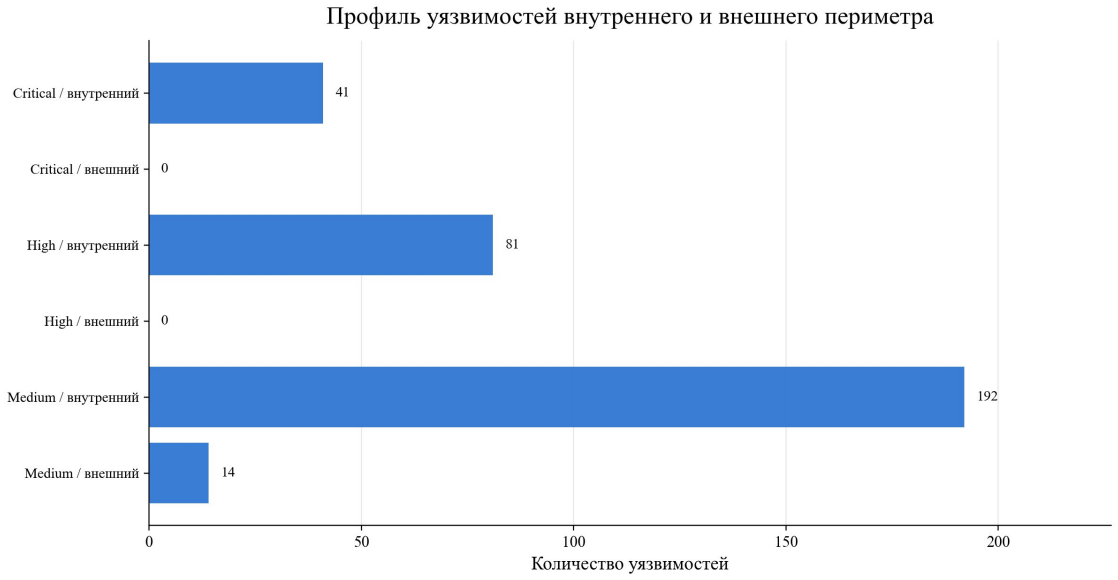

Рисунок 7. Профиль уязвимостей внутреннего и внешнего периметра

Таблица 4. Сканирование сети

№	Подразделение (объект сканирования)	Critical	High	Medium
1	Зам. рукапы	7	6	18
2	Упр. молодежной политики	4	10	17
3	Аппарат Ауэзовского района	3	16	51
4	Упр. экологии	3	8	12
5	Упр. гор.	3	5	11

DOC ID KZBW2Z120260000195576CDEC2
DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

	мобильности			
6	Аппарат Акима	3	4	5
7	Упр. цифровизации 1	3	4	4
8	Упр. градостроительного контроля	3	1	9
9	Упр. гос. активов	2	8	16
10	Упр. строительства	2	7	13

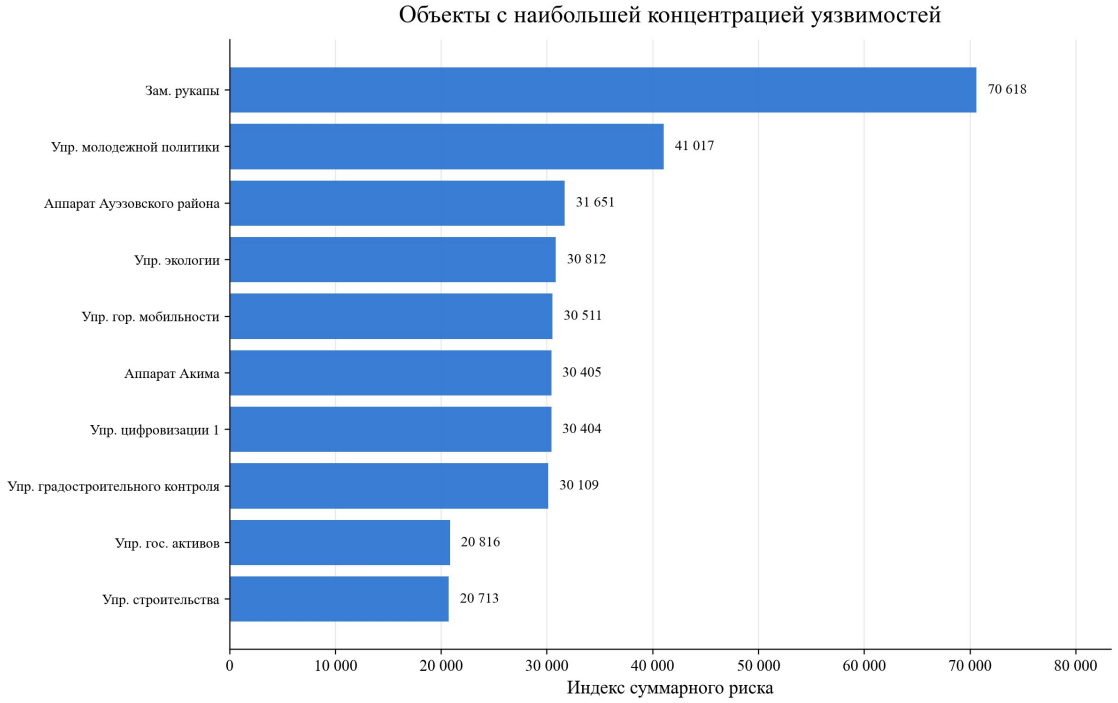

Рисунок 8. Объекты с наибольшей концентрацией уязвимостей

Примечание: Подробная информация по сканированиям сети указана в Приложениях 4, 5 и 6.

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 2026-04-29T08:28:20Z, предыдущий - 2026-03-31T16:40:41Z. Изменение профиля рисков составило: ΔCritical = +31, ΔHigh = +72, ΔMedium = +107. Новых критических уязвимостей по данным сравнения сканов зарегистрировано 31; подтвержденное снижение количества критических уязвимостей в апрельском срезе повторного сканирования не зафиксировано.

DOC ID KZBW2Z120260000195576CDEC2
DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

В рамках оказываемых услуг Исполнителем регулярно выполняются мероприятия по выявлению уязвимостей, анализу результатов сканирования и подготовке рекомендаций по их устранению. Информация о выявленных критических уязвимостях и соответствующие рекомендации доводятся до сведения Заказчика в установленном порядке. При этом непосредственное устранение уязвимостей на объектах Заказчика выполняется владельцами информационных систем и ответственными администраторами Заказчика с учетом их полномочий, уровня доступа и регламентов эксплуатации.

