ИСПОЛНИТЕЛЬ

Заместитель генерального директора

ТОО «MSSP.GL»

Р.С. Джансенгиров

_____

ЗАКАЗЧИК

Заместитель руководителя КГУ «Управления цифровизации города Алматы»

М.А. Дюсюков

_____

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

Акимат города Алматы

Отчетный период: с 01.06.2026 г. по 30.06.2026 г.

DOC ID KZBW2Z120260000201301F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

Оглавление

1. ОБЩАЯ ИНФОРМАЦИЯ 4
1.1. Ключевые показатели эффективности 4
1.2. Цель отчета 4
1.3. Область действия 4
2. Матрица соответствия структуре технической спецификации 5
3. Журналирование, сбор, хранение и передача журналов регистрации событий 13
3.1. Состояние агентов 14
3.2. Настройка и актуализация представлений данных (Data Views) 14
3.3. Усиление мониторинга и анализа событий через SIEM-систему 15
4. Уведомления, регистрация и обработка инцидентов, SLA реагирования 16
4.1. Статистика событий безопасности 18
4.2. Система уведомлений 23
4.3. Поиск угроз 29
4.4. Доступность веб-интерфейса 30
4.5. Автоматическое реагирование на угрозы 30
5. Аудит ИБ и обследование объекта на соответствие требованиям ТД/ИБ 30
6. Управление уязвимостями, сканирования, рекомендации и повторный контроль 31
6.1. Инструментальное сканирование 31
6.2. Статистика управления уязвимости 33
7. План непрерывности, восстановление деятельности, резервное копирование 36
8. Регламенты, SLA, планы работ и порядок взаимодействия 36
9. MDR, доступность услуги, поддержка и обработка событий 38
10. Контроль привилегированного доступа и/или bastion/PAM 38
11. Обучение работников Заказчика по вопросам ИБ 39
12. Процессы обеспечения ИБ: доступы, активы, уязвимости, обновления, резервирование, инциденты, изменения 39
13. Сетевая архитектура, сегментация, рекомендации по оптимизации/перепроектированию 39
14. Функции NGFW / Check Point 41
14.1. Checkpoint - межсетевой экран 46
15. Централизованное управление учетными записями и доступом / AD 48
16. SOAR: сценарии, playbook, интеграции, журнал действий, RBAC, TLS 49
17. Кибербразведка, IOC, запросы и рекомендации 54
17.1. OpenCTI — Платформа кибербразведки 54
17.2. MISP — Обмен индикаторами компрометации 55
17.3. T-Lab Sandbox — Защита от таргетированных атак 57
18. Система защиты конфиденциальных данных от утечки (DLP) 62
18.1. DLP – Предотвращение утечек данных (safetica) 62
18.2. Анализ веб – активности 63
18.3. Передачи данных 67

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

18.4. Служебные операции через интернет и внутренние сервисы.....70
19. Перечень приложений и подтверждающих материалов.....72
20. Отдельные подтверждающие документы.....72
21. Выводы и рекомендации.....74
21.1. Общие выводы.....75
21.2. Приоритетные планы работ.....75
21.3. Рекомендации.....75

DOC ID KZBW2Z120260000201301F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

1. ОБЩАЯ ИНФОРМАЦИЯ

Настоящий отчет представляет результаты оказания услуг по обеспечению информационной безопасности для Акимата города Алматы (далее - Заказчик) за отчетный период с 01.06.2026 года по 30.06.2026 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 отчетном периоде в SIEM зарегистрировано 16 796 событий безопасности, по которым обработано 34 кейса. Защита конечных точек обеспечивалась на 693 активных узлах (защита активна на 372), средствами EDR предотвращено 173 вредоносных действия. Через T-Lab Sandbox проверено 13 186 файлов/объектов, выявлено 257 угроз. По результатам сканирования Nessus обнаружены 41 критическая уязвимость и 157 уязвимостей высокого уровня критичности. В системе Safetica зафиксировано 252 494 событий контроля данных и 481 901 операция передачи данных. Средствами Check Point выполнено 13 345 760 блокировок.

Настоящая редакция отчета дополнительно приведена к структуре Технической спецификации и скорректированного проекта письма от 12.06.2026.

Настоящий отчет подготовлен в соответствии с пунктом 4.5 технической спецификации на услуги по обеспечению информационной безопасности и охватывает период с 01.06.2026 года по 30.06.2026 года.

1.2. 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.

1.3. Область действия

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

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

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

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.

2. Матрица соответствия структуре технической спецификации

Матрица построена по скорректированному проекту письма и показывает, какими разделами отчета, приложениями или отдельными документами подтверждаются пункты Технической спецификации.

Таблица 1. Пункты Технической спецификации и подтверждающие материалы

№	Пункт ТС	Требование / блок	Подтверждающие документы и материалы	Статус / комментарий
1	1.1.2, 1.1.23-1.1.26	Журналирование, сбор, хранение и передача журналов регистрации событий	Отчет: Приложение 1 «Правила корреляции»; Приложение 2 «Перечень обработанных инцидентов (кейсов)»; Приложение 3 «Проанализированные программы в рамках мониторинга»; эксплуатационные выгрузки Elastic SIEM/EDR; Правила по мониторингу событий и управлению инцидентами; Политика ИБ; выгрузка Elastic ILM/data streams/indices от 13.06.2026.	Операционная часть и хранение журналов в Elastic подтверждаются отчетными материалами SOC/MDR и административной выгрузкой Elastic: кластер в состоянии green, выявлено 39 ILM-политик, 211 data streams и 867 индексов; для основной политики logs указан жизненный цикл с хранением до 1095 дней. Порядок передачи архивов журналов, конфигураций

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

				и данных Заказчику по завершении контракта должен быть дополнительно закреплен отдельным техническим приложением или актом передачи.
2	1.1.4-1.1.5, 3.9, 3.13-3.14, 6.1-6.9	Уведомления, регистрация и обработка инцидентов, SLA реагирования	Отчет: разделы 4.1-4.5; Приложение 2; Правила по мониторингу событий и управлению инцидентами; журнал кейсов и уведомлений; регламентные материалы по реагированию.	Закрыто по отчетному периоду: подтверждены регистрация, обработка кейсов, уведомления и порядок реагирования. При необходимости может отдельно прикладываться детализация уведомлений с датой, адресатом, категорией события, статусом и временем реакции.
3	1.1.22, 3.1-3.7	Аудит ИБ и обследование объекта на соответствие требованиям ТД/ИБ	Правила проведения внутреннего аудита ИБ; Методика оценки рисков ИБ; Политика ИБ; отчетные	В ноябре 2025 года ежегодный аудит ИБ проведен; результаты направлены Заказчику исх.

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

			материалы по операционному контролю; график проведения аудита ИБ, подлежащий согласованию с Заказчиком. Приложение 9 «Статус реализации»; исх. №607 от 21.11.2025 (Отчет по аудиту ИБ).	№607 от 21.11.2025. Аудит ИБ 2026 года на стадии согласования плана-графика. Согласно ТС аудит ИБ проводится не менее одного раза в год, продолжительность — не более 90 рабочих дней с момента начала работ по аудиту.
4	1.1.19-1.1.21, 13.1-13.16	Управление уязвимостями, сканирования, рекомендации и повторный контроль	Отчет: раздел 5; Приложение 4 «Статистика уязвимостей»; Приложение 5 «Сканирование внутренней сети»; Приложение 6 «Сканирование внешней сети»; выгрузки Nessus; Методика оценки рисков ИБ; Каталог угроз.	Закрыто по отчетному периоду: представлены результаты сканирования, статистика уязвимостей, и методическая база оценки рисков. Повторный контроль устранения подтверждается результатами последующих сканирований и remediation-register.
5	1.1.30, 2.1, 9.1	План непрерывности, восстановление деятельности, резервное копирование	Правила по обеспечению непрерывной работы активов; Правила резервного	Документальная часть закрыта: определены требования к непрерывности

DOC ID KZBW2Z1202600002013O1F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z1202600002013O1F66B3

			копирования и восстановления информации; Руководство администратора по сопровождению объекта информатизации; Политика ИБ.	, резервному копированию и восстановлению. Фактическое проведение тестов восстановления, RTO/RPO и результаты контрольного восстановления должны подтверждаться отдельным актом или журналом тестирования.
6	1.2.2, 1.2.7-1.2.8, 5.1	Регламенты, SLA, планы работ и порядок взаимодействия	Политика ИБ; комплект ТД ИБ; Регламент взаимодействия; План-график работ; Диаграмма Ганта; Договор и Техническая спецификация; письма о плановых технических работах и организационном взаимодействии.	Закрыто организационно-регламентным комплектом: порядок взаимодействия, планирование работ, технические документы по ИБ и уведомления Заказчика подтверждают выполнение процессной части требований.
7	3.14.1-3.14.4, 10.1	MDR, доступность услуги, поддержка и обработка событий	Отчет: разделы 3 - 4; Приложения 1-3; Правила по мониторингу	Закрыто по отчетному периоду: подтверждены мониторинг,

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

			событий и управлению инцидентами; Политика ИБ; эксплуатационные выгрузки SIEM/EDR.	обработка событий, кейсы, уведомления, доступность сервиса и регламентная база управления инцидентами.
8	Раздел 7 / PAM	Контроль привилегированного доступа и/или bastion/PAM	Правила управления доступом, активами, обновлениями и изменениями; Правила организации процедуры аутентификации; сведения AD; матрица ролей и учетных записей в системах защиты при наличии.	Частично закрыто: общие требования к управлению доступом и аутентификации подтверждены ТД ИБ и AD-выгрузками. Отдельный контур PAM/bastion, журналы привилегированных сессий и архитектура PAM требуют самостоятельного подтверждающего комплекта, если данный пункт применим по ТС.
9	8.1-8.3	Обучение работников Заказчика по вопросам ИБ	Письмо/запрос по организации обучения сотрудников; ответные организационн	Частично закрыто организационно: подтверждается

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

			ые материалы Заказчика при наличии; программа обучения, список участников и ведомость/акт проведения после согласования.	инициирование процесса обучения, план-графика обучения и запрос участников исх.письмо №77 от 17.02.2026 г. Факт проведения обучения закрывается только после предоставления программы, списка участников и акта либо ведомости проведения.
10	9.1	Процессы обеспечения ИБ: доступы, активы, уязвимости, обновления, резервирование, инциденты, изменения	Политика ИБ; Правила управления доступом, активами, обновлениями и изменениями; Правила идентификации, классификации и маркировки активов; Правила резервного копирования и восстановления; Правила мониторинга событий и управления инцидентами;	Закрыто в части регламентной базы и отчетных процессов: доступы, активы, изменения, обновления, резервирование, инциденты и уязвимости описаны в ТД ИБ и подтверждаются отчетными материалами. Фактическое исполнение отдельных операций

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

			Приложение 9 «Статус реализации».	подтверждается эксплуатационными журналами владельцев процессов.
11	11.1-11.3	Сетевая архитектура, сегментация, рекомендации по оптимизации/перепроектированию	Отчет за июнь 2026 года, раздел 13; логические L3-схемы основной сети и удаленных управлений; раздел Check Point NGFW; эксплуатационные сведения по сетевым шлюзам и VPN-подключениям.	Закрыто: подтверждены сегментация основной сети и удаленных управлений, использование периметровых шлюзов Check Point, маршрутизация через L3-оборудование, VPN-связность и подключение к внешним операторам. По результатам анализа отражены рекомендации по межсегментному доступу, журналированию, резервированию каналов и контролю конфигураций.
12	12.1-12.20	Функции NGFW / Check Point	Отчет за июнь 2026 года, раздел 14; Таблица 7 «Функциональная матрица	Закрыто по функциональной матрице NGFW, эксплуатационным данным

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

			NGFW Check Point»; эксплуатационные данные Check Point Quantum Spark по 13 gateway; визуальные материалы интерфейса Quantum Spark; реестр лицензий Check Point по шлюзам Акимата.	Check Point, визуальным материалам Quantum Spark и реестру лицензий. Подтверждены ключевые функции: Firewall, IPS, Anti-Virus, Anti-Bot, URL Filtering/App Control, VPN, logging и role-based admins.
13	Раздел 14	Централизованное управление учетными записями и доступом / AD	Отчет за июнь 2026 года, раздел 15; эксплуатационная выгрузка Active Directory с доменного контроллера; сводка по учетным записям пользователей и компьютеров, группам безопасности, GPO, блокировкам и привилегированным группам.	Закрыто эксплуатационной проверкой AD: отражены учетные записи, компьютеры, группы, GPO, изменения за июнь, блокировки, отключенные объекты и состав привилегированных групп.
14	15.1-15.12	SOAR: сценарии, playbook, интеграции, журнал действий, RBAC, TLS	Отчет за июнь 2026 года, раздел 16; схема workflow Splunk SOAR; перечень playbook оркестрации и реагирования;	Закрыто: отражены использование Elastic SIEM/EDR совместно со Splunk SOAR, перечень playbook,

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

			сведения об интеграциях, RBAC/TLS и журналируемых автоматических действиях.	автоматизированный workflow, интеграции, ролевой доступ, TLS и эксплуатационный контур автоматизированного реагирования.
15	1.1.27, MISP/OpenCTI/АО "ГТС"	Киберразведка, IOC, запросы и рекомендации	Отчет за июнь 2026 года, разделы OpenCTI/MISP/T-Lab; Приложение 7 «Информация с системы защиты от целевых атак и атак нулевого дня»; сведения по IOC и аналитическим материалам; журнал запросов в АО «ГТС» при наличии обращений.	Работа с IOC и threat intelligence отражена в отчете. При наличии запросов в АО «ГТС» прикладывается отдельный журнал с датой, темой, рекомендациями и сроком ответа; при отсутствии запросов оформляется отметка «запросы не поступали».

3. Журналирование, сбор, хранение и передача журналов регистрации событий

Пункты ТС: 1.1.2, 1.1.23-1.1.26.

В данном разделе приведены материалы исходного отчета по состоянию агентов, представлениям данных Elastic и анализу событий SIEM/EDR. Операционная часть подтверждает сбор и обработку журналов. Параметры хранения журналов и порядок передачи архивов принимаются согласно требованиям Технической спецификации: хранение журналов регистрации событий не менее 3 лет и оперативный доступ не менее 2 месяцев. Детальные

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

параметры retention и порядок передачи архивов/конфигураций целесообразно закрепить отдельным техническим приложением.

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 отчетном периоде контроль состояния агентов EDR осуществлялся на 693 узлах, из которых защита была активна на 372 (53.68%). Выявлено 53 узла с признаками некорректной работы агентов и 268 узлов, находившихся вне связи. Статусы агентов: error - 53, offline - 268, online - 372. Наиболее затронутые хосты: desktop-llneh6f, nauz-pc-0007, desktop-mlq5rlg. Под мониторингом находилось 693 активных агента; offline - 268, нестабильных/требующих проверки - 53. Дополнительно вне активного парка: неактивных (давно не выходивших на связь) агентов - 415, снятых с учета - 48.

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. 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.

3.2. Настройка и актуализация представлений данных (Data Views)

В отчетном 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, .alerts-security.alerts-akimat, **, logs-*. Через указанные представления обеспечивался анализ событий по 51 правилам корреляции, 667 хостам и 218 учетным записям пользователей.

DOC ID KZBW2Z1202600002013O1F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

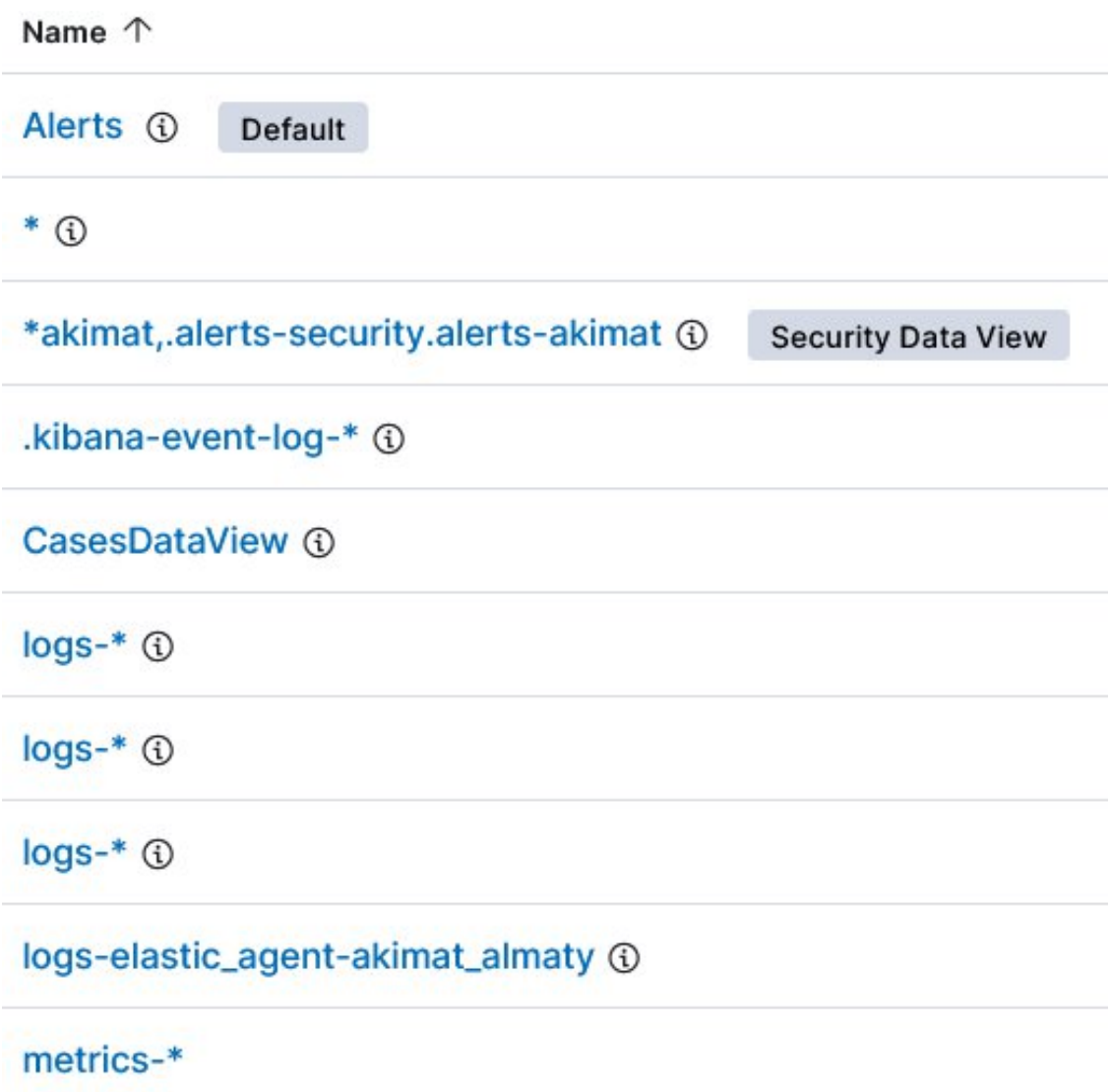


Рисунок 1. Состав представлений данных и рабочих источников Elastic

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.