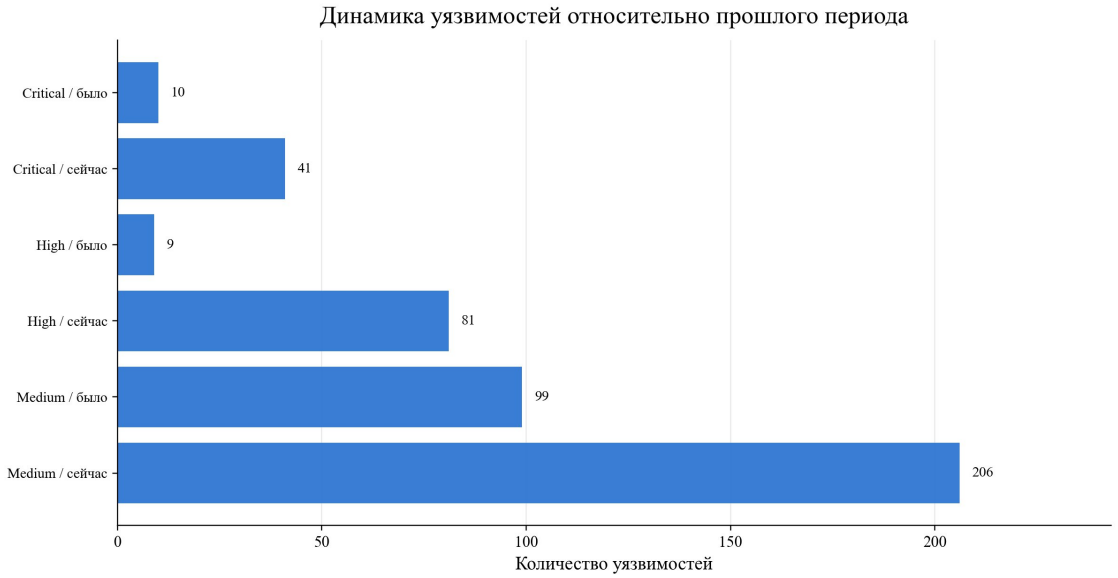

Рисунок 9. Динамика уязвимостей относительно прошлого периода

Таблица 5. Статистика управления уязвимостями

Скан	СЕЙЧАС К/В/С	БЫЛО К/В/С	ΔК/ΔВ/ΔС	Новые	Устранены	Без изм.	Крит.↑	Крит.↓	ΔХостов
Зам. рукапы	7/6/18	0/0/0	+7/+6/+18	1 252	0	0	7	0	+256
Упр. молодежной политики	4/10/17	0/0/0	+4/+10/+17	350	0	0	4	0	+256
Аппарат Ауэзовского района	3/16/51	1/6/23	+2/+10/+28	247	131	611	2	0	-1
Упр.	3/8/12	0/0/	+3/+8/	653	0	0	3	0	+256

DOC ID KZBW2Z120260000195576CDEC2
DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

экологии		0	+12						
Упр. гор. мобильности	3/5/11	0/0/0	+3/+5/+11	453	0	0	3	0	+256
Аппарат Акима	3/4/5	0/0/0	+3/+4/+5	676	0	0	3	0	+256
Упр. цифровизации 1	3/4/4	0/0/0	+3/+4/+4	561	0	0	3	0	+256
Упр. градостроительного контроля	3/1/9	8/2/24	-5/-1/-15	1 284	101	216	0	5	+129
Упр. гос. активов	2/8/16	0/0/0	+2/+8/+16	911	0	0	2	0	+256
Упр. строительства	2/7/13	0/0/0	+2/+7/+13	676	0	0	2	0	+256

Примечание: Подробная таблица по статистике управления уязвимостями приведена в Приложении 4.

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,

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

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.

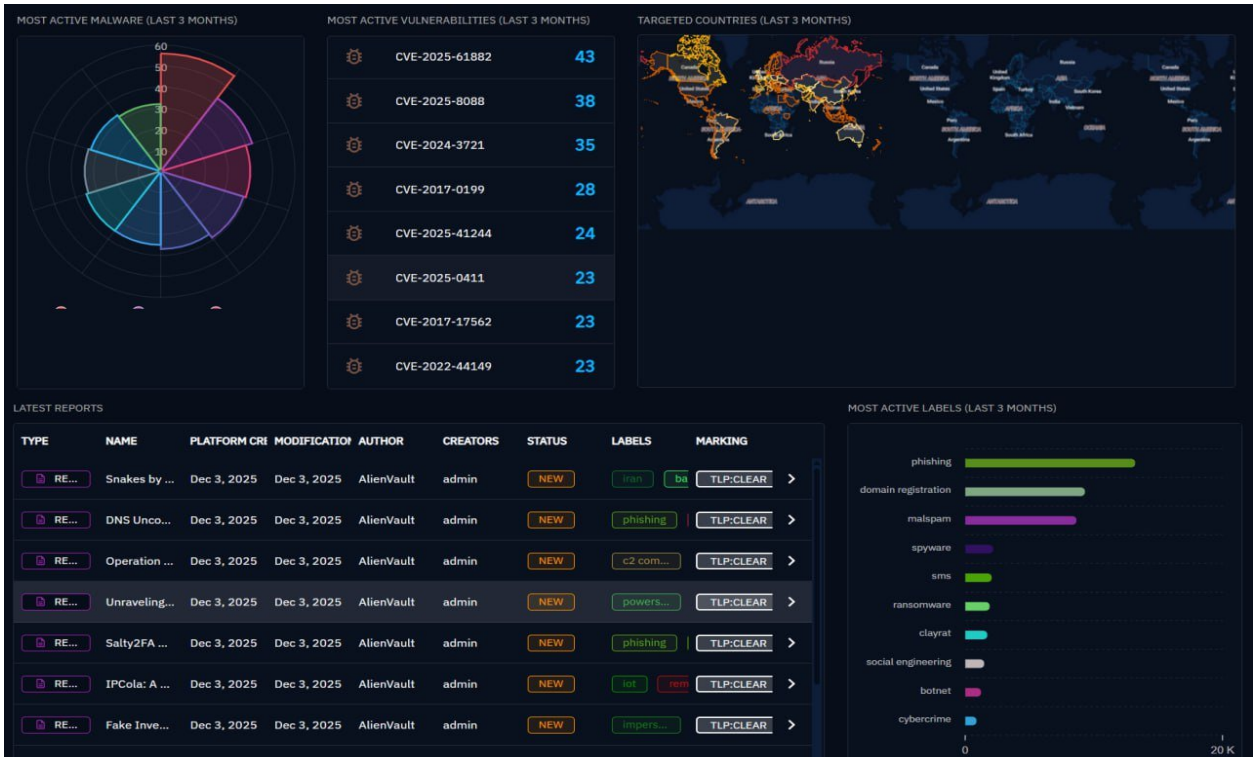

Рисунок 10. Информация с OpenCTI

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.

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

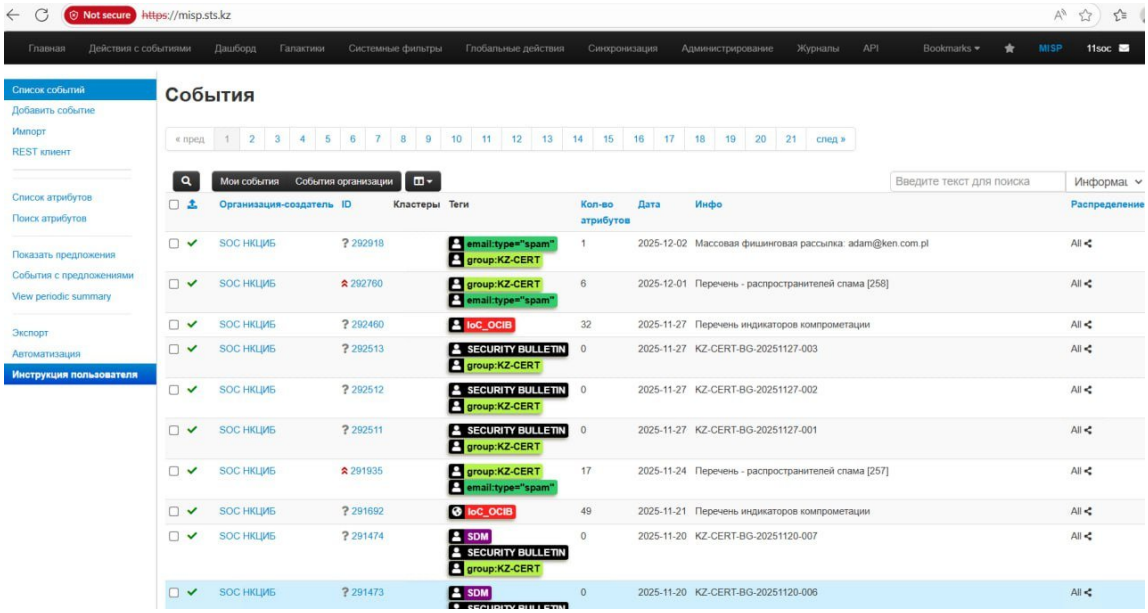

Рисунок 11. MISP

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 142 угроз и 290 подозрительных объектов, при общем количестве 9452 проверенных файлов/объектов. Активность носила равномерный характер в течение месяца. Основную долю проверяемых объектов составили текстовые файлы и Java Class. В выборку отчетного периода вошло 64 отчетов T-Lab; максимальная оценка риска по статистике платформы составила 128.32, сформировано 20 SHA-256 IOC. По результатам анализа все выявленные угрозы были обработаны средствами защиты, признаки массового заражения или распространения вредоносного программного обеспечения не зафиксировано. Дополнительно выполнялась сверка результатов sandbox-анализа с SIEM/EDR для уточнения повторяющихся сценариев и приоритизации вредоносных объектов.