3.3. Усиление мониторинга и анализа событий через SIEM-систему

За отчетный период в системе мониторинга обработано 16796 событий безопасности, в том числе critical - 41, high - 342, medium - 4585, low - 11828. Наиболее часто события фиксировались по правилам: System Service Discovery through built-in Windows Utilities, First Time Seen Removable Device, High Number of Process and/or Service Terminations. Всего в отчетном периоде срабатывания пришлись на 51 правило, 667 хостов и 218 пользователей. Наиболее затронутые хосты: desktop-llneh6f, nauz-pc-0007, desktop-mlq5rlg; пользователи: СИСТЕМА, akima, askhat.aldebayev. Детализация по ключевым правилам корреляции

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

показывает следующее: «System Service Discovery through built-in Windows Utilities» - 4 805 срабатываний (28.61%); Правило указывает на разведывательную активность внутри хоста и помогает выявлять подготовительные действия нарушителя. «First Time Seen Removable Device» - 1 973 срабатываний (11.75%); Правило фиксирует подключение или первое обнаружение съемных носителей и применяется для контроля несанкционированного переноса данных. «High Number of Process and/or Service Terminations» - 1 563 срабатываний (9.31%); Правило отражает попытки сокрытия следов или нарушения штатной работы защитных механизмов на конечной точке. «Process Termination followed by Deletion» - 1 497 срабатываний (8.91%); Правило отражает попытки сокрытия следов или нарушения штатной работы защитных механизмов на конечной точке. «Connection to Commonly Abused Web Services» - 1 003 срабатывания (5.97%); Правило предназначено для контроля сетевой активности и выявления нетиповых соединений либо коммуникаций с подозрительными узлами.

4. Уведомления, регистрация и обработка инцидентов, SLA реагирования

Пункты ТС: 1.1.4-1.1.5, 3.9, 3.13-3.14, 6.1-6.9.

Раздел содержит исходные материалы по мониторингу, кейсам, уведомлениям, поиску угроз, доступности SIEM и автоматическому реагированию. Для полного SLA-подтверждения отдельно прикладывается журнал уведомлений с временем обнаружения, временем уведомления, адресатом, категорией события и итоговым статусом.

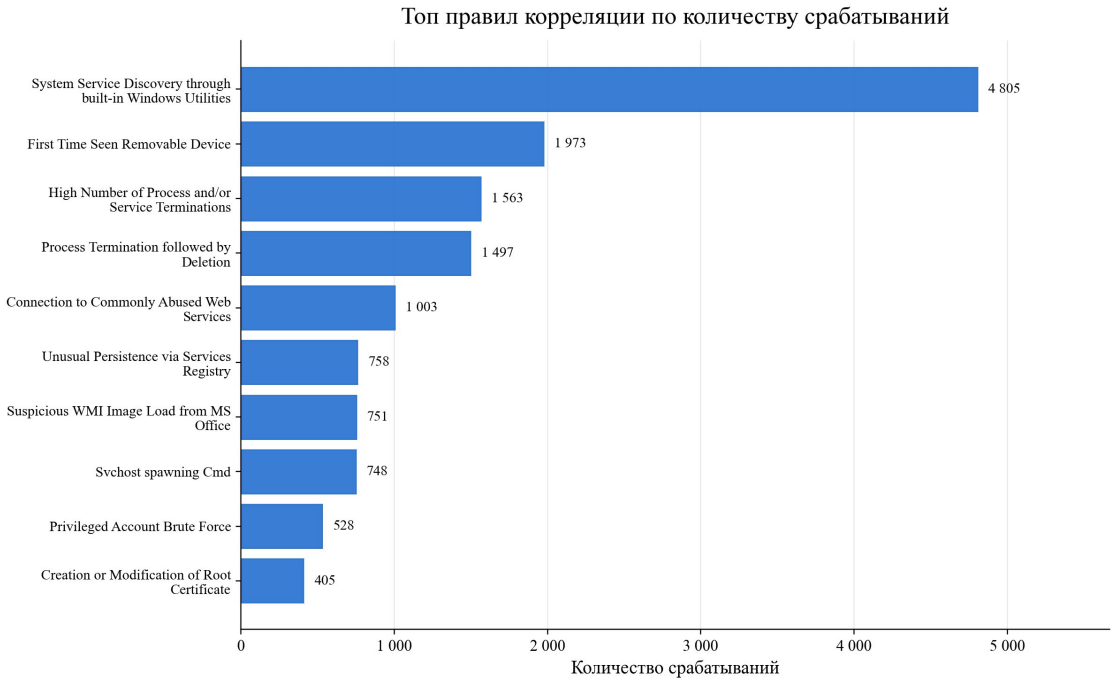


Рисунок 2. Топ правил корреляции по количеству срабатываний

На рисунке показаны корреляционные правила Elastic с наибольшим количеством срабатываний за отчетный период. Верхняя строка диаграммы соответствует правилу «System Service Discovery through built-in Windows

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Utilities» с количеством срабатываний 4 805. Всего в периоде срабатывания пришлись на 51 правило, 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 «System Service Discovery through built-in Windows Utilities» - 28.61%. Табличный формат дополняет диаграмму тем, что позволяет видеть точные значения и процентный вклад каждого правила без визуальной оценки длины полос.

Таблица 2. Правила корреляции

№	Название правила	Количество	Доля
1	System Service Discovery through built-in Windows Utilities	4 805	28.61%
2	First Time Seen Removable Device	1 973	11.75%
3	High Number of Process and/or Service Terminations	1 563	9.31%
4	Process Termination followed by Deletion	1 497	8.91%
5	Connection to Commonly Abused Web Services	1 003	5.97%
6	Unusual Persistence via Services Registry	758	4.51%
7	Suspicious WMI Image Load from MS Office	751	4.47%
8	Svchost spawning Cmd	748	4.45%
9	Privileged Account Brute Force	528	3.14%
10	Creation or Modification of Root Certificate	405	2.41%
11	Potential Process Injection from Malicious Document	312	1.86%

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

12	Persistence via a Windows Installer	309	1.84%
13	Component Object Model Hijacking	240	1.43%
14	Unusual Discovery Signal Alert with Unusual Process Command Line	204	1.21%
15	System Information Discovery via Windows Command Shell	200	1.19%

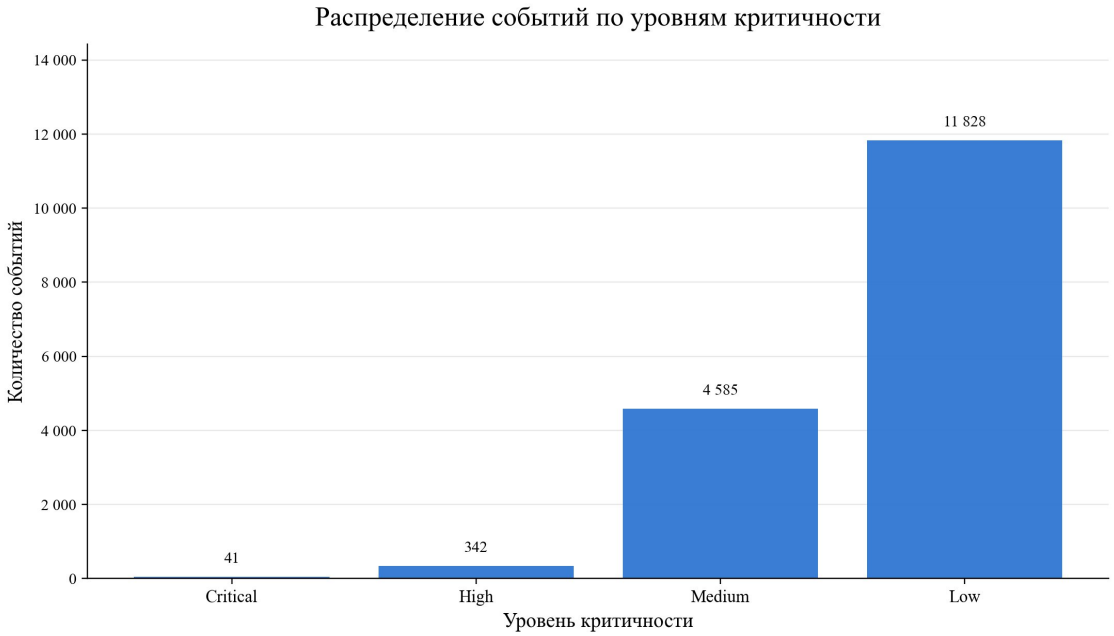


Рисунок 3. Распределение событий по уровням критичности

На рисунке показано распределение событий безопасности по уровням критичности: critical - 41, high - 342, medium - 4 585, low - 11 828. Суммарно по этим уровням отражено 16 796 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 отчетный период было зарегистрировано 16796 событий безопасности. Распределение по уровням критичности составило: critical - 41, high - 342, medium - 4585, low - 11828. Наиболее заметная активность наблюдалась по правилам System Service Discovery through built-in Windows Utilities, First Time Seen Removable Device, High Number of Process and/or Service Terminations, a также на узлах desktop-llneh6f, nauz-pc-0007, desktop-mlq5rlg. Статусы кейсов за период: closed - 1, in-progress - 33. Основной объем срабатываний пришелся на

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

сценарии, связанные с контролем внешних носителей, попытками перебора привилегированных учетных записей и разведывательной активностью внутри операционной системы.

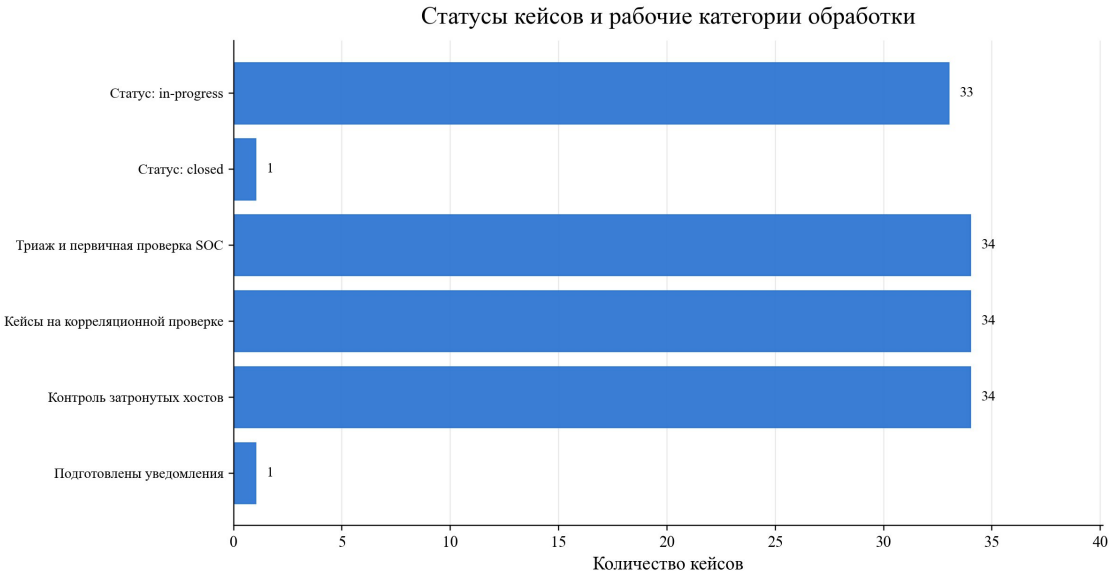


Рисунок 4. Статусы кейсов и уведомлений

На рисунке показано распределение кейсов и рабочих категорий обработки за отчетный период. Наиболее крупная категория на диаграмме: «Статус: in-progress» - 33. Общее количество кейсов в данных Elastic Cases составляет 34, количество направленных уведомлений - 1. Диаграмма объединяет фактические статусы кейсов и рабочие категории, использованные для отображения процесса обработки в отчете.

Строковая расшифровка раскрывает данные по кейсам и содержит 7 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 3. Статусы и категории обработки кейсов

№	Статус/категория	Количество	Комментарий
1	in-progress	33	Фактический статус из Elastic Cases
2	closed	1	Фактический статус из Elastic Cases

DOC ID KZBW2Z120260000201301F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

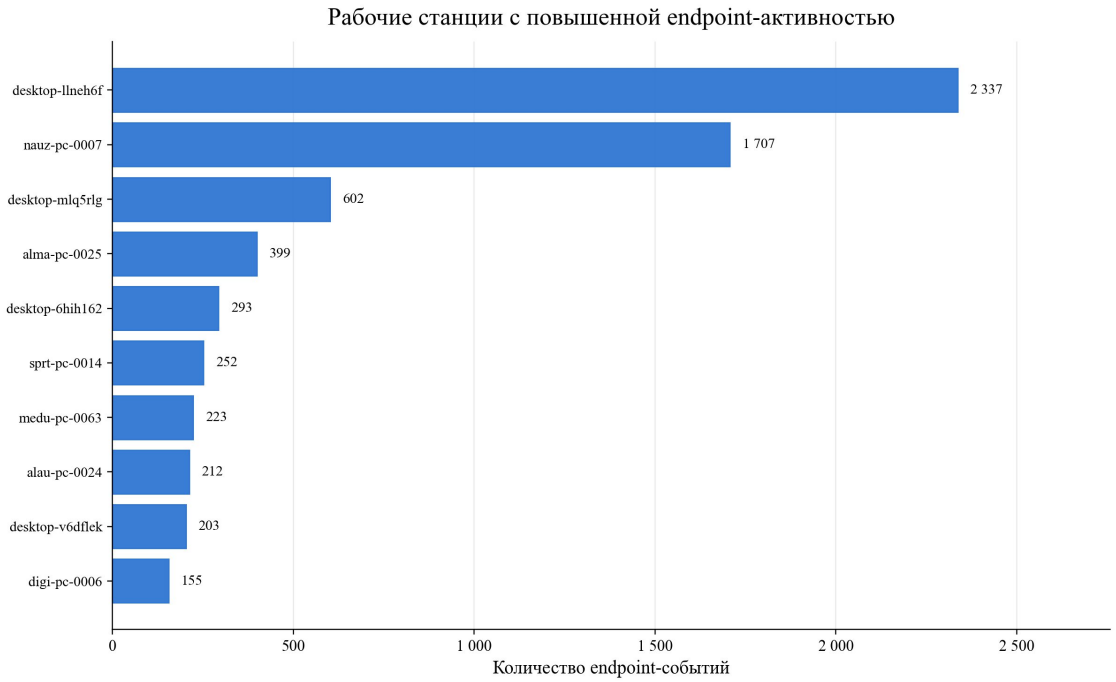


Рисунок 5. Рабочие станции с повышенной активностью

На рисунке показаны рабочие станции с наибольшим количеством endpoint-событий за отчетный период. Первое место в выборке занимает хост desktop-llneh6f с количеством событий 2 337. 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.

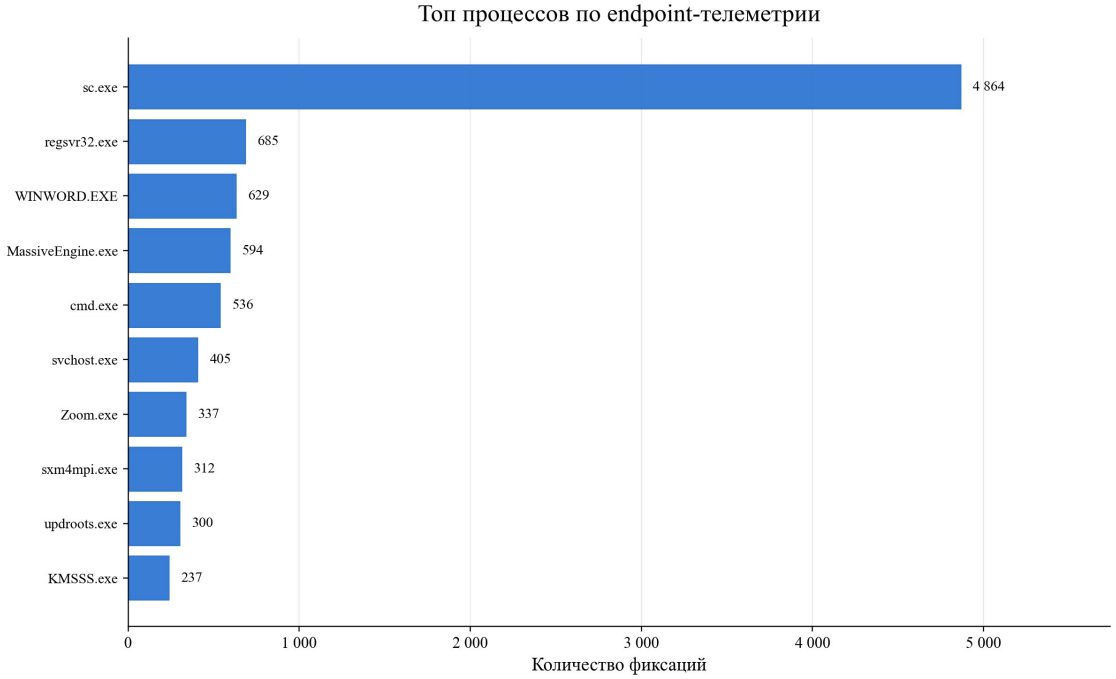


Рисунок 6. Топ процессов по endpoint-телеметрии

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

На рисунке показаны процессы, которые чаще всего встречались в endpoint-телеметрии за отчетный период. Верхняя строка диаграммы соответствует процессу sc.exe с количеством фиксаций 4 864. 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 sc.exe с наибольшим приростом активности относительно прошлого периода (+4 620 фиксаций). Таблица дополняет диаграмму процессов тем, что показывает не только текущую частоту, но и изменение относительно предыдущего отчетного периода.

Таблица 4. Процессы с изменением профиля активности

№	Процесс	Текущий период	Прошлый период	Δ	Комментарий
1	sc.exe	4 864	244	+4 620	рост активности относительно прошлого периода
2	regsvr32.exe	685	22	+663	рост активности относительно прошлого периода
3	MassiveEngine.exe	594	0	+594	новый или единичный в прошлом периоде
4	cmd.exe	536	120	+416	рост активности относительно прошлого периода
5	Zoom.exe	337	0	+337	новый или единичный в прошлом периоде
6	updroots.exe	300	0	+300	новый или единичный в

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

					прошлом периоде
7	WINWORD.EXE	629	370	+259	рост активности относительно прошлого периода
8	_iu14D2N.tmp	191	74	+117	рост активности относительно прошлого периода
9	KMSSS.exe	237	128	+109	рост активности относительно прошлого периода
10	AAct_x64.exe	234	126	+108	рост активности относительно прошлого периода
11	lsass.exe	107	0	+107	новый или единичный в прошлом периоде
12	msiexec.exe	147	70	+77	рост активности относительно прошлого периода
13	unins000.exe	98	26	+72	рост активности относительно прошлого периода
14	NCALayer.exe	94	23	+71	рост активности относительно прошлого периода
15	_unins.tmp	42	0	+42	новый или единичный в

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

					прошлом периоде

4.2. Система уведомлений

По событиям безопасности за отчетный период заведено и обработано 34 кейса. Количество направленных уведомлений составило 1. Распределение кейсов по статусам: closed - 1, in-progress - 33. 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: whatsapp Soft pc upload.exe, INSTAL~3.EXE | TumarCSP | Malware Prevention Alert, Open Incognito Tab extension | bgmlfdcgihhfheckfdmhnmedjigogmm. За отчетный период зарегистрировано 383 события уровня high/critical; основной вклад внесло правило «System Service Discovery through built-in Windows Utilities».

В отчетном периоде через рабочий канал взаимодействия с Заказчиком «Заявки на проверку хостов» обработано свыше 40 обращений по событиям безопасности, сведенных в 30 инцидентов. По каждому обращению средствами SIEM/EDR выполнены анализ и верификация, подготовлено заключение с рекомендациями; из общего числа подтверждено 3 ложных срабатывания. Сводный журнал обработанных обращений приведен в Таблице 5, детальные заключения ОЦИБ — в Приложении 2.

Таблица 5. Журнал обработанных обращений (заявок на проверку хостов) за июнь 2026

№	Дата	Хост(ы)	Событие / угроза	Заключение ОЦИБ и статус реагирования
1	01.06	desktop-qpta302	Malware Prevention (High): YandexPackLoader.exe, VT 31/71 (trojan/downloader)	Вредоносный загрузчик; хост изолирован, даны рекомендации по удалению — обработано
2	01–29.06	nauz-pc-0052, jets-pc-0051, medu-pc-0077, socp-pc-0047, auez-pc-	Червь Phorpiex/DriveMgr — запуск с USB (DriveMgr.exe / DrvSvcsrMgrsvr.exe / VolDriver.exe)	USB-червь; файлы в карантине, хосты изолированы, рекомендована проверка съемных носителей — изоляция/очистка, повторные сработки

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

		0016, bost-pc-0031, nauz-pc-0002 и др.		
3	02–22.06	1cserver, eclg-pc-0026, tksb-pc-0007, tksb-pc-0047, tksb-pc-0031, cntr-pc-0023	KMS-активатор: sppextcomobjpatcher.exe и инъекция SppExtComObjHook.dll (VT 47/69, hacktool.kmsauto)	Закрепившийся KMS-кряк с DLL-инжектором; EDR блокирует, требуется удалить источник — Принято, чистят (повторные сработки)
4	02.06	akmt-pc-0007	Privileged Account Brute Force с узла 192.168.31.14	Ложное срабатывание — источник 192.168.31.14 является хостом планового сканирования (Kali) — FP, закрыто
5	04–17.06	auez-pc-0112, auez-pc-0116, auez-pc-0011, auez-pc-0106, auez-pc-0113, auez-pc-0015	KMSAuto++ / gatherosstate.exe / SLC.DLL (VT 48/70, 25/72)	KMS-активатор; часть файлов не помещена в карантин (активна); рекомендованы удаление и проверка автозагрузки — Принято, изоляция/очистка
6	05.06	tansu	AnyDesk.exe — несанкционированное средство удаленного доступа	Несанкционированный инструмент удаленного доступа; рекомендовано удалить — обработано

DOC ID KZBW2Z1202600002013O1F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z1202600002013O1F66B3

7	08.06	nauz-pc-0035	Malware Prevention (High): исполняемый файл с USB (E:), ML-скоринг 0.999984, trojan/dropper	Троян/дроппер с USB; помещен в карантин, хост изолирован — почистили, разблокирован
8	09.06	bost-vs-1001 (DC)	Остановка службы Microsoft Defender (Event ID 7036)	Ложное срабатывание — плановое обновление Defender Platform (self-restart служб), не отключение AV — FP, закрыто
9	09.06	auez-pc-0101	KMS-активатор (KMSTools.exe)	По согласованию с Заказчиком добавлено разрешение (whitelist) на KMS для указанной папки — санкционировано
10	09.06	heal-pc-0033	winscan2pdf-9.39-installer.exe — потенциально нежелательное ПО	Подозрительный инсталлятор; рекомендована проверка — обработано
11	10.06	akmt-vs-1001	Регулярные DNS-запросы powershell.exe к api.telegram.org (05–10.06, учетная запись SYSTEM)	Подозрительная C2-подобная активность через Telegram API; проведено расследование — на контроле
12	10.06	akmt-vs-1001	Доступ notepad.exe к C:\Windows\Tasks\SA.DAT через OpenWith.exe	Нетипичный доступ к системному файлу; направлен запрос на подтверждение легитимности — проверка
1	10.06	nauz-pc-	Исполняемые объекты из кэша браузера Edge	Аномальные расширения в профиле

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

3		0043	(.scr/.bat/.exe)	Edge — временно разблокирован, запланирована очистка
14	11.06	nauz-vs-1001	Остановка Defender и установка компонента KslD (Kaspersky)	Паттерн замены антивирусного ПО; признаков ВПО не выявлено; запрошено подтверждение плановой замены — подтверждено
15	11–26.06	desktop-mlq5rlg	PUA MassiveEngine.exe (майнинг/перехват трафика под видом adblock), исходящий трафик и DNS	PUA с риском майнинга и утечки данных; рекомендовано удалить — рекомендации, повторные сработки
16	12.06	MEDU-PC-0028	Браузерное расширение Doodocs Sign (подпись ЭЦП в обход NCALayer)	Риск утечки ключевого контейнера/документо в через сторонний сервис; проверить/удалить — уточняется
17	12.06	desktop-eopkgau	Ярлык автозагрузки Documentolog.lnk, созданный msiexec.exe	Запрошено подтверждение легитимности установки (корпоративный дистрибутив) — уточняется
18	12.06	akmt-vs-1001	Privileged Account Brute Force	Ложное срабатывание — плановая проверка отработки правила Privileged Account Brute Force — FP,

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

				закрыто
19	17.06	desktop-uq6ns5g	downloader.exe (переименован в .tmp) через Opera в режиме инкогнито, VT 30/66 (trojan.yandex)	Троян-загрузчик; рекомендованы изоляция/удаление — Принято
20	17.06	SOCP-PC-0004 → akmt-vs-1002	Множественные неудачные сетевые аутентификации (Event 4625, учетная запись Admin, NTLM)	Подозрение на подбор пароля/сетевую аномалию — обработано
21	17.06	auez-pc-0113	uTorrent (нарушение политики ПО) и вредоносная SLC.DLL	Торрент-клиент и вредоносная DLL заблокированы и помещены в карантин — Healthy
22	17.06	nauz-pc-0007	Команда sc.exe query state= all (разведка служб) через стороннее АВПО ReasonLabs	Разведка системного окружения сторонним АВПО — Принято
23	18–19.06	gos1	taskhostw.exe из каталога …\ReaItekHD (маскировка под Realtek) с обращением к api.telegram.org	Маскировка под системный процесс и обращение к Telegram API (C2); правило Connection to Commonly Abused Web Services — Принято, повторные сработки
24	22.06	digi-pc-0007	Торрент-клиент и распакованная пиратская игра с вредоносными компонентами	Угроза нейтрализована; файлы заблокированы и помещены в карантин до исполнения — обработано

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

25	23–25.06	yout-pc-0009, invs-pc-0012	WinDivert64.sys (GammaTech VpnClient), цифровая подпись Trusted	Драйвер перехвата трафика легитимного VPN (подписан); помещен в карантин, проверка легитимности — повторные сработки
26	25.06	desktop-34b4kfl	ATIHelper.exe (Anytxt Searcher), VT чистый, подписан	Направлен запрос по списку разрешенного ПО — уточняется
27	29.06	bost-pc-0021	«whatsapp Soft pc upload.exe» (троян); агент EDR не отвечал на команды	Троян; после переназначения политики EDR хост изолирован — изолирован
28	29.06	desktop-qp7t2ok, medu-pc-0010, eclg-pc-0005, psps-pc-0007	AnyDesk — повышение привилегий и массовые запуски	Несанкционированный инструмент удаленного доступа с попыткой повышения привилегий — на контроле
29	29.06	medu-pc-0010, pinf-pc-0008	Активация встроенной учетной записи Администратора (net user administrator /active:yes)	Единый паттерн повышения привилегий через cmd.exe от обычных пользователей — обработано
30	29.06	множество хостов	Массовый сбой запуска Elastic EDR (установка проходит, агент не стартует) на хостах с NCALayer	Конфликт при запуске/политике EDR; добавлены исключения, политики переназначены (690 агентов онлайн) — устранено

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

4.3. Поиск угроз

В рамках проактивного поиска угроз (Threat Hunting) в отчетном периоде на основе телеметрии SIEM и EDR отрабатывались следующие гипотезы компрометации: распространение вредоносного ПО через съемные USB-носители (автозапуск и загрузчики семейства DriveMgr); несанкционированный майнинг криптовалют (процессы XMRig и аномальная вычислительная нагрузка); использование неавторизованных активаторов ПО (KMS-активаторы) и потенциально нежелательного ПО; аномальная активность процессов и механизмы закрепления (persistence) в автозагрузке и планировщике задач; обращения рабочих станций к внешним адресам с признаками командных серверов (C2). Поиск выполнялся путем корреляции событий конечных точек, сетевой активности и данных threat intelligence (OpenCTI); выявленные срабатывания верифицировались, по подтвержденным ложноположительным результатам исключения формировались точечно по SHA-256. Аналитическая обработка велась на фоне 383 событий уровня high/critical с основной концентрацией по правилам System Service Discovery through built-in Windows Utilities, First Time Seen Removable Device, High Number of Process and/or Service Terminations. Признаков результативной целенаправленной компрометации по итогам периода не выявлено; часть срабатываний классифицирована как ложноположительная, соответствующие узлы взяты на контроль. За отчетный период зарегистрировано 383 события уровня high/critical; основной вклад внесло правило «System Service Discovery through built-in Windows Utilities».

4.4. Доступность веб-интерфейса

В отчетном 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 отчетного периода.

4.5. Автоматическое реагирование на угрозы

Средствами EDR за отчетный период заблокировано 173 вредоносных действия и 47 запусков подозрительных объектов. Автоматическая изоляция, отраженная в телеметрическом счетчике Elastic Defend, была применена к 0 узлам. Дополнительно по телеметрии конечных точек выделены процессы с аномальным ростом активности относительно прошлого периода: sc.exe - 4 864 запусков за текущий период против 244 ранее (Δ +4620); рост активности относительно прошлого периода. regsvr32.exe - 685 запусков за текущий период против 22 ранее (Δ +663); рост активности относительно прошлого периода. MassiveEngine.exe - 594 запусков за текущий период против 0 ранее (Δ +594);

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

новый или единичный в прошлом периоде. cmd.exe - 536 запусков за текущий период против 120 ранее (Δ +416); рост активности относительно прошлого периода.

По операционным сообщениям за июнь дополнительно выполнялись меры локализации и реагирования: изоляция или подготовка к изоляции хостов при недоступности агента, проверка и очистка зараженных рабочих станций, перевод хостов на release/разблокировку после устранения угрозы, а также блокировка C2-адресов и доменов на уровне Check Point.

В отчетном периоде по операционным сообщениям выполнялись стандартные процедуры реагирования: анализ и верификация срабатываний средствами SIEM/EDR и T-Lab Sandbox, изоляция и очистка затронутых рабочих станций, блокировка вредоносных адресов и доменов на межсетевом экране Check Point, а также последующая разблокировка узлов после устранения угроз. Детальный журнал действий реагирования с указанием даты, узла, типа угрозы и предпринятых мер ведется отдельно и предоставляется по запросу.

5. Аудит ИБ и обследование объекта на соответствие требованиям ТД/ИБ

Пункты ТС: 1.1.22, 3.1-3.7.

Операционный отчет за июнь отражает состояние систем мониторинга и защиты. Аудит информационной безопасности, согласно ТС, проводится не менее одного раза в год, продолжительностью не более 90 рабочих дней. В ноябре 2025 года ежегодный аудит ИБ был проведен; результаты аудита и рекомендации по устранению выявленных нарушений направлены Заказчику сопроводительным письмом исх. №607 от 21.11.2025. Аудит ИБ 2026 года находится в процессе согласования плана-графика с Заказчиком. Подтверждающими материалами в рамках настоящего отчета являются Приложение 9 «Статус реализации», а также комплект ТД ИБ: Правила проведения внутреннего аудита ИБ, Методика оценки рисков ИБ, Политика ИБ.

6. Управление уязвимостями, сканирования, рекомендации и повторный контроль

Пункты ТС: 1.1.19-1.1.21, 13.1-13.16.

Раздел содержит исходные материалы по инструментальному сканированию Nessus, статистике уязвимостей и динамике относительно предыдущего периода. Для полного подтверждения remediation-процесса рекомендуется прикладывать реестр устранения: владелец, хост/IP, уязвимость, рекомендация, дата направления, срок, статус и дата повторного скана.

6.1. Инструментальное сканирование

Ежемесячно проводится комплексное инструментальное сканирование внутреннего и внешнего периметра сети. Работы выполняются в строгом соответствии с технической спецификацией и включают анализ на наличие уязвимостей, отклонений в конфигурациях и потенциальных точек

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

компрометации. Проведение регулярного сканирования позволяет поддерживать высокий уровень защищенности инфраструктуры, своевременно выявлять риски и обеспечивать их оперативную обработку. По результатам сканирования за отчетный период установлено, что основная часть выявленных уязвимостей относится к уровню Medium (внутренний периметр - 618, внешний периметр - 13). Наибольшая событийная активность зафиксирована в подразделениях Управление городского планирования и урбанистики, Заместители руководителя аппарата акима города Алматы, Управление финансов, Управление предпринимательства и инвестиций города Алматы. По результатам внутреннего сканирования выявлено критических уязвимостей - 41, высоких - 157, средних - 618. По внешнему периметру выявлено критических - 0, высоких - 0, средних - 13. В целом результаты анализа свидетельствуют о контролируемом уровне рисков информационной безопасности и эффективности действующих процессов мониторинга и управления уязвимостями. Подробная информация по сканированиям сети приведена в приложениях 4, 5 и 6.

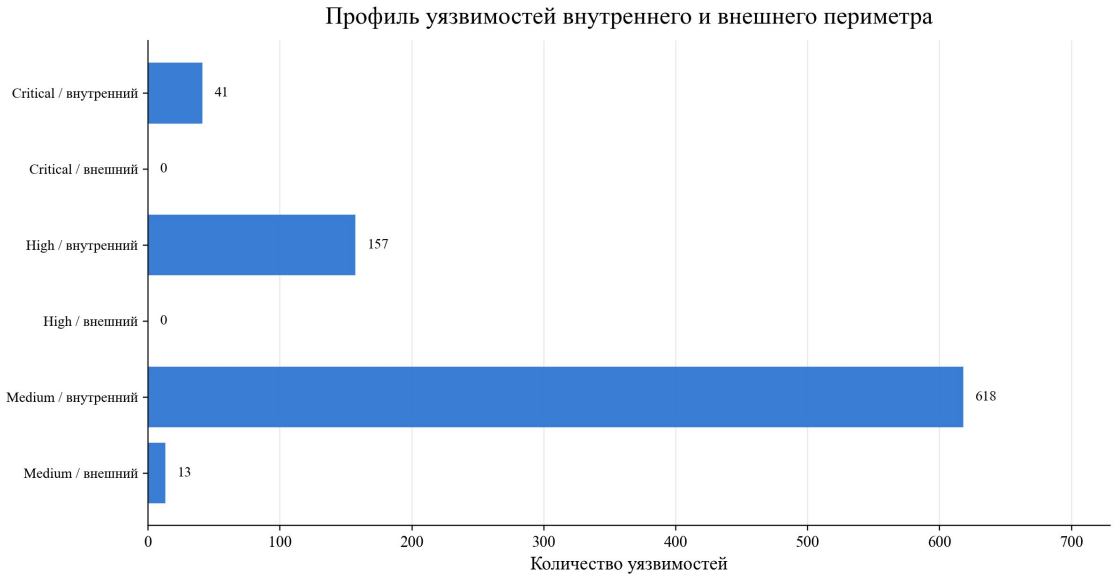


Рисунок 7. Профиль уязвимостей внутреннего и внешнего периметра

Таблица 6. Сканирование сети

№	Подразделение (объект сканирования)	Critical	High	Medium
1	Управление городского планирования и урбанистики	6	6	24
2	Заместители руководителя аппарата акима города Алматы	6	5	21

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

3	Управление финансов	4	9	15
4	Управление предпринимательства и инвестиций города Алматы	3	34	82
5	Аппарат Акима	3	2	9
6	Управление молодежной политики	2	9	17
7	Управление экологии	2	8	11
8	Управление энергетики	2	8	17
9	Управление строительства	2	6	10
10	Управление городской мобильности	2	5	10

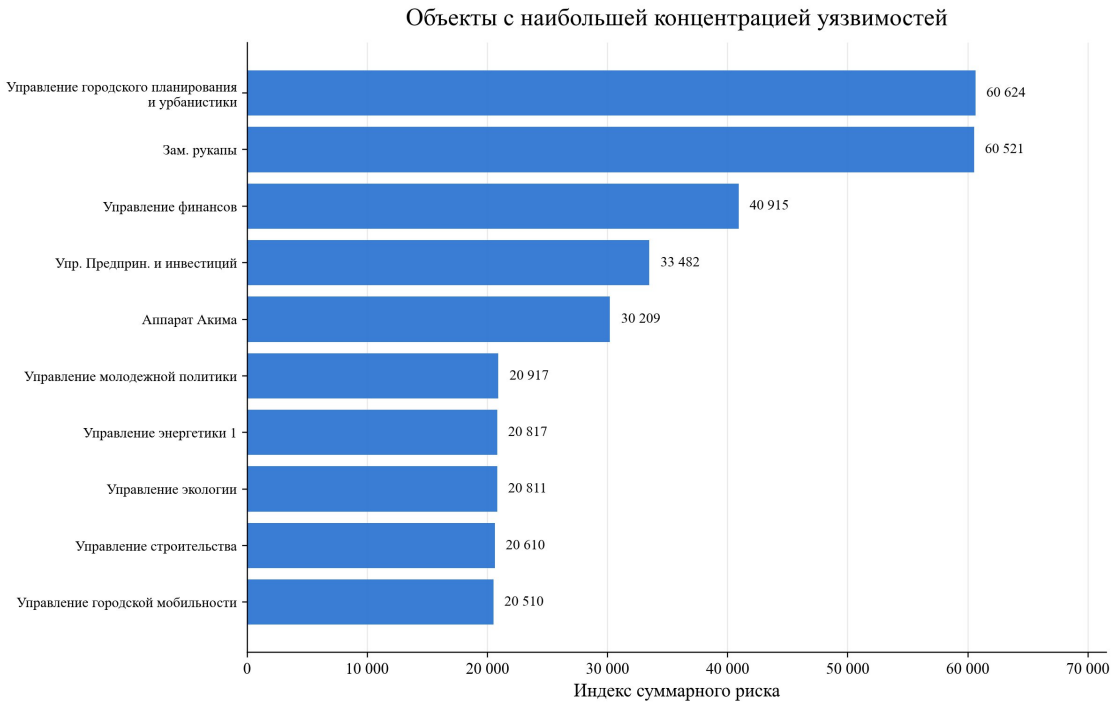


Рисунок 8. Объекты с наибольшей концентрацией уязвимостей

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

6.2. Статистика управления уязвимости

Диаграмма отражает сравнение количества выявленных уязвимостей по уровням критичности между текущим и предыдущим запусками сканирования.