Сводный блок показателей фиксирует общий объем работы T-Lab за отчетный период: количество проверенных объектов - 9 452, из них 142 классифицированы как вредоносные, 290 отнесены к подозрительным, а 9 020 не имели признаков вредоносной активности. Доля вредоносных объектов составила 1.50%, доля подозрительных - 3.07%. В таблице отдельно выделены количество отчетов T-Lab, число сформированных IOC и максимальная оценка риска, что позволяет видеть одновременно объем проверок и количество технических индикаторов, сформированных по результатам анализа. Значения в таблице описывают итоговую сводку за месяц и не заменяют карточки отдельных объектов: они показывают агрегированный результат работы sandbox-контура за отчетный период. Такой формат удобен

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

для сопоставления общего числа проверок, количества подозрительных результатов и числа IOC в одном месте без детализации по каждому отдельному файлу.

Таблица 6. Сводные показатели T-Lab Sandbox

Показатель	Значение	Комментарий
Проверено объектов	9 452	Общее количество объектов, прошедших проверку в T-Lab.
Вредоносные объекты	142	Объекты, классифицированные как вредоносные.
Подозрительные объекты	290	Объекты с подозрительным verdict в выгрузке T-Lab.
Отчетов T-Lab в периоде	64	Количество отчетов, попавших в отчетный период.
IOC SHA-256	20	Количество сформированных индикаторов компрометации.
Максимальный риск/score	128	Максимальная оценка риска по статистике T-Lab.

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

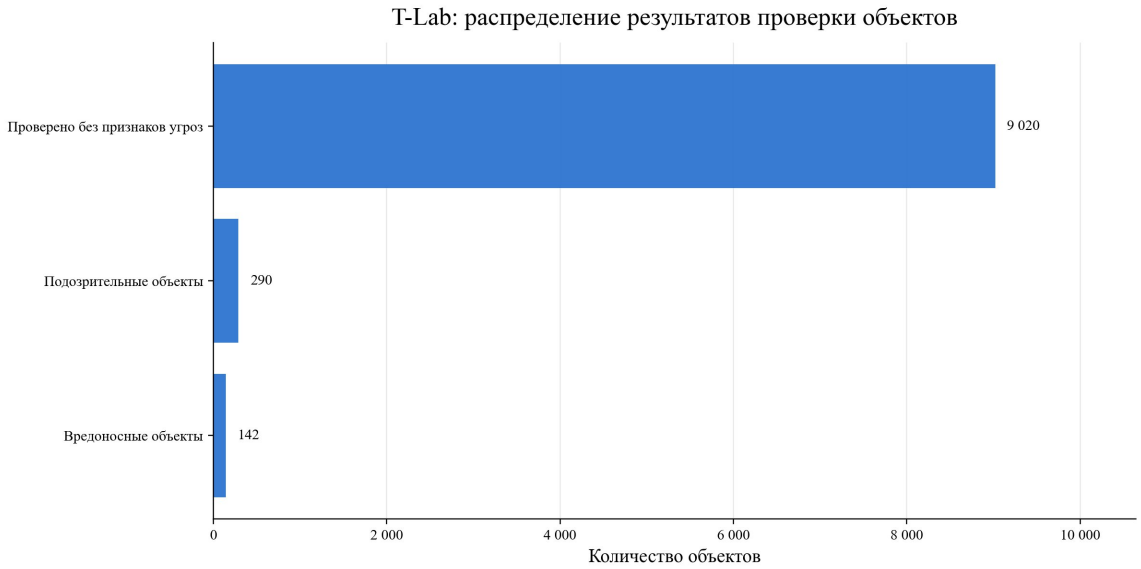

Рисунок 12. Распределение результатов проверки T-Lab

На диаграмме распределения результатов проверки показано, как общий поток из 9 452 объектов разделился по итоговым verdict-статусам T-Lab. Безопасная часть выборки составила 9 020 объектов, вредоносная - 142, подозрительная - 290. На рисунке визуально отделены объекты без признаков вредоносности от объектов, получивших вредоносный или подозрительный verdict. Размер каждого сегмента соответствует количеству объектов в соответствующей категории, поэтому по диаграмме видно соотношение основной безопасной массы и меньших групп с повышенным уровнем риска. Текстовое описание рядом с диаграммой фиксирует эти же значения числами, чтобы результат был понятен без обращения к исходной выгрузке T-Lab.

Рисунок 13. Динамика анализа объектов T-Lab по дням

На графике динамики по дням показано, как распределялась активность T-Lab внутри отчетного месяца. В исходной статистике использовано 144 временных интервалов, из которых 102 содержали фактические отчеты,

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

поэтому график отражает не единичную выгрузку, а поведение системы во времени. По горизонтальной оси отображены даты периода, по вертикальной оси - количество отчетов или объектов, пришедших на анализ в соответствующий день. Участки с более высокими значениями показывают дни, когда в T-Lab поступало больше объектов, а участки с низкими значениями отражают периоды меньшей активности. График используется как временная расшифровка месячной сводки: он показывает, распределялись ли проверки равномерно или были сконцентрированы в отдельные даты.

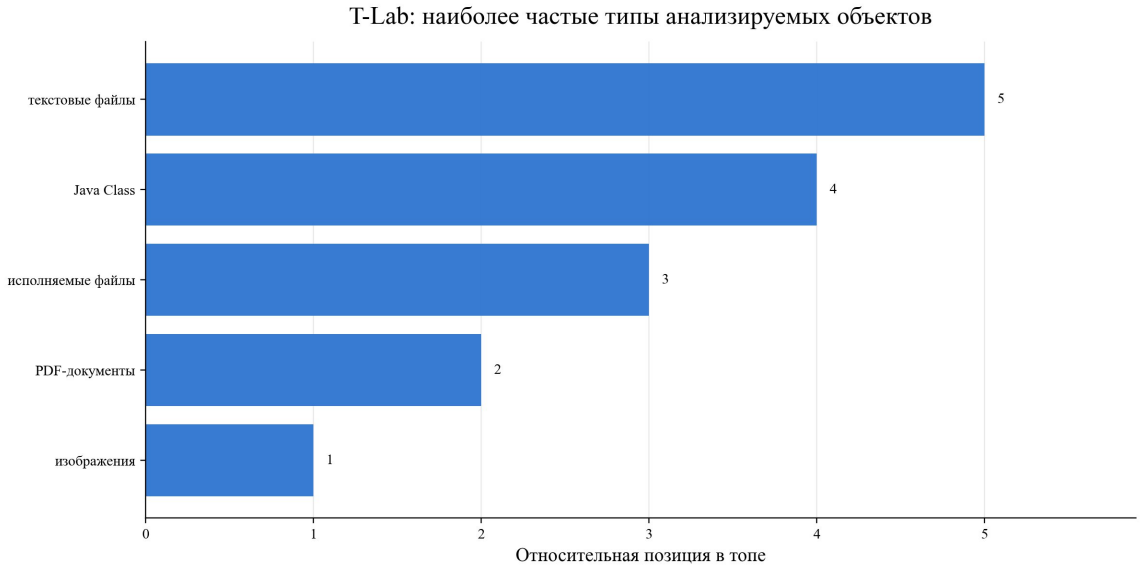

Рисунок 14. Наиболее частые типы анализируемых объектов T-Lab

На диаграмме типов объектов показано, какие форматы файлов чаще всего поступали в T-Lab на динамический или статический анализ. В текущем периоде среди наиболее частых типов указаны: текстовые файлы, Java Class, исполняемые файлы, PDF-документы, изображения. Каждая полоса диаграммы соответствует отдельному типу объекта, а ее длина отражает относительное место этого типа в выборке. Рисунок показывает структуру анализируемого потока файлов без детализации по конкретным пользователям или источникам поступления. По этой диаграмме видно, какие форматы составляют основную часть материалов, обработанных T-Lab за отчетный период.