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business
DOC ID KZBW2Z120260000201301F66B3

Текущий запуск выполнен 30.06.2026 в 07:52:05, предыдущий — 28.06.2026 в 10:58:18; источником данных для сравнения использовано состояние предыдущего запуска, зафиксированное в нормализованной выгрузке Nessus. В распределении уязвимостей уровней Critical, High и Medium зафиксированы изменения: ΔCritical = +40, ΔHigh = +147, ΔMedium = +564. Это указывает на изменение текущего профиля рисков и требует продолжения мероприятий по remediation и перепроверке проблемных узлов. По результатам сравнения текущего и предыдущего запусков сканирования зарегистрировано новых критических уязвимостей - 40, устранено критических - 0. Новых высоких уязвимостей - 147, устранено высоких - 0. Наиболее уязвимые узлы: 192.168.164.11, 192.168.164.12, 192.168.156.27, 192.168.152.123, 192.168.135.173. В отчетном периоде совместно с системными администраторами Управления финансов акимата города Алматы ведутся работы по устранению, выявленной и подтвержденной (проверенной совместно со специалистами ОЦИБ) уязвимости; процесс устранения (remediation) находится в стадии выполнения. По данным Nessus в отчетном периоде сохраняются 41 критических и 157 высоких уязвимостей. Наиболее уязвимые узлы по суммарной тяжести находок: 192.168.164.11, 192.168.164.12, 192.168.156.27. Подробная сводная таблица по статистике управления уязвимостями приведена в приложении 4.

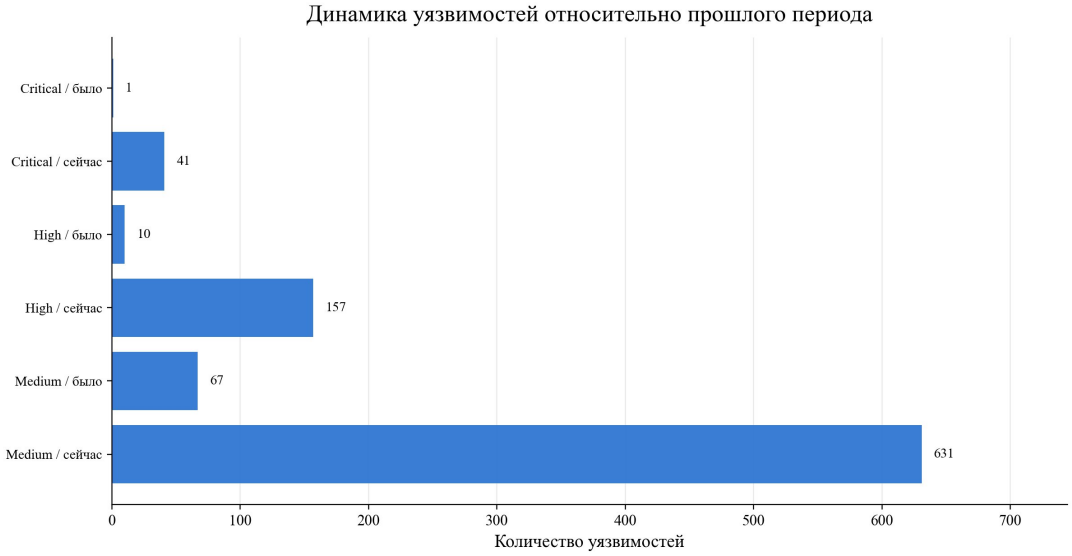


Рисунок 9. Динамика уязвимостей относительно прошлого периода

Таблица 7. Статистика управления уязвимостями

Скан	СЕЙЧАС К/В/С	БЫЛО К/В/С	ΔК/ΔВ/ΔС	Новые	Устранены	Без изм.	Крит.↑	Крит.↓	ΔХостов

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Управление городского планирования и урбанистики	6/6/24	0/0/0	+6/+6/+24	2 585	0	0	6	0	+256
Заместители руководителя аппарата акима города Алматы	6/5/21	0/0/0	+6/+5/+21	1 512	0	0	6	0	+256
Управление финансов	4/9/15	0/0/0	+4/+9/+15	905	0	0	4	0	+256
Управление предпринимательства и инвестиций города Алматы	3/34/82	0/0/0	+3/+34/+82	2 659	0	0	3	0	+254
Аппарат Акима	3/2/9	0/0/0	+3/+2/+9	1 327	0	0	3	0	+256
Управление молодежной политики	2/9/17	0/0/0	+2/+9/+17	423	0	0	2	0	+256
Управление экологии	2/8/11	0/0/0	+2/+8/+11	690	0	0	2	0	+256
Управление энергетики	2/8/17	0/0/0	+2/+8/+17	467	0	0	2	0	+256
Управление строительства	2/6/10	1/3/9	+1/+3/+1	39	243	406	1	0	+0
Управление городской мобильности	2/5/10	0/0/0	+2/+5/+10	455	0	0	2	0	+256

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

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Тестирование на проникновение (пентест) внешнего и внутреннего периметра сети запланировано к проведению в октябре 2026 года. По его результатам будет подготовлен отчет с перечнем выявленных уязвимостей, оценкой рисков и рекомендациями по устранению, который будет предоставлен Заказчику отдельным комплектом.

7. План непрерывности, восстановление деятельности, резервное копирование

Пункты ТС: 1.1.30, 2.1, 9.1.

В рамках требований Технической спецификации обеспечивается контроль готовности процедур непрерывности, восстановления деятельности и сохранности конфигураций средств защиты информации. Для подтверждения указанного направления в составе эксплуатационной документации должны поддерживаться план непрерывности, сценарии восстановления, параметры RTO/RPO, перечень ответственных лиц, периодичность тестов восстановления и журнал выполнения резервного копирования. Указанные материалы используются для подтверждения управляемости критичных ИБ-сервисов и готовности к восстановлению после отказов или инцидентов.

8. Регламенты, SLA, планы работ и порядок взаимодействия

Пункты ТС: 1.2.2, 1.2.7-1.2.8, 5.1.

Порядок взаимодействия сторон, SLA, плановые работы и маршрут эскалации закреплены договорной и организационной документацией. В отчетном периоде взаимодействие осуществлялось через рабочие коммуникации по событиям информационной безопасности, уведомления по инцидентам, согласование доступов и сбор подтверждающих материалов. Для обеспечения единообразного исполнения ТС рекомендуется поддерживать актуальный реестр контактных лиц, регламент эскалации, календарный план работ, статусную матрицу выполнения требований и журнал согласованных изменений. Перечень ответственных администраторов и контактных лиц со стороны Заказчика (включая системного администратора Исполнителя), осуществляющих взаимодействие в рамках Технической спецификации (пп. 1.2.2, 1.2.7–1.2.8, 5.1):

Таблица 8. Перечень ответственных администраторов

ФИО	Управление / Объект	Должность	Телефон
Рябцев Андрей	ТОО «MSSP.GL» (Исполнитель)	Системный администратор	8 707 922 95 75
Андрей Данил	Аппарат акима / Упр. культуры / Упр. строительства	Администратор	8 701 943 74 22
Никита	Управление спорта	Администратор	8 705 164 45 07

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Адильхан	Упр. городской мобильности, молодежной политики, энергетики, экологии и др.; Алмалинский р-н; Бостандыкский р-н	Администратор	8 702 166 66 24
Темирлан	Управление общественного здравоохранения	Администратор	8 707 101 24 84
Андрей Хозу	Управление экономики	Администратор	8 701 943 74 22
Темирлан	Управление образования	Администратор	8 707 970 06 97
Акылбек	Управление государственных активов	Администратор	8 707 381 17 40
Диас	Управление занятости и социальных программ	Администратор	8 778 689 16 61
Еркін	Управление развития коммунальной инфраструктуры	Администратор	8 707 937 88 87
Иван	Управление городского планирования и урбанистики	Администратор	8 707 407 94 22
Фархад	Упр. градостроительного контроля / Упр. земельных отношений	Администратор	8 701 799 56 42
Роллан	Аппарат акима Алатауского района	Администратор	8 700 268 00 69
Светлана	Аппарат акима Алатауского района	Зав. хоз.	8 702 319 15 59
Ханторе	Аппарат акима Жетысуского района	Администратор	8 771 444 72 50
Бауржан	Аппарат акима Медеуского района	Администратор	8 747 953 21 73
Рахымділдә Жігер Талғатұлы	Аппарат акима Наурызбайского	Администратор	8 747 687 43 06

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

	района		
Букей Жасұлан Ерланұлы	Аппарат акима Наурызбайского района	Администратор	8 708 416 74 48
—	Аппарат акима Турксибского района	Администратор	—
—	Управление предпринимательства и инвестиций города Алматы	Администратор	—
—	Управление по делам религий	Администратор	—
—	Управления сейсмической безопасности	Администратор	—

9. MDR, доступность услуги, поддержка и обработка событий

Пункты ТС: 3.14.1-3.14.4, 10.1.

В отчетном периоде услуга MDR функционировала в штатном режиме. Обеспечивались мониторинг событий SIEM/EDR, первичный триаж сработавших правил, проверка затронутых хостов, обработка 34 кейсов и направление 1 уведомления ответственным администраторам. Доступность веб-интерфейса SIEM сохранялась в рабочем режиме, что позволяло выполнять оперативный анализ событий и контроль статусов реагирования. Для регулярного подтверждения SLA целесообразно вести журнал дежурств, журнал уведомлений, метрики времени реакции и ежемесячную сводку доступности сервисов мониторинга.

10. Контроль привилегированного доступа и/или bastion/PAM

Пункты ТС: Раздел 7 / PAM.

Контроль привилегированного доступа (PAM / bastion) находится в стадии внедрения. Требования Технической спецификации (Раздел 7) предусматривают развертывание PAM-системы для управления привилегированными учетными записями, записи сессий, разграничения административных ролей и ротации секретов. В отчетном периоде проведена инвентаризация административных ролей и состава привилегированных групп в Active Directory и Check Point; результаты систематизированы. Архитектура PAM, перечень подключаемых систем, матрица ролей и порядок ротации секретов формализуются — внедрение PAM-решения запланировано и ведется в рамках согласованного плана работ с Заказчиком.

11. Обучение работников Заказчика по вопросам ИБ

Пункты ТС: 8.1-8.3.

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Направление обучения работников Заказчика по вопросам информационной безопасности (ТС пп. 8.1–8.3) находится в процессе реализации. Исполнителем направлен запрос Заказчику о предоставлении списка сотрудников для участия в обучении; ответ от Заказчика ожидается. После согласования состава участников будут оформлены: программа обучения, учебные материалы, ведомость/акт проведения и подтверждение прохождения инструктажа. Мероприятие по повышению осведомленности в области ИБ запланировано на период Q3 2026 года по согласованию с Заказчиком.

12. Процессы обеспечения ИБ: доступы, активы, уязвимости, обновления, резервирование, инциденты, изменения

Пункты ТС: 9.1.

В отчетном периоде обеспечены и документально закреплены ключевые процессы информационной безопасности в соответствии с требованиями ТС (п. 9.1) и утвержденной технической документацией по ИБ (ТД ИБ):

– Управление доступом, активами, обновлениями и изменениями: «Правила по управлению доступом, активами, обновлениями и изменениями» (ТД ИБ №6);

– Резервное копирование и восстановление: «Правила резервного копирования и восстановления информации» (ТД ИБ №11);

– Мониторинг событий и управление инцидентами: «Правила по мониторингу событий и управлению инцидентами» (ТД ИБ №13);

– Идентификация и классификация активов: «Правила идентификации, классификации и маркировки активов» (ТД ИБ №2);

– Управление рисками ИБ: «Правила по управлению рисками информационной безопасности» (ТД ИБ №12).

Комплект ТД ИБ передан Заказчику в рамках настоящего отчетного пакета (раздел 20, комплект ТД ИБ). Исполнение указанных документов ведется в штатном режиме.

13. Сетевая архитектура, сегментация, рекомендации по оптимизации/перепроектированию

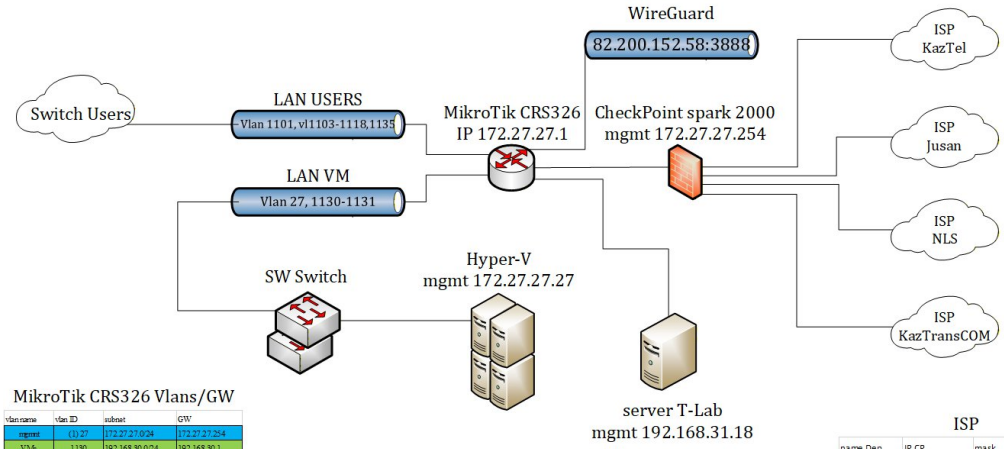
Пункты ТС: 11.1-11.3.

По результатам рассмотрения логических L3-схем подтверждена сегментированная архитектура основной площадки и удаленных управлений Акимата. Центральный контур построен на периметровом шлюзе Check Point Spark 2000 и L3-коммутации MikroTik, при этом пользовательские, серверные и ведомственные сегменты выделены в отдельные подсети и VLAN. Удаленные управления подключаются через периметровые шлюзы Check Point 1775, отдельные каналы операторов связи и VPN-туннели IPSec/WireGuard. Такая архитектура обеспечивает базовое разделение периметра, серверной зоны, основной сети и сетей управлений.

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Схема Акимата (головной) L3



MikroTik CRS326 Vlans/GW

vlan name	vlan ID	subnet	GW
mgmt	(1)27	172.27.27.0/24	172.27.27.254
VMs	1130	192.168.30.0/24	192.168.30.1
IB	1131	192.168.31.0/24	192.168.31.1
AKIM	1101	192.168.101.0/24	192.168.101.246
STROY	1103	192.168.103.0/24	192.168.103.10
FINANCE	1104	192.168.104.0/24	192.168.104.10
ECOMONY	1105	192.168.105.0/24	192.168.105.10
SPORT	1106	192.168.106.0/24	192.168.106.10
MOL-POLIT	1107	192.168.107.0/24	192.168.107.10
OBRAZOV	1108	192.168.108.0/24	192.168.108.10
ZDRAVO	1109	192.168.109.0/24	192.168.109.10
GOS-AKTIV	1110	192.168.110.0/24	192.168.110.10
ECOLOGY	1111	192.168.111.0/24	192.168.111.10
GOR-MOBIL	1112	192.168.112.0/24	192.168.112.10
OB-RAZVIT	1113	192.168.113.0/24	192.168.113.10
KULTURY	1114	192.168.72.0/24	192.168.72.5
ENERGY1	1115	192.168.115.0/24	192.168.115.10
ENERGY2	1116	192.168.116.0/24	192.168.116.10
CIFROVIZ1	1117	192.168.117.0/24	192.168.117.10
CIFROVIZ2	1118	192.168.118.0/24	192.168.118.10
ZAMRUK	1135	192.168.135.0/25	192.168.135.10

ISP

name Dep	IP CP	mask	GW
AKIM	188.127.49.35	255.255.255.224	188.127.49.33
STROY	80.242.214.218	255.255.255.252	80.242.214.217
FINANCE	212.154.213.154	255.255.255.252	212.154.213.153
MOL-POLIT	82.200.148.114	255.255.255.252	82.200.148.113
OBRAZOV	5.188.65.73	255.255.255.0	5.188.65.1
ZDRAVO	82.200.241.218	255.255.255.252	82.200.241.217
GOS-AKTIV	88.204.131.18	255.255.255.252	88.204.131.17
ECOLOGY	185.97.114.139	255.255.255.240	185.97.114.129
GOR-MOBIL	188.127.49.22	255.255.255.252	188.127.49.21
OB-RAZVIT	178.88.162.206	255.255.255.252	178.88.162.205
KULTURY	82.200.145.102	255.255.255.252	82.200.145.101
ENERGY1	82.200.152.58	255.255.255.252	82.200.152.57
ENERGY2	88.204.140.6	255.255.255.252	88.204.140.5
CIFROVIZ1	88.204.255.178	255.255.255.240	88.204.255.177
ZAMRUK	212.134.243.46	255.255.255.252	212.134.243.45

Рисунок 10. Логическая L3-схема основной сети Акимата города Алматы

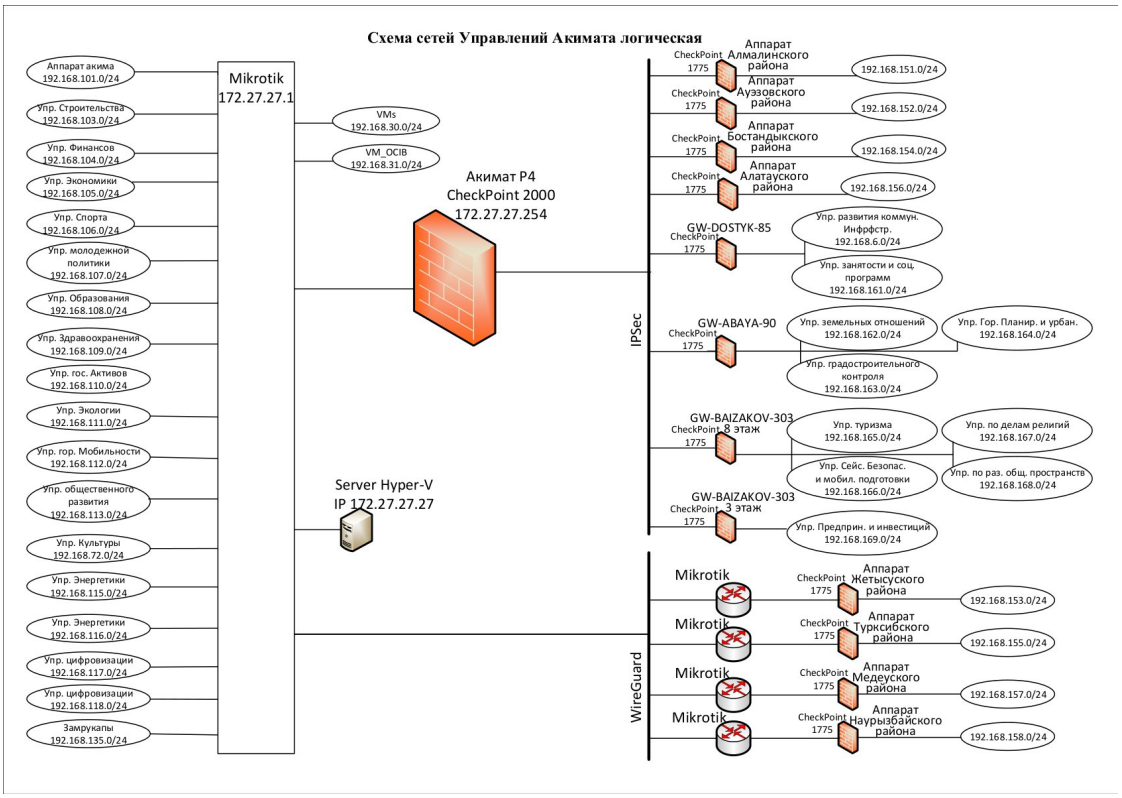


Рисунок 11. Логическая схема сетей удаленных управлений Акимата города Алматы

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Примечание: Обе логические схемы (основная площадка и сети удаленных управлений) предоставлены в составе отчетного пакета в разделе «Сетевые схемы».