В табличной расшифровке типы объектов представлены в ранжированном виде, что удобно для последующей сверки с источниками поступления файлов и правилами обработки вложений. В первой колонке указан порядковый номер, во второй - тип объекта из нормализованной выгрузки T-Lab. Таблица повторяет содержательный смысл диаграммы, но представляет данные в текстовом виде, чтобы перечень форматов можно было прочитать без визуальной оценки длины полос. Такой формат фиксирует состав наиболее часто встречавшихся типов объектов за месяц и сохраняет его в отчете как отдельный структурированный блок.

Таблица 7. Наиболее частые типы анализируемых объектов T-Lab

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

№	Тип объекта
1	текстовые файлы
2	Java Class
3	исполняемые файлы
4	PDF-документы
5	изображения

Блок IOC содержит первые 10 SHA-256 индикаторов из 20 сформированных значений. Каждая строка таблицы представляет конкретный файловый хэш, полученный из результатов T-Lab. В первой колонке указан порядковый номер, во второй - тип индикатора, в третьей - само значение SHA-256. Таблица показывает технические индикаторы в текстовом виде и дополняет диаграммы, где отражены только агрегированные показатели по verdict-статусам, датам и типам файлов.

Таблица 8. IOC

№	Тип индикатора	Значение
1	File Hash (SHA-256)	696f18a21c58b04c6fe4d2d5ecf1ac5e9135c9e2922abc804aabd1425942e449
2	File Hash (SHA-256)	877c0907e1d644b1ea15c6835d2e4dce20534519755fb28a3e2f0d4dfcdde2b5
3	File Hash (SHA-256)	644548d2a7e61ced03b85cb364b71350362a7ee0a396cd683247d2dcdd827dfc
4	File Hash (SHA-256)	99f0eed78f3ddb507e3158b317f1d29c371752ab5a4e759049cdf5470eeb314e
5	File Hash (SHA-256)	a186ca8c36b068cf2bb786fb6672199924eb874bd10633a1f39c678345554064
6	File Hash	7924d9136fd2c9b582588792426f48793e1e4d4191979a8809d9

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

	(SHA-256)	2769c99738ac
7	File Hash (SHA-256)	0f00f547f3779071f6c2cfec7df9da8d83021f53dc2883b1d4beeef589e8b345
8	File Hash (SHA-256)	cd18dd71e679b82fd6f70d0f11c36976edb0220e55bc405dfb90094a9100a2e7
9	File Hash (SHA-256)	d73511a09b076541cca395a772084a1654bdcee2e095399adbfa813173229680
10	File Hash (SHA-256)	e50a2206c8fc400f33741c70044faaf894b532d36678213731b30a26fbbe9210

Примечание: Смотреть подробный отчет T-Lab в Приложении 7

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 329136 событий контроля операций с данными. Диапазон наблюдения по выгрузке: 01.04.2026 00:01 - 30.04.2026 21:18. Наиболее активные пользователи: User@DESKTOP-8A0IELC, HP@AUEZ-PC-0110, УНБ@DESKTOP-KERVJRP, Meirzhan Zhumakhanov, Ben@DESKTOP-OSN7JUO. Основные приложения: Google Chrome (chrome.exe), Microsoft Word (WINWORD.EXE), Проводник (explorer.exe), Microsoft Excel (EXCEL.EXE), Firefox (firefox.exe). Совокупный объем передачи данных составил 1,2 ТБ; отдельно выделены веб-риски, операции передачи данных и служебная активность приложений. Заметная часть DLP-активности пришлась на веб-направление: 30200 событий веб-активности. Передача данных преимущественно фиксировалась по каналам: Копировать, Переместить, Печать. По доступной выгрузке Safetica наблюдаемая активность покрывает диапазон 01.04.2026 00:01 - 30.04.2026 21:18. Подробная выгрузка Safetica приведена в Приложении 8.

6.4.1. Анализ веб – активности

В отчётном периоде по направлению веб-активности зарегистрировано 30200 событий. Преобладающие категории веб-ресурсов: Веб-приложения для мгновенных сообщений, Веб-порталы, Внутренняя сеть, Инструменты ИИ, Досуг. Наибольшая активность наблюдалась по ресурсам web.whatsapp.com, almaty.qujat.gov.kz, eotinish.gov.kz, 10.61.140.66,

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

chatgpt.com. В перечень объектов, требующих дополнительной проверки, вошли almaty.qujat.gov.kz, eotinish.gov.kz, chatgpt.com. Такая детализация используется для разграничения рабочей веб-активности, облачных сервисов и ресурсов с повышенным DLP-риск-профилем.

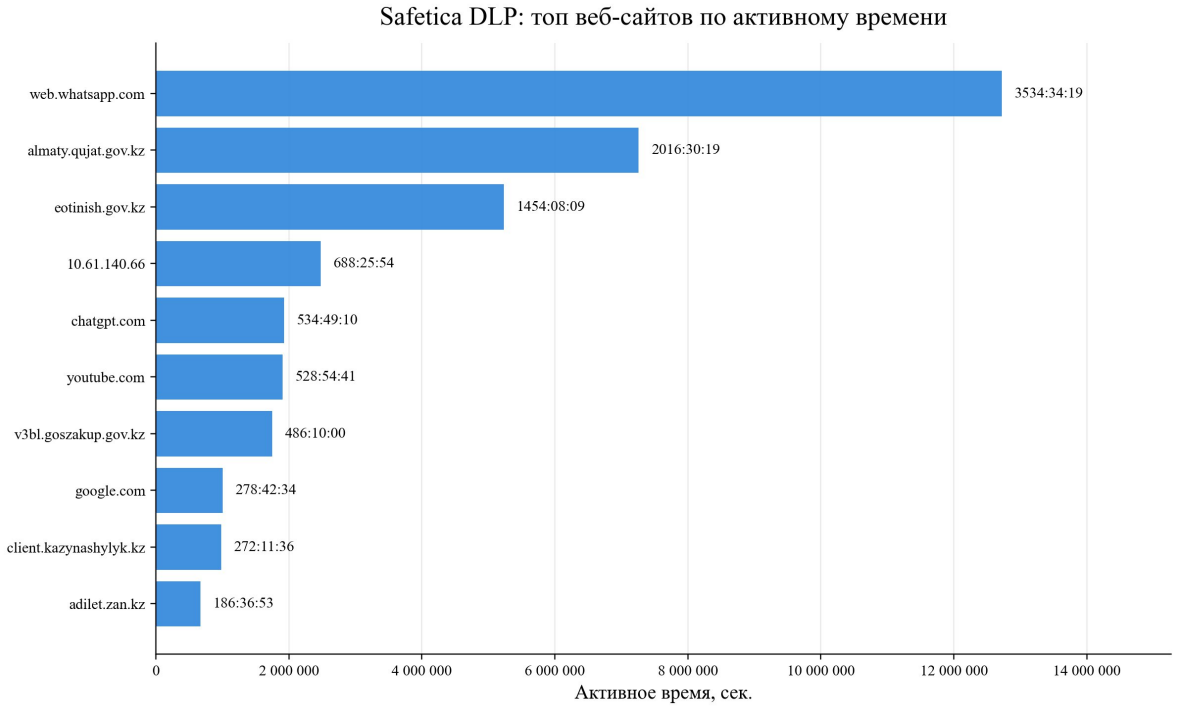

Рисунок 15. Веб-сайты

На диаграмме веб-активности показаны ресурсы, на которых пользователи провели наибольшее суммарное активное время в течение отчетного периода. Лидирующий ресурс: web.whatsapp.com с активным временем 3534:34:19 и охватом 345 пользователей. Также в верхней части выборки представлены almaty.qujat.gov.kz и eotinish.gov.kz, что позволяет увидеть не только единичный максимум, но и общий профиль наиболее используемых веб-направлений. Длина полосы отражает суммарное активное время по ресурсу, а подписи рядом с элементами диаграммы показывают конкретные значения времени. Рисунок отображает верхнюю часть выборки Safetica по веб-активности и не включает все посещенные ресурсы за месяц. Данные на рисунке связаны с таблицей ниже: диаграмма дает визуальное сравнение, а таблица раскрывает категории и количество пользователей по тем же объектам.

В числовой расшифровке веб-ресурсы представлены в виде рабочего перечня для анализа: указаны название ресурса, категория, суммарное активное время и количество пользователей. Категория помогает понять функциональный тип ресурса, активное время показывает интенсивность использования, а количество пользователей позволяет отличать массовую активность от индивидуальных отклонений. Порядок строк соответствует убыванию активности: в верхней части находятся ресурсы с наибольшим активным временем. В отличие от диаграммы, таблица содержит не только название ресурса и время, но и дополнительный контекст по категории и

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

охвату пользователей. Такая структура показывает, какие веб-ресурсы сформировали основную часть наблюдаемой веб-активности в Safetica за отчетный период.

Таблица 9. Топ веб-ресурсов по активному времени пользователей

№	Веб-ресурс	Категория	Активное время	Пользователи
1	web.whatsapp.com	Веб-приложения для мгновенных сообщений	3534:34:19	345
2	almaty.qujat.gov.kz	Веб-порталы	2016:30:19	189
3	eotinish.gov.kz	Веб-порталы	1454:08:09	158
4	10.61.140.66	Внутренняя сеть	688:25:54	96
5	chatgpt.com	Инструменты ИИ	534:49:10	262
6	youtube.com	Досуг	528:54:41	208
7	v3bl.goszakup.gov.kz	Правительство, закон и религия	486:10:00	84
8	google.com	Поисковые системы	278:42:34	338
9	client.kazynashylyk.kz	Не установлено	272:11:36	33
10	adilet.zan.kz	Не установлено	186:36:53	202

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

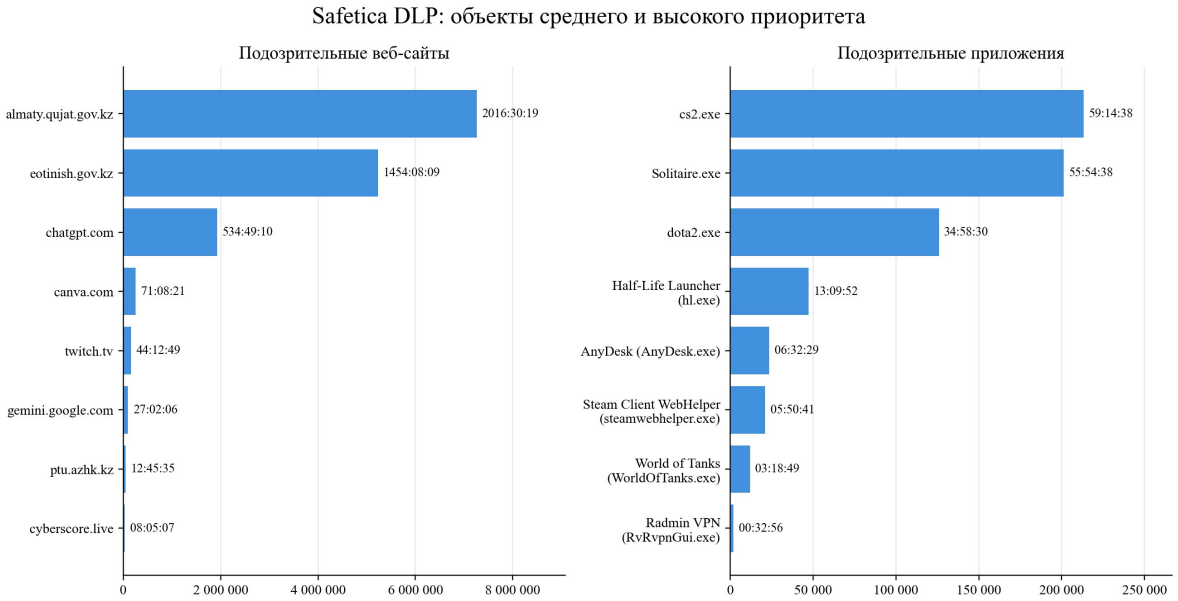

Рисунок 16. Средний и высокий степень важности

На диаграмме средней и высокой степени важности объединены веб-сайты и приложения, которые Safetica отнесла к соответствующим категориям в выгрузке. Наиболее заметные объекты в текущей выборке: веб-ресурс almaty.qujat.gov.kz и приложение cs2.exe. В левой части рисунка представлены подозрительные веб-сайты, в правой части - подозрительные приложения. Для каждого объекта отображается активное время, а также дополнительная информация о категории и количестве пользователей, если она присутствует в выгрузке. Диаграмма показывает верхнюю часть списка объектов средней и высокой степени важности и используется в отчете как визуальная сводка по наиболее заметным элементам этого раздела.

В перечне объектов средней и высокой степени важности данные разделены по типу объекта: отдельно отражаются веб-сайты и приложения. Для каждого объекта указаны категория, активное время и количество пользователей, поэтому таблица позволяет понять не только факт попадания в риск-зону, но и масштаб распространения активности. Колонка 'Тип' показывает, относится ли строка к веб-сайту или приложению, колонка 'Объект' содержит имя сайта или процесса, а последующие колонки раскрывают категорию, активное время и охват пользователей. Таблица дополняет диаграмму выше тем, что сохраняет значения в структурированном виде и позволяет видеть все отобранные объекты в одном списке. Содержание таблицы соответствует данным Safetica за отчетный период и не является перечнем всех событий DLP.