Рекомендации по результатам анализа сетевых схем: актуализировать единый адресный план и закрепить владельцев подсетей; унифицировать параметры VPN-подключений и порядок резервирования каналов связи; централизовать журналирование Check Point и MikroTik в SIEM; ограничить межсегментное взаимодействие по принципу минимально необходимого доступа; закрыть административные интерфейсы от внешних сетей; обеспечить резервное копирование конфигураций сетевого оборудования и контроль их изменений.

Дополнительно рекомендуется вести матрицу правил межсетевого экранирования с указанием бизнес-назначения, владельца, срока актуальности и даты последнего пересмотра. Для удаленных управлений необходимо контролировать доступность VPN-туннелей, состояние каналов операторов связи, своевременность обновления прошивок Check Point/MikroTik и передачу событий безопасности в централизованный контур мониторинга.

14. Функции NGFW / Check Point

Пункты ТС: 12.1-12.20.

Раздел содержит сведения Check Point NGFW по защитным механизмам, сетевой активности, вредоносному ПО и IPS. На основании визуальных подтверждающих материалов интерфейса Quantum Spark 2000 Appliance сформирована функциональная матрица NGFW по ключевым требованиям ТС: Security Dashboard, Threat Prevention, IPS Protections, Security Logs, VPN и роли администраторов.

Функциональная матрица ниже фиксирует состояние ключевых модулей на примере шлюза GW-AKIMAT и закрывает функциональные подпункты NGFW в части наличия и эксплуатации Firewall, IPS, Anti-Virus, Anti-Bot, URL Filtering/App Control, VPN, Security Logs и role-based administrators. Визуальные материалы интерфейса Check Point Quantum Spark 2000 Appliance подтверждают сведения о модели и версии шлюза, лицензии, активных blades, статусе Access Policy, Threat Prevention и VPN, настройках IPS/Anti-Virus/Anti-Bot, наличии журналов Security Logs и ролевой модели администраторов. Дополнительно отчет опирается на эксплуатационные данные Check Point по 13 gateway, где отражены события защитных механизмов, сетевые приложения, вредоносные объекты и IPS-срабатывания за отчетный период.

DOC ID KZBW2Z1202600002013O1F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

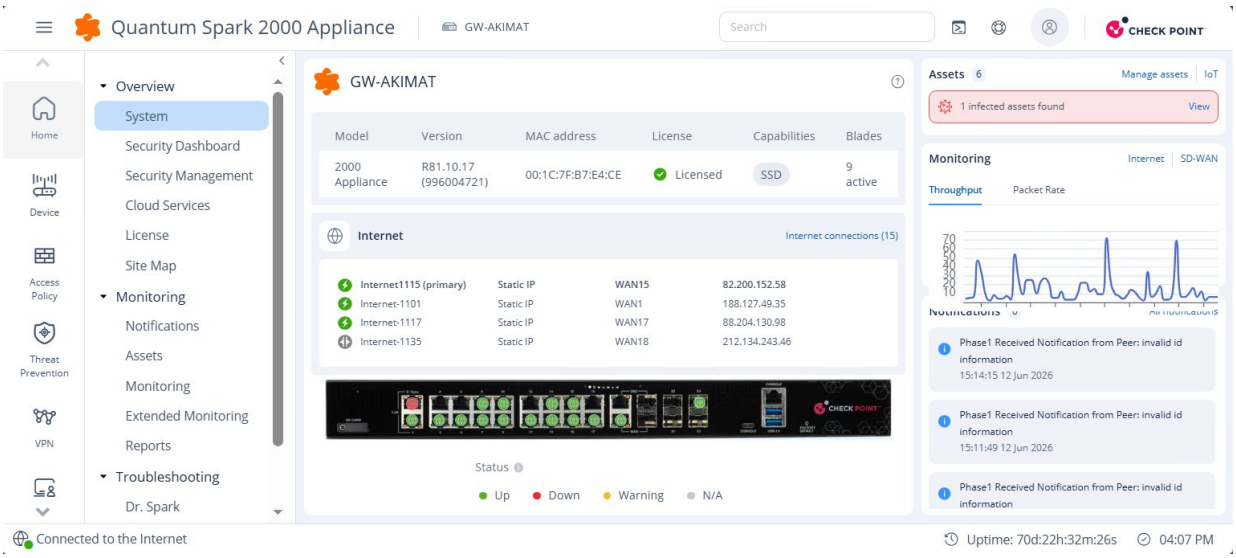


Рисунок 12. Общая информация о шлюзе Check Point Quantum Spark GW-AKIMAT

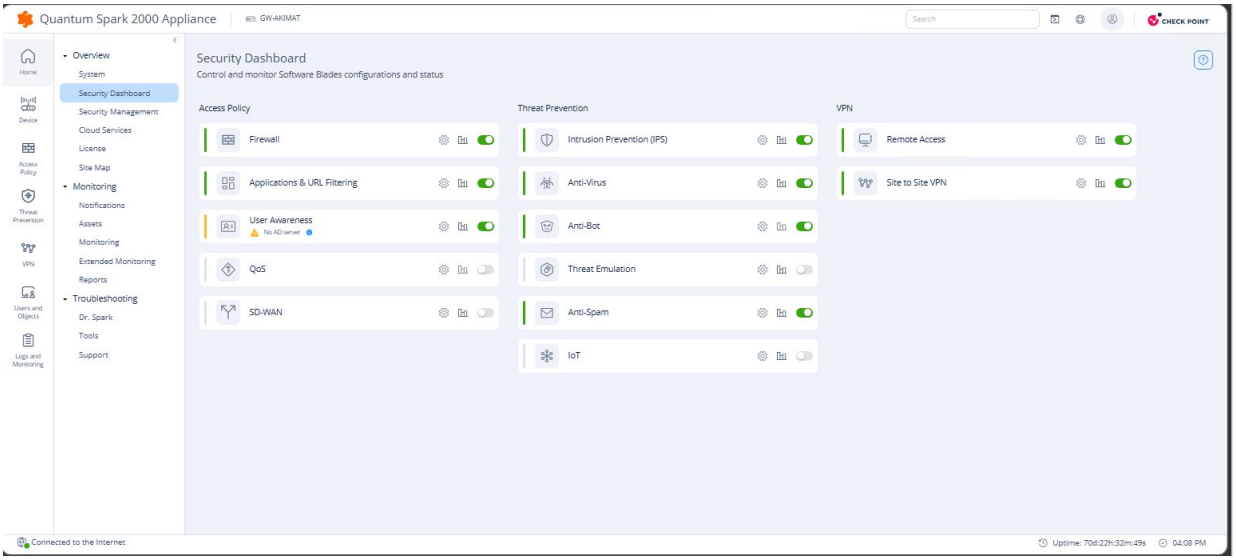
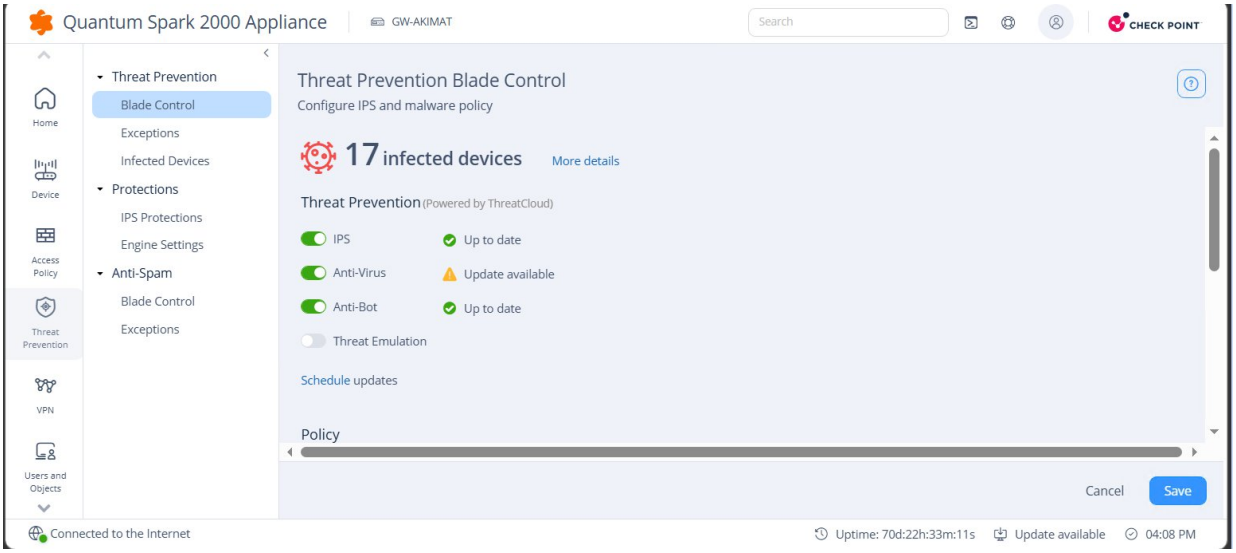


Рисунок 13. Панель Security Dashboard Check Point Quantum Spark



DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Рисунок 14. Состояние модулей Threat Prevention Check Point

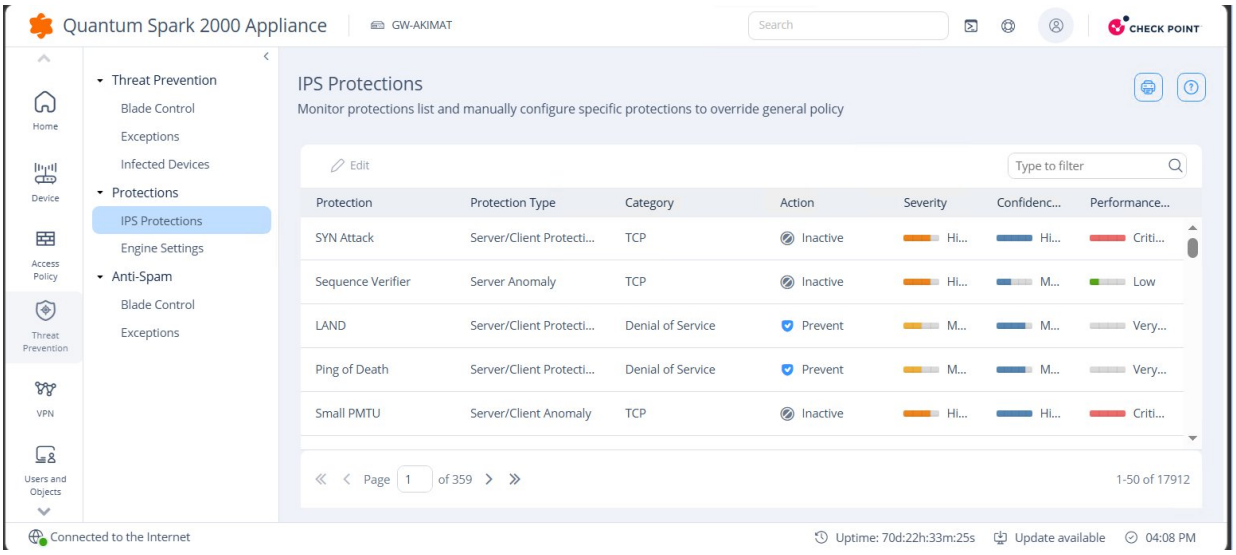


Рисунок 15. Перечень IPS Protections Check Point

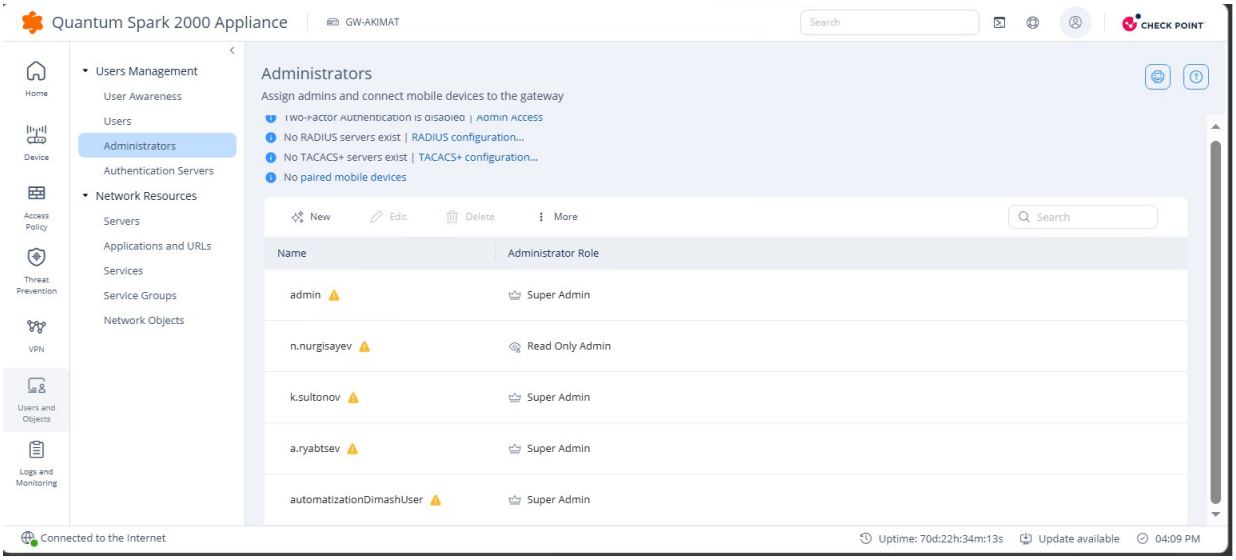


Рисунок 16. Администраторы и роли доступа Check Point

Отдельным подтверждающим материалом представлен реестр лицензий Check Point по 13 шлюзам Акимата. Реестр фиксирует наличие ключевых защитных модулей, включая Application Control, URL Filtering, User Awareness, IPS, Anti-Virus, Anti-Bot, Threat Emulation, Anti-Spam, Site-to-Site VPN и Firewall. Основная часть срочных лицензий действует до 01.12.2026; бессрочные позиции отражены отдельно в реестре.

Таблица 9. Функциональная матрица NGFW Check Point

№	Функция / требование	Подтверждение по интерфейсу Quantum Spark	Статус
1	Платформа и	Quantum Spark 2000	Подтверждено

DOC ID KZBW2Z1202600002013O1F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z1202600002013O1F66B3

	лицензирование	Appliance; версия R81.10.17 (996004721); лицензия активна; 9 active blades; 15 Internet connections; статус подключения к Internet - Connected.	
2	Firewall	В Security Dashboard модуль Firewall включен; журналирование Firewall-событий отображается в Security Logs.	Включено
3	Applications & URL Filtering	В Security Dashboard модуль Applications & URL Filtering включен; в Security Logs присутствуют события URL Filtering.	Включено
4	User Awareness	Модуль User Awareness включен; на панели отображается предупреждение No AD server.	Включено, требуется проверка AD-интеграции
5	Intrusion Prevention (IPS)	IPS включен; в Threat Prevention Blade Control статус IPS - Up to date; доступен перечень IPS Protections.	Включено
6	IPS Protections	В разделе IPS Protections отображается 17 912 защит; примеры: LAND - Prevent, Ping of Death - Prevent, SYN Attack - Inactive, Sequence Verifier - Inactive.	Настроено частично по политикам
7	Anti-Virus	Anti-Virus включен; в Threat Prevention Blade Control отображается статус Update available.	Включено, требуется обновление
8	Anti-Bot	Anti-Bot включен; статус Anti-Bot - Up to date.	Включено
9	Threat Emulation	Threat Emulation отображается в Security Dashboard и Threat	Отключено

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

		Prevention Blade Control как отключенный модуль.	
10	Anti-Spam	Anti-Spam включен в блоке Threat Prevention.	Включено
11	Remote Access VPN	Remote Access включен в блоке VPN.	Включено
12	Site-to-Site VPN	Site to Site VPN включен в блоке VPN.	Включено
13	QoS / SD-WAN / IoT	QoS, SD-WAN и IoT отображаются в Security Dashboard как отключенные.	Отключено
14	Security Logs	Раздел Security Logs доступен; отображаются события Accept/Drop, blades Firewall/URL Filtering, интерфейсы, source/destination, service и rule; визуальные материалы подтверждают наличие 23 732 записей журнала.	Журналирование активно
15	Администраторы и роли	В разделе Administrators отображаются учетные записи с ролями Super Admin и Read Only Admin; сервисная учетная запись автоматизации имеет роль Super Admin. Two-Factor Authentication disabled; RADIUS/TACACS+ servers не настроены.	RBAC настроен, MFA/RADIUS/TACACS+ требуют отдельного решения

14.1. Checkpoint - межсетевой экран

В отчетном периоде на шлюзах Check Point NGFW осуществлялся мониторинг сетевой активности, выявление вредоносного трафика и блокирование потенциально опасных соединений. Совокупно зарегистрировано 13 345 760 срабатываний защитных механизмов, в том числе Anti-Bot - 5 198 755, Anti-Virus - 6 956 569, IPS - 1 190 436. Наибольшая активность наблюдалась на шлюзе GW-AUEZOV.