Таблица 10. Объекты Safetica среднего и высокого приоритета

№	Тип	Объект	Категория	Активное время	Пользователи
1	Веб-сайт	almaty.qujat.gov.k	Веб-	2016:30:1	189

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

		z	порталы	9	
2	Веб-сайт	eotinish.gov.kz	Веб-порталы	1454:08:09	158
3	Веб-сайт	chatgpt.com	Инструменты ИИ	534:49:10	262
4	Веб-сайт	canva.com	Инструменты ИИ	71:08:21	26
5	Веб-сайт	twitch.tv	Финансовый	44:12:49	2
6	Веб-сайт	gemini.google.com	Инструменты ИИ	27:02:06	30
7	Веб-сайт	ptu.azhk.kz	Веб-порталы	12:45:35	13
8	Веб-сайт	cyberscore.live	Финансовый	08:05:07	1
9	Приложение	cs2.exe	Кейлоггер	59:14:38	3
10	Приложение	Solitaire.exe	Игры	55:54:38	11
11	Приложение	dota2.exe	Игры	34:58:30	1
12	Приложение	Half-Life Launcher (hl.exe)	Игры	13:09:52	13
13	Приложение	AnyDesk (AnyDesk.exe)	VPN клиент	06:32:29	37
14	Приложение	Steam Client WebHelper (steamwebhelper.exe)	Игры	05:50:41	18
15	Приложение	World of Tanks (WorldOfTanks.exe)	Игры	03:18:49	1

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

16	Приложение	Radmin VPN (RvRvpnGui.exe)	VPN клиент	00:32:56	3

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) (≈1,0 ТБ), что обусловлено активной работой пользователей с файловой системой и сетевыми ресурсами. Существенную долю также занимают веб-браузеры (Google Chrome (chrome.exe), Firefox (firefox.exe) и Microsoft Edge (msedge.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.

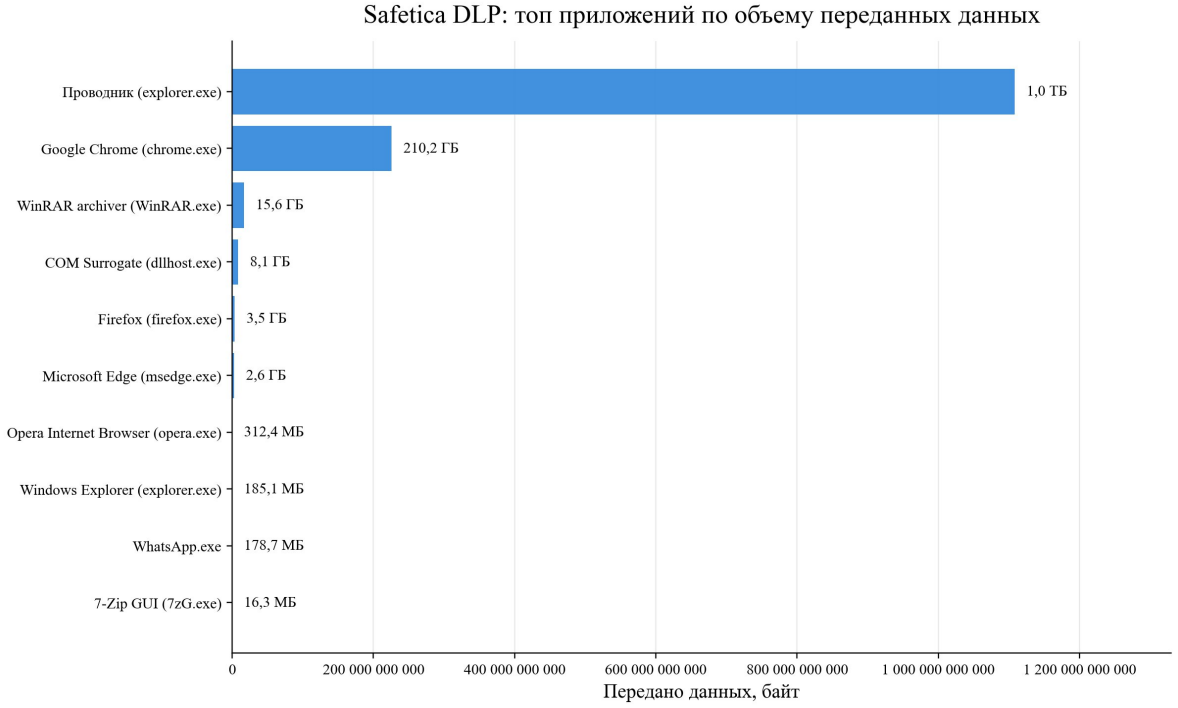

Рисунок 17. Топ-10 приложений

На диаграмме передачи данных показаны приложения, сформировавшие основной объем операций с данными в отчетном периоде. Лидирующее приложение: Проводник (explorer.exe) с объемом 1,0 ТБ; далее в верхней части выборки находятся Google Chrome (chrome.exe) и WinRAR archiver (WinRAR.exe). По горизонтальной оси отражен объем переданных данных, а по вертикальной - приложения из верхней части выборки. Длина полосы показывает относительный вклад приложения в общий объем передачи среди

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

отображенных объектов. Рисунок описывает распределение объема по приложениям и связан с таблицей ниже, где для тех же приложений дополнительно указаны категория, средний объем в активный день и количество пользователей.

В детализации передачи данных диаграмма раскрывается до уровня конкретных приложений: по каждой строке указаны категория, общий объем передачи, средний объем в активный день и количество пользователей. Совокупный объем передачи за период составил 1,2 ТБ, поэтому таблица используется как основа для оценки того, какие процессы реально формируют основную нагрузку на DLP. Общий объем показывает суммарный размер операций за месяц, средний объем в активный день показывает усредненное значение только по дням активности, а количество пользователей показывает охват приложения. Таблица содержит числовую расшифровку диаграммы и позволяет видеть не только порядок приложений по объему, но и дополнительные поля, отсутствующие на рисунке. Все значения приведены в агрегированном виде по отчетному периоду.

Таблица 11. 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	1,0 ТБ	34,4 ГБ	351
2	Google Chrome (chrome.exe)	Веб-браузер	210,2 ГБ	7,0 ГБ	342
3	WinRAR archiver (WinRAR.exe)	Не указано	15,6 ГБ	727,3 МБ	32
4	COM Surrogate (dllhost.exe)	Не указано	8,1 ГБ	359,1 МБ	37
5	Firefox (firefox.exe)	Веб-браузер	3,5 ГБ	149,0 МБ	81
6	Microsoft	Веб-браузер	2,6 ГБ	97,2 МБ	88

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

	Edge (msedge.exe)				
7	Opera Internet Browser (opera.exe)	Не указано	312,4 МБ	26,0 МБ	4
8	Windows Explorer (explorer.exe)	Не указано	185,1 МБ	61,7 МБ	1
9	WhatsApp.exe	Мгновенные сообщения и интернет-телефония (VOIP)	178,7 МБ	8,1 МБ	10
10	7-Zip GUI (7zG.exe)	Не указано	16,3 МБ	5,4 МБ	1

6.4.3. Служебные операции через интернет и внутренние сервисы

По служебным операциям и активности приложений зарегистрировано 936445 событий. Наибольшая активность отмечалась в приложениях Google Chrome (chrome.exe), Microsoft Word (WINWORD.EXE), Проводник (explorer.exe), Microsoft Excel (EXCEL.EXE), Firefox (firefox.exe). Максимальное активное время пользователя за период: User@DESKTOP-8A0IELC - 294:21:11; доля подозрительной активности по данному пользователю составила 0.0%. Полученные значения используются для приоритизации ручной проверки пользователей и уточнения исключений DLP-политик.

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

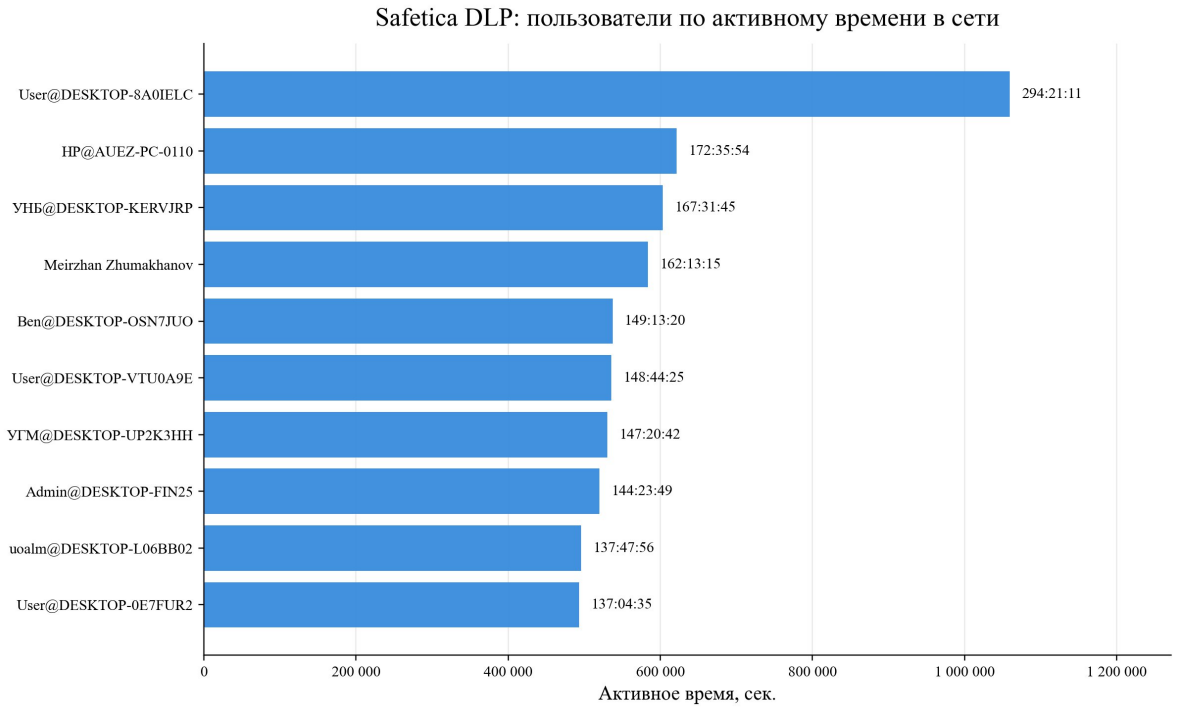

Рисунок 18. Время нахождения пользователя в сети

На диаграмме пользовательской активности показаны пользователи с максимальным суммарным временем работы в сети за отчетный период. Лидирующий пользователь: User@DESKTOP-8A0IELC с активным временем 294:21:11; также в верхней части выборки находятся HP@AUEZ-PC-0110 и УНБ@DESKTOP-KERVJRP. Длина полосы соответствует общему активному времени пользователя, рассчитанному по данным Safetica. Рисунок показывает верхнюю часть выборки пользователей по сетевой активности и визуально сравнивает значения между ними. Подробные числовые значения по активным дням, подозрительной активности и доле подозрительной активности приведены в таблице ниже.

В детализации сетевой активности по пользователям приведены активные дни, общее активное время, время подозрительной активности и ее доля. Колонка 'Активные дни' показывает, в течение скольких дней пользователь был представлен в наблюдаемой активности, а колонка 'Общее активное время' отражает суммарную длительность. Отдельно показано время подозрительной активности и его процентная доля относительно общей активности пользователя. Таблица дополняет диаграмму тем, что переводит визуальное сравнение пользователей в числовой формат и показывает дополнительные показатели, которые не помещаются на рисунке.

Таблица 12. Сетевая активность пользователя

№	Пользователь	Активные дни	Общее активное время	Подозрительная активность	Доля подозрительной активности

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

1	User@DESKTOP-8A0IELC	24	294:21:11	00:04:25	0.0%
2	HP@AUEZ-PC-0110	23	172:35:54	00:22:59	0.2%
3	УНБ@DESKTOP-KERVJRP	22	167:31:45	00:37:07	0.4%
4	Meirzhan Zhumakhanov	22	162:13:15	00:05:06	0.1%
5	Ben@DESKTOP-OSN7JUO	23	149:13:20	00:00:15	0.0%
6	User@DESKTOP-VTU0A9E	27	148:44:25	02:35:30	1.7%
7	УГМ@DESKTOP-UP2K3HH	23	147:20:42	00:05:13	0.1%
8	Admin@DESKTOP-FIN25	24	144:23:49	01:05:48	0.8%
9	uoalm@DESKTOP-L06BB02	23	137:47:56	00:01:01	0.0%
10	User@DESKTOP-0E7FUR2	25	137:04:35	00:00:10	0.0%

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 16 127 725 срабатываний защитных механизмов, в том числе Anti-Bot - 8 353 306, Anti-Virus - 5 473 737, IPS - 2 300 682. Наибольшая активность наблюдалась на шлюзе GW-NAURYZBAY.

Таблица 13. Зафиксированный активность в Межсетевом экране

№	Категория	Показатель	Значение
1	Общие события безопасности	Anti-Bot события	8 353 306
2	Общие события	Anti-Virus	5 473 737

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

	безопасности	события	
3	Общие события безопасности	IPS-инциденты	2 300 682

Анализ сетевой активности показывает преобладание приложений удалённого доступа, обмена файлами и проксирующих сервисов. Наиболее заметная нагрузка пришлась на приложение BitTorrent Protocol (сессии - 9 574 012, трафик - 153,1 ГБ). Основные категории сетевой активности: P2P File Sharing, Critical Risk, Remote Administration, Anonymizer, File Storage and Sharing. Указанные показатели требуют периодической проверки на предмет соответствия деловым задачам пользователей.

Таблица 14. Сетевая активность

№	Приложение	Сессии	Трафик
1	BitTorrent Protocol	9 574 012	153,1 ГБ
2	ZeroTier One	603 583	227,8 МБ
3	AnyDesk	151 122	708,1 МБ
4	MediaGet	58 265	597,5 МБ
5	uTorrent	40 568	83,5 МБ
6	TeamViewer	12 675	334,2 МБ
7	VeePN	7 264	69,6 МБ
8	BitTorrent Sync	6 625	12,9 МБ
9	Radmin VPN	1 677	2,4 МБ
10	Perfect Dark	1 241	407,8 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, Cryptominer.TC.9e2cUoIa, Swift.TC.e7e0XsOZ, что указывает на постоянный фон сетевых угроз в адрес инфраструктуры. Признаков массового заражения по итогам отчётного периода не выявлено.

Таблица 15. Заблокированный ВПО

№	Вредоносное ПО	События
1	PUA.TC.3626Wodp	832

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

2	Cryptominer.TC.9e2cUoIa	700
3	Swift.TC.e7e0XsOZ	622
4	Infecting_URL.ME.RS.TC.530drvMW	601
5	Generic.TC.5d3djpnb	527
6	Infecting_URL.VUP.RS.TC.c5edmXPX	259
7	Infecting_URL.UF.RS.TC.7d6enwyz	209
8	Trojan.Linux.RubyMiner.B	197
9	Generic.TC.f355Nkqa	192
10	Phorpiex.TC.6860TADZ	165

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.

Таблица 16. Система предотвращения вторжений

№	Тип события	Сессии
1	Microsoft Windows NT Null CIFS Sessions	943 459
2	TCP Segment Limit Enforcement	837 638
3	Max Ping Size	412 317
4	TCP Invalid Retransmission	86 799
5	Command Injection	13 140
6	ZMap Security Scanner	2 084
7	GnuTLS DistinguishedName Decoding Double Free	1 242
8	Non Compliant IKE	511

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

9	Sensitive Configuration File Disclosure	404
10	SQL Injection	401

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.
Количество объектов мониторинга и состав обслуживаемой инфраструктуры формировались на основании сведений и перечней активов, предоставленных Заказчиком на этапе реализации проекта. В случае наличия дополнительных объектов инфраструктуры, не включенных в ранее переданные перечни, Исполнитель готов выполнить актуализацию состава обслуживаемых активов и обеспечить их подключение к сервисам мониторинга после получения актуализированного реестра серверного, сетевого и пользовательского оборудования.