Таблица 10. Зафиксированный активность в Межсетевом экране

№	Категория	Показатель	Значение

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

1	Общие события безопасности	Anti-Bot события	5 198 755
2	Общие события безопасности	Anti-Virus события	6 956 569
3	Общие события безопасности	IPS-инциденты	1 190 436

Анализ сетевой активности показывает преобладание приложений удаленного доступа, обмена файлами и проксирующих сервисов. Наиболее заметная нагрузка пришлась на приложение BitTorrent Protocol (сессии - 8 994 018, трафик - 121,4 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 11. Сетевая активность

№	Приложение	Сессии	Трафик
1	BitTorrent Protocol	7 046 112	34,0 ГБ
2	ZeroTier One	718 239	258,8 МБ
3	AnyDesk	377 268	2,5 ГБ
4	BitTorrent Sync	228 159	125,9 МБ
5	uTorrent	224 026	235,0 МБ
6	MediaGet	85 734	483,8 МБ
7	Radmin VPN	38 290	69,8 МБ
8	TeamViewer	35 438	1,1 ГБ
9	VeePN	2 917	36,3 МБ
10	iTop VPN	2 287	19,8 МБ

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, Trojan.Linux.RubyMiner.B, что указывает

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

на постоянный фон сетевых угроз в адрес инфраструктуры. Признаков массового заражения по итогам отчетного периода не выявлено.

Таблица 12. Заблокированный ВПО

№	Вредоносное ПО	События
1	Cryptominer.TC.9e2cUoIa	892
2	Infecting_URL.VDP.RS.TC.ed94skRK	441
3	Phorpiex.TC.345agexN	367
4	PUA.TC.3626Wodp	364
5	Phorpiex.TC.725ebNyK	337
6	Phorpiex.TC.6860TADZ	336
7	dga-QrAt8.TC.1651mzJp	272
8	Infecting_URL.VDP.RS.TC.5e7dWDBD	197
9	Infecting_URL.VDP.RS.TC.2f39TeWj	186
10	Infecting_URL.VDP.RS.TC.273akXKG	136

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

Таблица 13. Система предотвращения вторжений

№	Тип события	Сессии
1	TCP Segment Limit Enforcement	526 035
2	Max Ping Size	246 452
3	TCP Invalid Retransmission	53 802
4	Command Injection	7 492
5	ZMap Security Scanner	1 269
6	Cross-Site Scripting Over HTTP	443

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

7	Potential network configuration problem	430
8	Dasan GPON Router Authentication Bypass	252
9	TCP anomaly	163
10	Directory Traversal	117

15. Централизованное управление учетными записями и доступом / AD

Пункты ТС: Раздел 14.

По восстановленному доступу к доменному контроллеру выполнена эксплуатационная выгрузка Active Directory за отчетный период. Проверка охватила домен DC=int,DC=almaty,DC=kz, 3 доменных контроллера, 1315 учетных записей пользователей, 856 учетных записей компьютеров, 143 группы безопасности и 53 объекта групповых политик. В июне изменены 336 пользовательских учетных записей, 458 учетных записей компьютеров и 8 групп. Дополнительно проконтролированы заблокированные учетные записи (10), отключенные объекты (пользователи — 13, компьютеры — 17), устаревшие объекты без актуального входа (пользователи — 935, компьютеры — 342) и членство в привилегированных группах (18).

Таблица 14. Сводка Active Directory

№	Контрольная область	Показатель	Значение
1	Учетные записи пользователей	Всего / включено / отключено	1315 / 1302 / 13
2	Учетные записи пользователей	Заблокировано / изменено за июнь	10 / 336
3	Учетные записи компьютеров	Всего / включено / отключено	856 / 839 / 17
4	Учетные записи компьютеров	Устаревшие 90+ дней / изменено за июнь	342 / 458
5	Группы безопасности	Всего / изменено за июнь	143 / 8
6	Групповые политики	Всего / изменено за июнь	53 / 3
7	Привилегированный доступ	Членства в контролируемых привилегированных группах	18

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Сводка сформирована на основании контролируемой выгрузки с доменного контроллера и включает сведения об учетных записях пользователей и компьютеров, группах безопасности, объектах групповых политик, заблокированных и отключенных объектах, а также составе привилегированных групп. Административный доступ применялся только на период выполнения сбора сведений; секреты и учетные данные в отчетные материалы не включались.

16. SOAR: сценарии, playbook, интеграции, журнал действий, RBAC, TLS

Пункты ТС: 15.1-15.12.

В июне для оркестрации и автоматизации анализа событий безопасности используется Splunk SOAR. Elastic сохраняется как основной SIEM/EDR-контур для сбора, хранения, корреляции и первичного анализа событий, а Splunk SOAR вынесен в отдельный слой реагирования, поскольку в применяемой open-source/базовой конфигурации Elastic отсутствует полноценный SOAR-функционал для построения playbook, оркестрации действий и автоматизированного workflow реагирования. Релевантные события, индикаторы и результаты корреляции из контура мониторинга передаются в Splunk SOAR для автоматизированной проверки репутации объектов, обогащения данных, ветвления по уровню риска, формирования verdict, создания задач/инцидентов и фиксации действий SOC. Подтверждающими материалами являются схема автоматизированного workflow Splunk SOAR и перечень playbook, приведенный ниже.

DOC ID KZBW2Z120260000201301F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

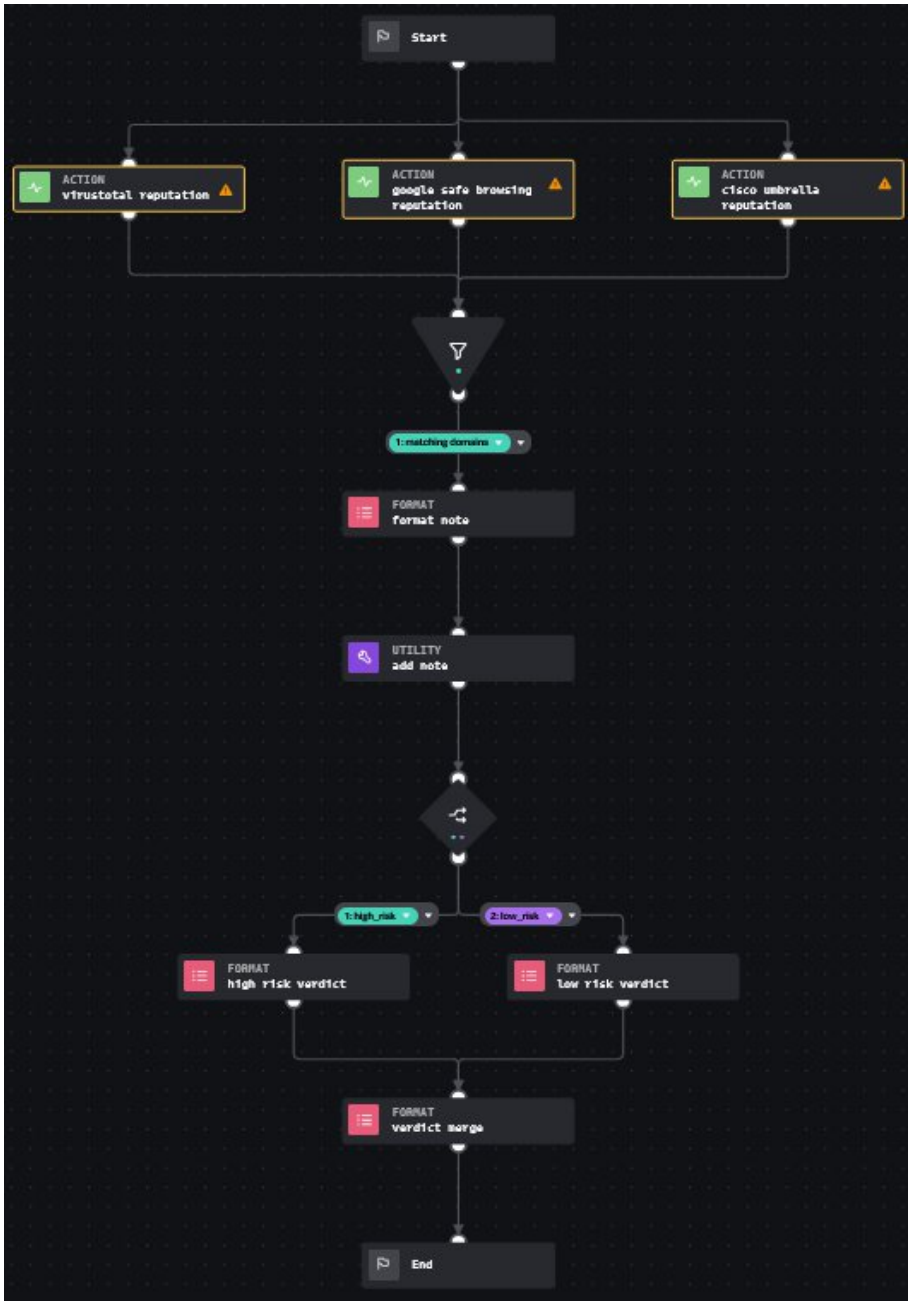


Рисунок 17. Сценарий автоматизации анализа событий в Splunk SOAR

На рисунке приведен пример workflow Splunk SOAR, в котором входящее событие проходит автоматизированные действия проверки через внешние источники репутации, последующее ветвление по уровню риска и формирование итоговой заметки/verdict. Такая логика используется для ускорения первичного анализа, унификации действий аналитика и сохранения проверяемой последовательности реагирования по событиям безопасности.

Таблица 15. Перечень playbook Splunk SOAR

№	Playbook	Контур	Назначение
1	Automated_Enrichment	Обогащение инцидента	Открывает событие и

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

			запускает dispatch-сценарии Reputation Analysis, Attribute Lookup и Related Tickets для первичного обогащения.
2	Identifier_Reputation_Analysis_Dispatch	Репутационный анализ IOC	Определяет доступные индикаторы и маршрутизирует их в playbook проверки репутации URL, IP, доменов и хэшей.
3	AD_LDAP_Entity_Attribute_Lookup	Active Directory	Выполняет поиск атрибутов пользователя или устройства и формирует нормализованный вывод по AD-объекту.
4	AD_LDAP_Account_Locking	Active Directory	Выполняет блокировку учетной записи Microsoft LDAP Active Directory и возвращает результат действия.
5	AD_LDAP_Account_Unlocking	Active Directory	Выполняет разблокировку учетной записи Microsoft LDAP Active Directory и возвращает результат действия.
6	activedirectory_reset_password	Active Directory	Сценарий сброса пароля

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

			потенциально скомпрометированной учетной записи после подтверждения аналитиком.
7	excessive_account_lockouts_enrichment_and_response	Account Monitoring	Обогащает события массовых блокировок учетных записей, выполняет расследование и поддерживает реагирование через WinRM/Splunk.
8	risk_notable_auto_investigate	Risk Notable	Запускает автоматическое расследование risk notable по заданному порогу риска.
9	risk_notable_auto_containment	Risk Notable	Реализует containment для активов и идентификаторов при высоком риске или подтвержденной угрозе.
10	risk_notable_block_indicators	Risk Notable	Определяет индикаторы, требующие блокировки, и подбирает соответствующие блокирующие playbook.
11	VirusTotal_v3_Identifier_Reputation_Analysis	Threat Intelligence	Проверяет репутацию URL, IP, домена или файлового хэша через VirusTotal

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

			v3 и формирует нормализованный score.
12	VirusTotal_v3_Dynamic_Analysis	Threat Intelligence	Выполняет динамический анализ URL или объекта в sandbox VirusTotal и формирует отчет по observable.
13	UrlScan_IO_Dynamic_Analysis	URL analysis	Выполняет detonation/анализ URL через urlscan.io с формированием глобального и per-observable отчета.
14	user_prompt_and_block_domain	Network blocking	Оценивает риск домена и после подтверждения пользователя выполняет временную блокировку домена.
15	zscaler_hunt_and_block_url	Web security	Ищет внутренние устройства, обращавшиеся к подозрительному URL, и поддерживает блокировку URL через Zscaler.
16	ServiceNow_Create_Incident	ITSM / Incident management	Создает инцидент в ServiceNow по результатам автоматизации и передает сводку расследования.

Перечень сформирован по выгрузке интерфейса Splunk SOAR 8.4.0.166 и используется как подтверждение наличия сценариев оркестрации, обогащения,

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

реагирования, работы с AD, репутационной проверки индикаторов, containment и создания инцидентов.

17. Кибербразведка, IOC, запросы и рекомендации

Пункты ТС: 1.1.27, MISP/OpenCTI/АО "ГТС".

Раздел содержит исходные материалы OpenCTI, MISP и T-Lab. За отчетный период запросы от АО «ГТС» не поступали. При поступлении запросов в последующих периодах необходимо прикладывать отдельный журнал с датой, темой, IOC, рекомендациями, сроком ответа и итоговым статусом исполнения.

17.1. OpenCTI — Платформа кибербразведки

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

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

По результатам текущего анализа и расследования инцидентов выявленные индикаторы компрометации (IP-адреса, хэши файлов, домены, URL, имена процессов и иные артефакты) были проанализированы и добавлены в базу OpenCTI, что обеспечивает их последующее использование при корреляции событий, threat hunting и автоматизированном выявлении схожих угроз в инфраструктуре.

DOC ID KZBW2Z1202600002013O1F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

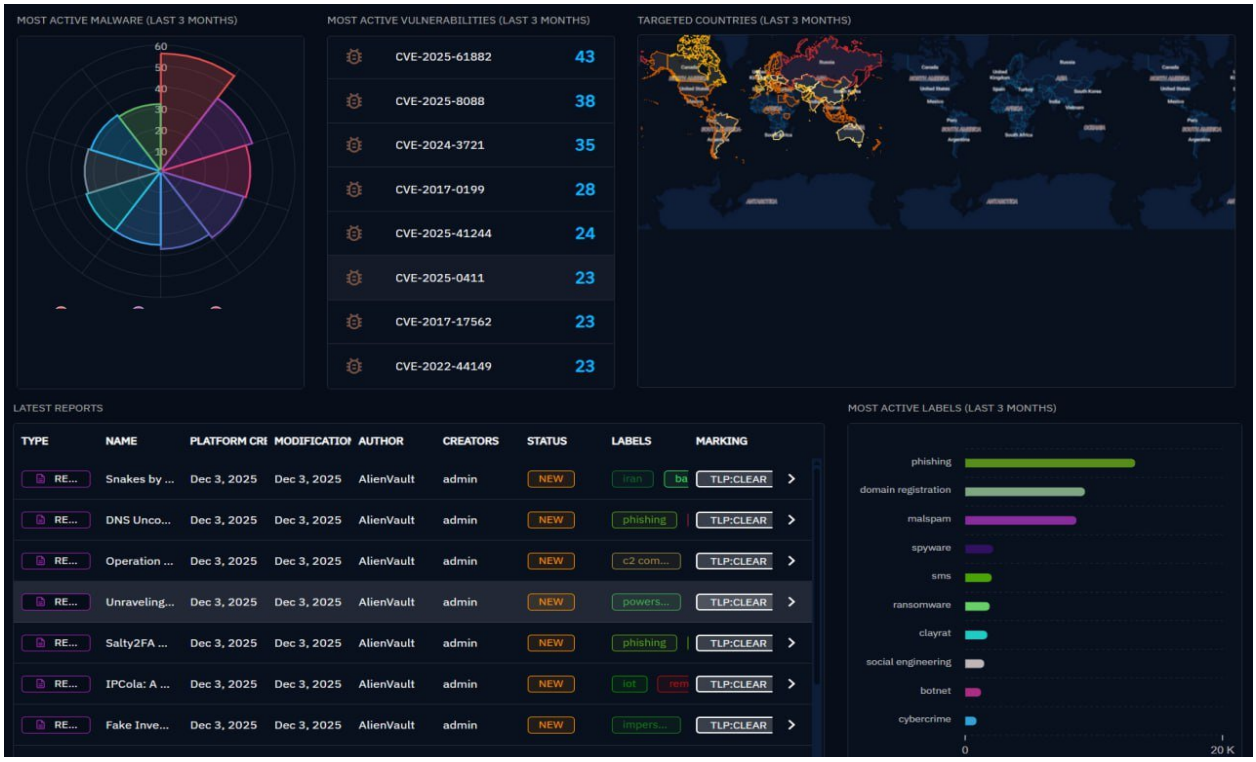


Рисунок 18. Информация с OpenCTI

В отчетном периоде выполнена интеграция платформы OpenCTI с SIEM-системой Заказчика: обеспечена автоматизированная передача и корреляция индикаторов компрометации из OpenCTI с событиями SIEM, за счет чего организован результативный мониторинг релевантных IoC в инфраструктуре. 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.

17.2. MISP — Обмен индикаторами компрометации

На стороне Поставщика функционирует и поддерживается платформа MISP, посредством которой осуществляется обмен индикаторами компрометации и обработка обращений SOC НКЦИБ (ЕШДИ). Поставщиком (ОЦИБ) обеспечивается постоянный мониторинг поступающих событий и их отработка в рамках действующих процедур реагирования: каждое обращение анализируется на предмет вредоносной активности, при необходимости выполняется корреляция индикаторов компрометации с телеметрией внутренних узлов средствами мониторинга, NGFW/IPS и EDR. За отчетный период под мониторингом находилось 289 событий MISP. По состоянию на конец периода: закрыто со стороны НКЦИБ — 8; на сопровождении (в работе) — 281 (в том числе «в работе» — 165, «на проверке» — 65, «открыто» — 51). По 18 событиям Поставщиком предоставлены заключения (всего 47 комментариев по результатам анализа), в том числе по 2 событиям по результатам корреляции подтвержден ложноположительный характер срабатываний. Основные категории обрабатываемых обращений: перечни C&C-серверов — 69, перечни

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

распространителей спама — 77, атаки на веб- и сетевые сервисы по данным ЕШДИ — 77, еженедельная статистика KZ-CERT — 49, ботнет-активность — 6. Наиболее значимые обращения, обработанные Поставщиком в отчетном периоде (с предоставлением заключений), приведены в таблице ниже.