В части контроля привилегированного доступа мероприятия по внедрению соответствующего решения требуют предварительного согласования технической архитектуры, перечня защищаемых систем, схем интеграции и порядка эксплуатации. Исполнителем выполнены подготовительные мероприятия по реализации указанного требования; дальнейшие этапы зависят от согласования архитектуры и ответственных владельцев систем.

По вопросу обучения работников Заказчика Исполнителем проведена дополнительная проверка комплектности отчетных материалов. 17 февраля 2026 года в адрес Заказчика было направлено письмо за исходящим №77 о готовности проведения обучения и согласовании графика. Исполнитель подтверждает готовность провести обучение в согласованное с Заказчиком время после определения даты и времени проведения.

Процессы обеспечения информационной безопасности в рамках оказываемых услуг выполняются в соответствии с условиями Договора и Технической спецификации. В рабочем комплекте материалов отражены сведения по процессам управления доступом, управления активами, управления изменениями, резервного копирования, обеспечения непрерывности

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

деятельности и иным процессам, предусмотренным Технической спецификацией.

8. ВЫВОДЫ И РЕКОМЕНДАЦИИ

8.1. Общие выводы

На отдельных шлюзах фиксировалось использование приложений удалённого доступа, VPN и P2P-обмена, включая BitTorrent Protocol, ZeroTier One, AnyDesk. Выявленные вредоносные объекты своевременно блокировались средствами Check Point; наиболее часто встречались PUA.TC.3626Wodp, Cryptominer.TC.9e2cUoIa, Swift.TC.e7e0XsOZ. IPS фиксировала типовые сценарии сетевого воздействия, при этом признаков успешной эксплуатации уязвимостей не выявлено. Под мониторингом находилось 641 узлов; offline - 289, нестабильных/требующих проверки - 52. За отчетный период зарегистрировано 1487 событий уровня high/critical; основной вклад внесло правило «First Time Seen Removable Device». По данным Nessus в отчётном периоде сохраняются 41 критических и 81 высоких уязвимостей.
По замечанию об объектах в статусе offline отмечается, что данный статус отражает техническое состояние подключения источников событий на момент формирования отчета. Мониторинг осуществлялся по всем источникам, которые были подключены и фактически передавали события в контур SIEM/EDR; расширение охвата инфраструктуры продолжается по мере выполнения организационно-технических мероприятий и получения необходимых доступов.

По замечанию о полноте охвата инфраструктуры состав объектов мониторинга сформирован на основании перечней активов, предоставленных Заказчиком. Для подключения дополнительных объектов требуется актуализированный реестр инфраструктуры, после чего такие активы могут быть включены в контур обслуживания и мониторинга.

По замечанию о критических уязвимостях в отчете отражены результаты выявления, анализа и подготовки рекомендаций. Исполнитель обеспечивает регулярное сканирование и доведение рекомендаций до Заказчика, при этом непосредственное устранение уязвимостей на объектах Заказчика выполняется владельцами информационных систем и ответственными администраторами Заказчика.

8.2. Приоритетные планы работ

Продолжить актуализацию и оптимизацию правил корреляции в SIEM с учётом выявленных сценариев, повторяющихся срабатываний и особенностей инфраструктуры Заказчика. Усилить контроль полноты

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000195576CDEC2

телеметрии от агентов, качества интеграций между системами защиты и своевременного подключения источников, фактически передающих события в контур мониторинга.
По направлению управления уязвимостями продолжить регулярное сканирование внутреннего и внешнего периметра, подготовку рекомендаций по устранению выявленных критических и высоких уязвимостей, а также контроль повторной проверки после выполнения работ ответственными владельцами систем и администраторами Заказчика. Непосредственное устранение уязвимостей на объектах Заказчика выполняется ответственными администраторами в пределах их полномочий и доступа.

Для дальнейшего закрытия организационных замечаний необходимо выполнить сверку актуального реестра активов, согласовать архитектуру контроля привилегированного доступа, определить дату обучения работников Заказчика и продолжить документальное подтверждение процессов управления доступом, активами, изменениями, резервным копированием и непрерывностью деятельности.

По направлению Check Point NGFW продолжить контроль и актуализацию политик межсетевого экрана с акцентом на risky applications, VPN, P2P-категории и приложения удаленного администрирования. Дополнительно требуется перепроверить необходимость использования BitTorrent Protocol, ZeroTier One, AnyDesk, OpenVPN и аналогичных приложений в инфраструктуре Заказчика.

8.3. Рекомендации

Заказчику рекомендуется предоставить актуализированный перечень серверного, сетевого и пользовательского оборудования для сверки состава обслуживаемых активов и дальнейшего расширения охвата мониторингом. Отдельно рекомендуется обеспечить своевременный ввод рабочих станций в домен после переустановки операционной системы и определить порядок модернизации либо замены устаревших ОС, на которых установка или стабильная работа EDR-агента ограничена.
По направлению мониторинга и реагирования рекомендуется продолжить контроль источников, фактически передающих события в SIEM/EDR, актуализацию правил корреляции, проверку offline/unhealthy агентов и сверку состояния политик на проблемных хостах. Для повторяющихся сценариев DriveMgr.exe, AnyDesk.exe, KMS-R@1nHook.exe и аналогичных процессов рекомендуется сохранять связку SOC-анализа, уведомления ответственных администраторов, очистки хостов и последующей контрольной проверки.

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

По направлению управления уязвимостями рекомендуется продолжить регулярное сканирование внутреннего и внешнего периметра, передачу рекомендаций владельцам систем, контроль сроков устранения и повторную проверку после выполнения работ ответственными администраторами Заказчика. Критические и высокие уязвимости должны устраняться владельцами информационных систем с учетом полномочий, доступов и регламентов эксплуатации.

По направлению контроля привилегированного доступа рекомендуется согласовать техническую архитектуру PAM, перечень защищаемых систем, схемы интеграции и порядок эксплуатации решения. После согласования указанных параметров необходимо определить этапы внедрения и ответственных владельцев процесса.

По направлению обучения работников Заказчика рекомендуется определить дату и время проведения обучения по вопросам информационной безопасности с учетом ранее направленного письма Исполнителя от 17 февраля 2026 года за исходящим №77 о готовности проведения обучения и согласовании графика.

По направлению процессов обеспечения информационной безопасности рекомендуется продолжить документальное подтверждение процессов управления доступом, управления активами, управления изменениями, резервного копирования, обеспечения непрерывности деятельности и иных процессов, предусмотренных Технической спецификацией.

По направлению Check Point NGFW рекомендуется продолжить контроль и актуализацию политик межсетевого экрана с акцентом на risky applications, VPN, P2P-категории и приложения удаленного администрирования. Необходимо перепроверить необходимость использования BitTorrent Protocol, ZeroTier One, AnyDesk, OpenVPN и аналогичных приложений в инфраструктуре Заказчика.

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z120260000195576CDEC2
Тип документа	Исходящее письмо
Тема	Исправленный отчет. Ответ на исх. №50.3-50.04/329-И от 29.05.2026 г.
Статус	Доставлен
Рег. Номер:	01-01/203
Рег. Дата:	05.06.2026
Количество страниц	49
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	Заместитель Генерального директора
IP-адрес	109.163.197.162
Email	info@kazdream.kz
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWMwYJ...oK1+xlBQ=
Дата подписания	05.06.2026 10:59

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Заместитель Генерального директора
IP-адрес	109.163.197.162
Email	info@kazdream.kz
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWbAYJ...ocQMIWRQ=

Дата подписания 05.06.2026 11:00

DOC ID KZBW2Z120260000195576CDEC2

DOC ID KZBW2Z120260000195576CDEC2
Электронный документ подписан в Documentolog Business