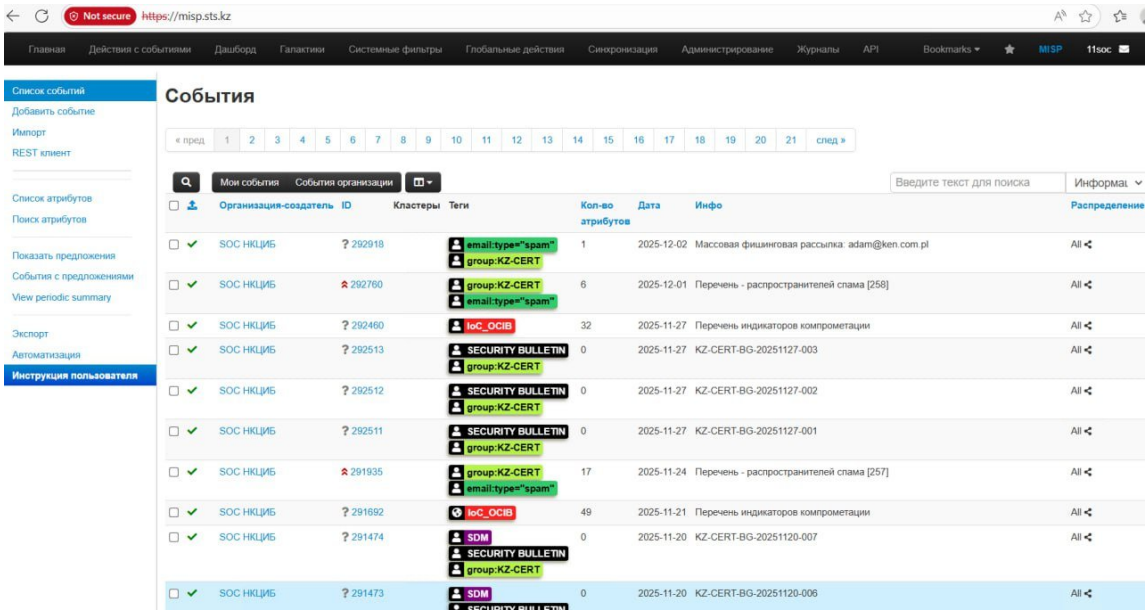


Рисунок 19. MISP

Таблица 16. Наиболее значимые события MISP, обработанные в отчетном периоде

№	Событие	Дата	Тип / сигнатура	Статус	Вывод
1	№323172	2026-06-30	Ботнет-активность	В работе	Заключение предоставлено
2	№323162	2026-06-30	Атака: Multiple.Web.Servers.CVE-2026-49975.HTTP2.Bomb.DoS	В работе	Заключение предоставлено
3	№323161	2026-06-30	Атака: Multiple.Web.Servers.CVE-2026-49975.HTTP2.Bomb.DoS	В работе	Заключение предоставлено

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

4	№323139	2026-06-30	Атака: Multiple.Web.Servers.CVE-2026-49975.HTTP2.Bomb.DoS	На проверке	Заключение предоставлено
5	№323127	2026-06-30	Атака: Multiple.Web.Servers.CVE-2026-49975.HTTP2.Bomb.DoS	В работе	Заключение предоставлено
6	№322819	2026-06-29	Атака: Multiple.Web.Servers.CVE-2026-49975.HTTP2.Bomb.DoS	Закрыто (НКЦИБ)	Закрыто
7	№322818	2026-06-29	Атака: Multiple.Web.Servers.CVE-2026-49975.HTTP2.Bomb.DoS	Закрыто (НКЦИБ)	Закрыто
8	№322443	2026-06-28	Атака: MS.IE.Var.Object.Recycle.Memory.Corruption	Закрыто (НКЦИБ)	Ложноположительное
9	№322309	2026-06-26	Ботнет-активность	Закрыто (НКЦИБ)	Закрыто
10	№322294	2026-06-26	Атака: Multiple.Web.Servers.CVE-2026-49975.HTTP2.Bomb.DoS	Закрыто (НКЦИБ)	Закрыто

Полная статистика по событиям MISP (распределение по статусам, категориям и периодам, а также перечень обращений с предоставленными заключениями) приведена в Приложении 11.

17.3. 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

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business
DOC ID KZBW2Z120260000201301F66B3

мониторинга и реагирования. В отчетном периоде система анализа угроз в режиме реального времени выявила 257 угроз и 319 подозрительных объектов, при общем количестве 13186 проверенных файлов/объектов. Активность носила равномерный характер в течение месяца. Основную долю проверяемых объектов составили текстовые файлы и исполняемые файлы. В выборку отчетного периода вошло 64 отчета T-Lab; максимальная оценка риска по статистике платформы составила 128.32, сформировано 24 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 - 13 186, из них 257 классифицированы как вредоносные, 319 отнесены к подозрительным, а 12 610 не имели признаков вредоносной активности. Доля вредоносных объектов составила 1.95%, доля подозрительных - 2.42%. 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 для сопоставления общего числа проверок, количества подозрительных результатов и числа IOC в одном месте без детализации по каждому отдельному файлу.

Таблица 17. Сводные показатели T-Lab Sandbox

Показатель	Значение	Комментарий
Проверено объектов	13 186	Общее количество объектов
Вредоносные объекты	257	Классифицированы как вредоносные
Подозрительные объекты	319	Требуют дополнительной проверки
Безопасные объекты	12 610	Без признаков вредоносной активности
Отчетов T-Lab	64	Учтено в выборке

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

Сформировано IOC (SHA-256)	24	Технические индикаторы
Максимальная оценка риска	128.32	По статистике платформы

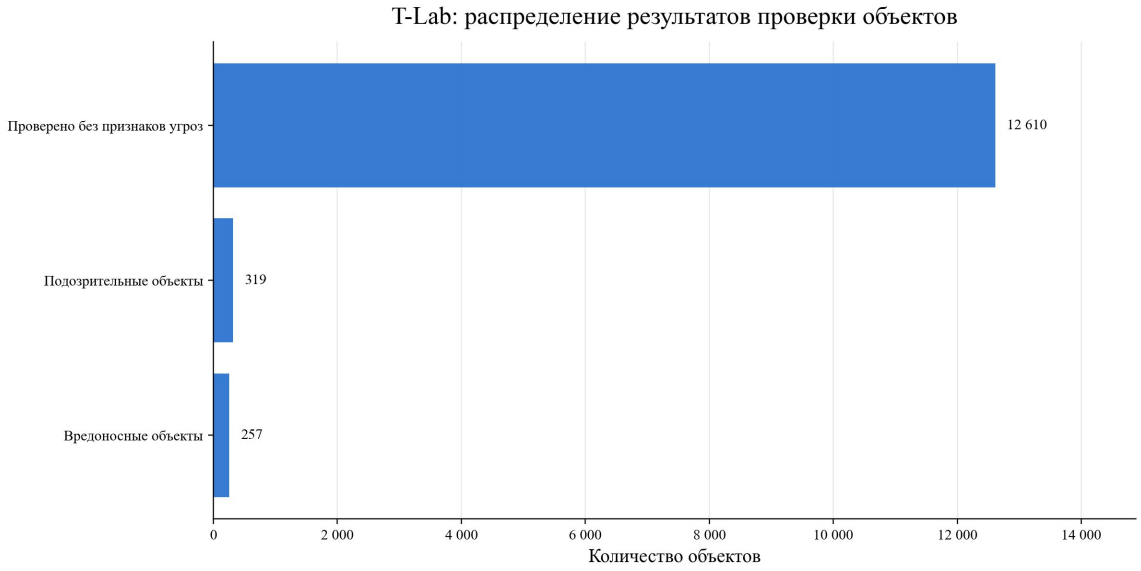


Рисунок 20. Распределение результатов проверки T-Lab

На диаграмме распределения результатов проверки показано, как общий поток из 13 186 объектов разделился по итоговым verdict-статусам T-Lab. Безопасная часть выборки составила 12 610 объектов, вредоносная - 257, подозрительная - 319. 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.

DOC ID KZBW2Z120260000201301F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

Рисунок 21. 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 149 временных интервалов, из которых 141 содержали фактические отчеты, 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.

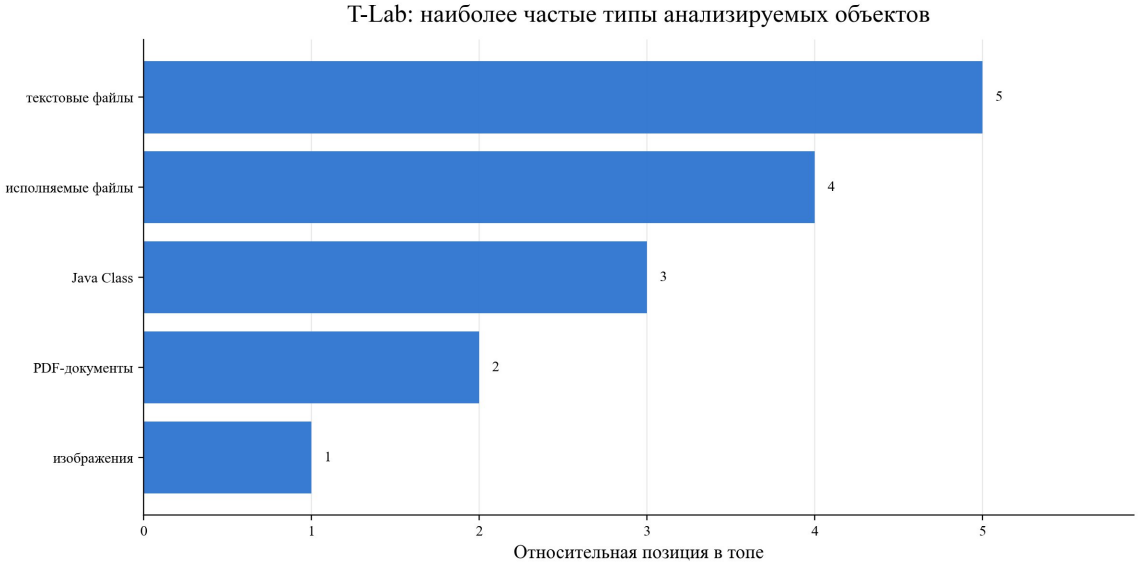


Рисунок 22. Наиболее частые типы анализируемых объектов T-Lab

На диаграмме типов объектов показано, какие форматы файлов чаще всего поступали в T-Lab на динамический или статический анализ. В текущем периоде

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

среди наиболее частых типов указаны: текстовые файлы, исполняемые файлы, Java Class, 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 18. Наиболее частые типы анализируемых объектов T-Lab

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

Блок IOC содержит первые 10 SHA-256 индикаторов из 21 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 19. IOC

№	Тип индикатора	Значение
1	File Hash (SHA-256)	b1f155711432f2f21c8e4bda1a131cfdd311e6d25a5f68a695325b2400904c75

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

2	File Hash (SHA-256)	5fb09fdada99a771618cc9ab222b07244e8b87f1572f76de95132807aaefd41f
3	File Hash (SHA-256)	addd688f104a64461579b8fa7cf1de44a8bddff0fd56807c6a87e909d86ccc56
4	File Hash (SHA-256)	08afd013eb9c375e9b8ffbc6308eb7b469ff140fa0fb02bdc9022f72168e0f82
5	File Hash (SHA-256)	6f8186c882326e7c1c535d02d3ee9bd93dccfd9824ede9f763d2ee942582eac3
6	File Hash (SHA-256)	435a4b9c3a484a7a842e2d2747658c55a3b31805ff19828633f3737e32f203a8
7	File Hash (SHA-256)	7c494ac1303a2220bbe298b6ad29be433931acfb516447db62d0d15830164add
8	File Hash (SHA-256)	131c3f58635c9f814b1c4b70bf99bae046b0475acb8807c9cafdcb7d9c50fff2
9	File Hash (SHA-256)	6a6275dbf0789110e38cfcedf1fb67f2ace208e3735b222ff5f9c9aae04b500a
10	File Hash (SHA-256)	296e234dae727d659ccdd9f07ec90803de7861ae422871740ae0a0d2ad770d32

Примечание: Смотреть подробный отчет T-Lab в Приложении 7

18. Система защиты конфиденциальных данных от утечки (DLP)

Раздел DLP сохранен из исходного майского отчета, так как Safetica DLP является отдельным направлением услуги и подтверждается Приложением 8. Данные отражают события контроля операций с данными за период 01.06.2026-30.06.2026.

18.1. DLP – Предотвращение утечек данных (safetica)

В ходе анализа телеметрии, поступающей с рабочих станций в систему предотвращения утечек данных Safetica, за отчетный период зафиксировано 252 494 события контроля операций с данными. Диапазон наблюдения по выгрузке: 01.06.2026 - 30.06.2026. Наиболее активные пользователи: УГМ, ПК, усиб, Sayat Kuanyshbekov, aika_. Основные приложения: Google Chrome (chrome.exe), Проводник (explorer.exe), Microsoft Word (WINWORD.EXE), Firefox (firefox.exe), Microsoft Word (WINWORD.EXE). Совокупный объем передачи данных составил 2,0 ТБ; отдельно выделены веб-риски, операции передачи данных и служебная активность приложений. Объекты среднего и высокого приоритета в разделе рассматриваются как кандидаты на ручную проверку, а не как

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

подтвержденные факты утечки. По данным Safetica за отчетный период зафиксировано 252 494 операции контроля данных и 481 901 операция передачи данных. Основные каналы передачи: Съемные USB-носители, Печать, Веб-загрузка. Наибольшая веб-активность приходится на категории: Веб-приложения для мгновенных сообщений, Веб-порталы, Внутренняя сеть. Подробная выгрузка Safetica приведена в Приложении 8.

18.2. Анализ веб – активности

В отчетном периоде по направлению веб-активности выделено 25 объектов среднего и высокого приоритета для дополнительной проверки. 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, chatgpt.com, youtube.com. В перечень объектов, требующих дополнительной проверки, вошли веб-ресурсы almaty.qujat.gov.kz, eotinish.gov.kz, chatgpt.com и приложения Half-Life Launcher (hl.exe), Solitaire.exe, AnyDesk (AnyDesk.exe), cs2.exe, SupremoHelper.exe. Отдельного внимания требуют категории инструментов ИИ, мессенджеров, игровых приложений и средств удаленного доступа: часть такой активности может быть рабочей, но для DLP-контроля она должна быть сопоставлена с должностными задачами пользователя и разрешенными бизнес-сценариями. Такая детализация используется для разграничения штатной веб-активности, облачных сервисов и ресурсов с повышенным DLP-риск-профилем.

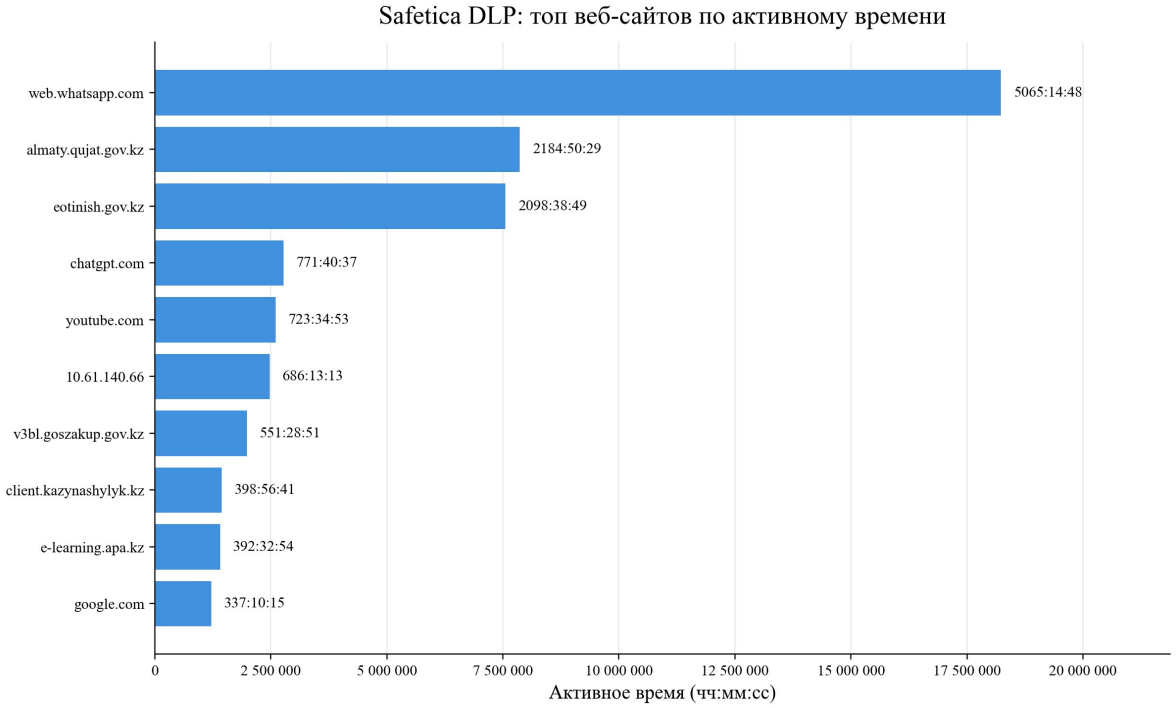


Рисунок 23. Веб-сайты

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 5065:14:48

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

(чч:мм:сс, накопительно по всем пользователям) и охватом 563 пользователя. 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 охвату пользователей. Такая структура показывает, какие веб-ресурсы сформировали основную часть наблюдаемой веб-активности в Safetica за отчетный период.

Таблица 20. Топ веб-ресурсов по активному времени пользователей

№	Веб-ресурс	Категория	Активное время (чч:мм:сс)	Пользователи
1	web.whatsapp.com	Веб-приложения для мгновенных сообщений	5065:14:48	563
2	almaty.qujat.gov.kz	Веб-порталы	2184:50:29	267
3	eotinish.gov.kz	Веб-порталы	2098:38:49	245
4	chatgpt.com	Инструменты ИИ	771:40:37	409
5	youtube.com	Досуг	723:34:53	315
6	10.61.140.66	Внутренняя сеть	686:13:13	133

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

7	v3bl.goszakup.gov.kz	Правительство, закон и религия	551:28:51	134
8	client.kazynashylyk.kz	Не установлено	398:56:41	52
9	e-learning.apa.kz	Не установлено	392:32:54	192
10	google.com	Поисковые системы	337:10:15	543

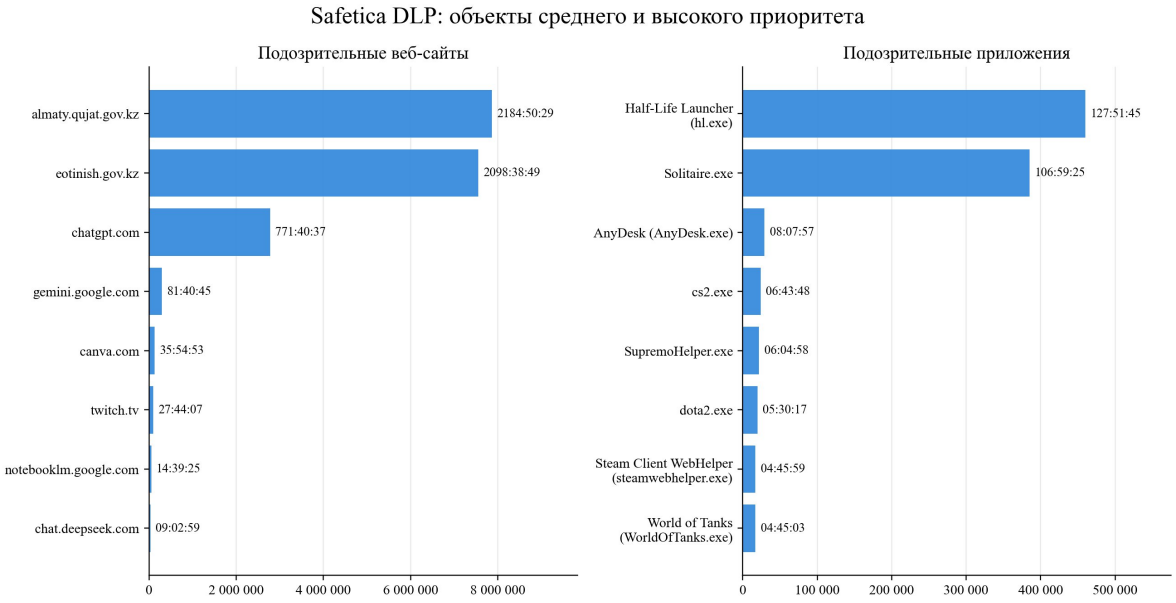


Рисунок 24. Объекты Safetica средней и высокой степени важности

На диаграмме средней и высокой степени важности объединены веб-сайты и приложения, которые Safetica выделила в отдельный отчет по этому признаку. Наиболее заметные объекты в текущей выборке: веб-ресурс almaty.qujat.gov.kz и приложение Solitaire.exe. В левой части рисунка представлены веб-сайты, отмеченные Safetica как объекты повышенного внимания, в правой части - аналогичные приложения. Отдельно отметим: по данным Safetica оба государственных портала (almaty.qujat.gov.kz, eotinish.gov.kz) относятся к обычной категории «Веб-порталы», признаков вредоносной или запрещенной активности по ним не зафиксировано - то есть попадание в перечень не означает вредоносности. При этом по обоим ресурсам зафиксировано очень высокое суммарное активное время пользователей (2-е и 3-е место по этому показателю во всей выгрузке), что, по всей видимости, и стало основанием для включения в выборку; точный алгоритм отбора Safetica не раскрывает. Для каждого объекта отображается активное время, а также дополнительная информация о категории

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

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 21. Объекты Safetica среднего и высокого приоритета

№	Тип	Объект	Категория	Активное время (чч:мм:сс)	Пользователи
1	Веб-сайт	almaty.qujat.gov.kz	Веб-порталы	2184:50:29	267
2	Веб-сайт	eotinish.gov.kz	Веб-порталы	2098:38:49	245
3	Веб-сайт	chatgpt.com	Инструменты ИИ	771:40:37	409
4	Веб-сайт	gemini.google.com	Инструменты ИИ	81:40:45	62
5	Веб-сайт	canva.com	Инструменты ИИ	35:54:53	24
6	Веб-сайт	twitch.tv	Финансовый	27:44:07	4
7	Веб-сайт	notebooklm.google.com	Инструменты ИИ	14:39:25	12

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

8	Веб-сайт	chat.deepseek.com	Инструменты ИИ	9:02:59	10
9	Приложение	Half-Life Launcher (hl.exe)	Игры	127:51:45	19
10	Приложение	Solitaire.exe	Игры	106:59:25	16
11	Приложение	AnyDesk (AnyDesk.exe)	VPN клиент	8:07:57	54
12	Приложение	cs2.exe	Кейлоггер	6:43:48	3
13	Приложение	SupremoHelper.exe	VPN клиент	6:04:58	1
14	Приложение	dota2.exe	Игры	5:30:17	1
15	Приложение	Steam Client WebHelper (steamwebhelper.exe)	Игры	4:45:59	17

18.3. Передачи данных

По операциям передачи данных зафиксировано 481 901 событие. Основные каналы передачи: Съемные USB-носители, Печать, Веб-загрузка, Мессенджеры. События используются для оценки рисков несанкционированного перемещения информации и уточнения DLP-политик.

DOC ID KZBW2Z120260000201301F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

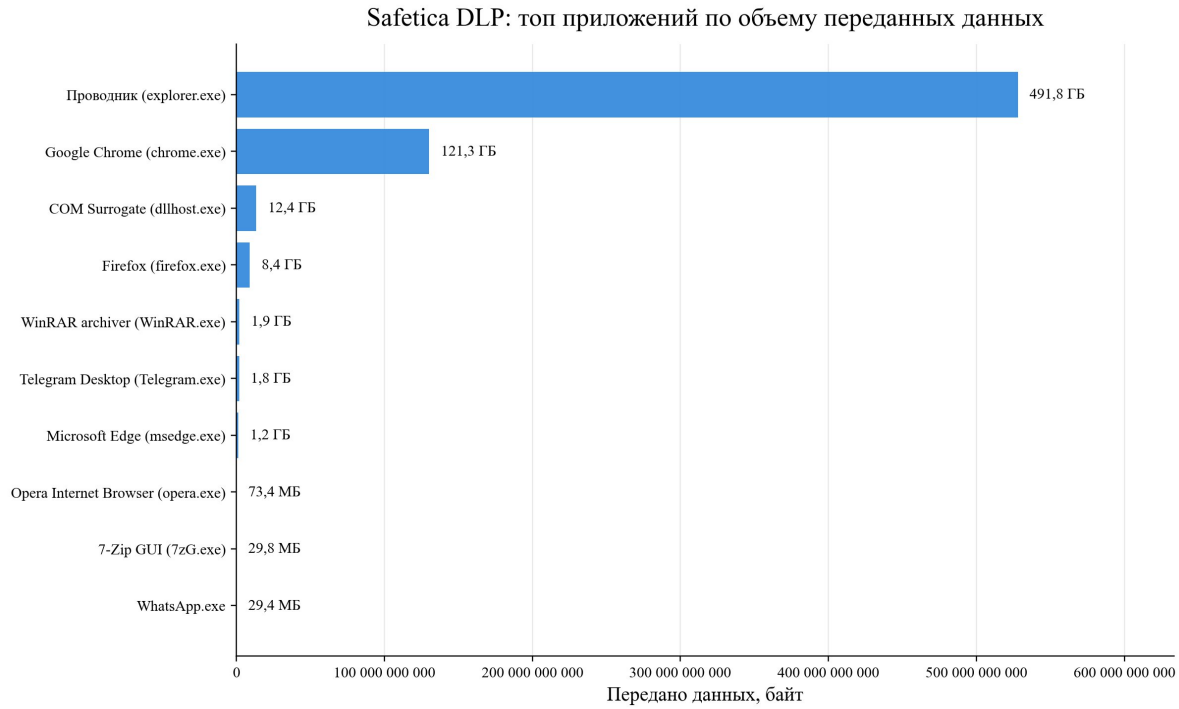


Рисунок 25. Топ-10 приложений

На диаграмме передачи данных показаны приложения, сформировавшие основной объем операций с данными в отчетном периоде. Лидирующее приложение: Проводник (explorer.exe) с объемом 491,8 ГБ; далее в верхней части выборки находятся Google Chrome (chrome.exe) и COM Surrogate (dllhost.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 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 2,0 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 22. Распределение объема переданных данных по основным пользовательским и системным приложениям

DOC ID KZBW2Z1202600002013O1F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z1202600002013O1F66B3

№	Приложение	Категория	Объем переданных данных (итого)	Средний объем в активный день	Пользователи
1	Проводник (explorer.exe)	Windows	491,8 ГБ	15,9 ГБ	313
2	Google Chrome (chrome.exe)	Веб-браузер	121,3 ГБ	3,9 ГБ	302
3	COM Surrogate (dllhost.exe)	Не указано	12,4 ГБ	409,5 МБ	39
4	Firefox (firefox.exe)	Веб-браузер	8,4 ГБ	276,7 МБ	77
5	WinRAR archiver (WinRAR.exe)	Не указано	1,9 ГБ	62,7 МБ	14
6	Telegram Desktop (Telegram.exe)	Не указано	1,8 ГБ	58,5 МБ	1
7	Microsoft Edge (msedge.exe)	Веб-браузер	1,2 ГБ	40,6 МБ	73
8	Opera Internet Browser (opera.exe)	Не указано	73,4 МБ	2,4 МБ	4
9	7-Zip GUI (7zG.exe)	Не указано	29,8 МБ	985,4 КБ	1
10	WhatsApp.exe	Мгновенные сообщения и интернет-телефония (VOIP)	29,4 МБ	970,7 КБ	6

DOC ID KZBW2Z120260000201301F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

18.4. Служебные операции через интернет и внутренние сервисы

По служебным операциям и активности приложений в поведенческую выборку Safetica включено 137 пользователей. Наибольшая активность отмечалась в приложениях Google Chrome (chrome.exe), Проводник (explorer.exe), Microsoft Word (WINWORD.EXE), Firefox (firefox.exe), Microsoft Word (WINWORD.EXE). Максимальное активное время пользователя за период: Guest JETS - 426:43:44; доля подозрительной активности по данному пользователю составила 0.0%. В отдельный список для проверки попали приложения Half-Life Launcher (hl.exe), Solitaire.exe, AnyDesk (AnyDesk.exe), cs2.exe, SupremoHelper.exe, включая игровые приложения, средства удаленного доступа или сервисы, требующие проверки на соответствие рабочему профилю. Полученные значения используются для приоритизации ручной проверки пользователей, уточнения исключений DLP-политик и настройки допустимых сценариев работы с веб-сервисами, файлами и приложениями.

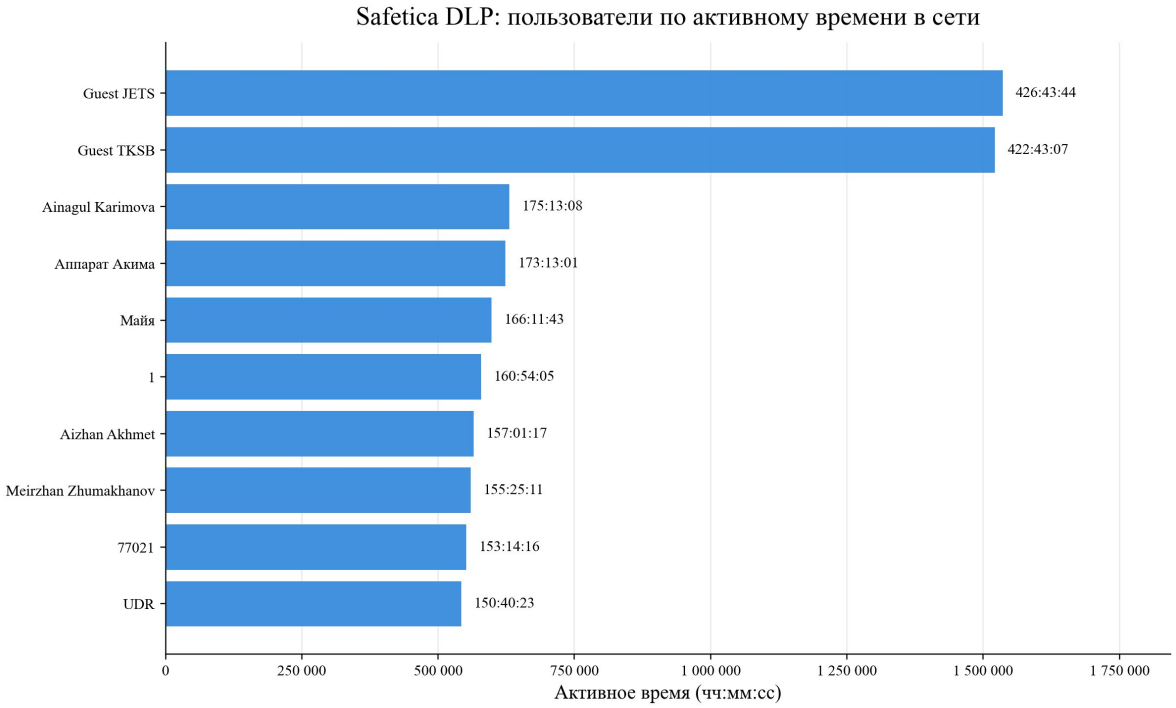


Рисунок 26. Время нахождения пользователя в сети

На диаграмме пользовательской активности показаны пользователи с максимальным суммарным временем работы в сети за отчетный период. Лидирующий пользователь: DeLux@Buh2 с активным временем 148:05:43; также в верхней части выборки находятся Госзакупка@DESKTOP-6L825P7 и ПК@DESKTOP-P3IF86U. 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.

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

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 23. Сетевая активность пользователя

№	Пользователь	Активные дни	Общее активное время	Подозрительная активность	Доля подозрительной активности
1	Guest JETS	23	426:43:44	0:00:28	0.0%
2	Guest TKSB	25	422:43:07	1:31:45	0.4%
3	Ainagul Karimova	22	175:13:08	0:31:23	0.3%
4	Аппарат Акима	24	173:13:01	0:07:20	0.1%
5	Майя	22	166:11:43	0:00:13	0.0%
6	1	22	160:54:05	0:36:23	0.4%
7	Aizhan Akhmet	23	157:01:17	0:28:55	0.3%
8	Meirzhan Zhumakhanov	22	155:25:11	0:01:08	0.0%
9	77021	22	153:14:16	0:19:26	0.2%
10	UDR	23	150:40:23	0:00:08	0.0%

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

19. Перечень приложений и подтверждающих материалов

Таблица 24. Перечень приложений к отчету за июнь 2026 года

№	Наименование	Что подтверждает
Приложение 1	Правила корреляции	Срабатывания правил SIEM/EDR и покрытие сценариев мониторинга
Приложение 2	Перечень обработанных инцидентов (кейсов)	Регистрация, обработка и статус кейсов за июнь
Приложение 3	Проанализированные программы в рамках мониторинга	Endpoint-аналитика и программная активность
Приложение 4	Статистика уязвимостей	Сводная статистика Nessus по подразделениям и уровням критичности
Приложение 5	Сканирование внутренней сети	Результаты внутреннего инструментального сканирования
Приложение 6	Сканирование внешней сети	Результаты внешнего сканирования
Приложение 7	Информация с системы защиты от целевых атак и атак нулевого дня	Sandbox-анализ, угрозы, подозрительные объекты и IOC
Приложение 8	Информация с DLP	Выгрузка Safetica DLP за июнь
Приложение 9	Статус реализации	Состояние основных направлений услуги
Приложение 10	Справка о резервном копировании и репликации AD	Состояние служб AD/VSS/DNS/KDC на DC (AKMT-VS-1001, int.almaty.kz), теневые копии, задания резервирования, статус VSS
Приложение 11	Статистика по MISP событиям	Сводная статистика и перечень обработанных событий MISP за июнь

20. Отдельные подтверждающие документы

Ниже перечислены материалы, которые предоставляются отдельным комплектом и подтверждают процессные, проектные и организационные требования Технической спецификации: лицензирование средств защиты, техническая документация по ИБ, схемы сети (L3), Регламент взаимодействия, отчет по аудиту ИБ и материалы переписки с Заказчиком.

Таблица 25. Материалы, предоставляемые отдельным комплектом

Блок	Статус и подтверждающие материалы
Retention / архивы	Параметры хранения журналов и порядок передачи

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

журналов	архивов должны быть закреплены отдельным техническим приложением с указанием сроков retention, ответственных лиц и процедуры предоставления архивных данных.
BCP/DRP	По данным выгрузки с DC AKMT-VS-1001 (int.almaty.kz) от 01.07.2026: ключевые службы Active Directory (NTDS, KDC, Netlogon, DNS) функционируют в штатном режиме. Служба VSS запущена; теневые копии томов на DC не обнаружены (0 снимков). Плановые задания резервного копирования в Task Scheduler не выявлены. Проверить наличие Windows Server Backup или стороннего ПО резервирования и настроить регулярные снимки VSS/резервные копии DC. Подробности — Приложение 10 «Справка о резервном копировании и репликации AD».
PAM/bastion	Направление PAM/bastion находится в проработке. Для полного закрытия требуется архитектура, матрица ролей, перечень подключенных систем, порядок MFA/ротации секретов и журналы привилегированных сессий.
Обучение	Исполнителем направлен запрос Заказчику о предоставлении списка участников. После согласования прикладываются программа обучения, материалы, список участников и акт либо ведомость проведения.
SOAR	Подтверждено разделом 16: представлена схема автоматизированного workflow Splunk SOAR, перечень playbook, описание интеграций, RBAC/TLS и журналируемых автоматических действий.
AD	Подтверждено разделом 15: выполнена эксплуатационная проверка AD с доменного контроллера, отражены учетные записи, GPO, изменения за июнь, блокировки, отключенные объекты и привилегированные группы.
NGFW функциональная матрица	Подтверждено разделом 14: сформирована функциональная матрица NGFW, отражены IPS, Anti-Virus, Anti-Bot, URL Filtering/App Control, VPN, logging, role-based admins и эксплуатационные данные Check Point.
Лицензирование Check Point NGFW	Предоставлен реестр лицензий по 13 шлюзам Check Point Акимата, подтверждающий состав активных

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

	защитных модулей, SKU и сроки действия лицензий.
Комплект технической документации по ИБ	Предоставлен комплект ТД ИБ: политика ИБ, правила классификации активов, методика оценки рисков, внутренний аудит ИБ, криптографическая защита, управление доступом/активами/изменениями, аутентификация, непрерывность, антивирусный контроль, физическая защита, резервное копирование, управление рисками, мониторинг событий и инцидентов, руководства администратора, каталог угроз, проект приказа и проект служебной записки.
Переписка и материалы, направленные Заказчику	Предоставлены исходящие и сопроводительные письма, материалы по AD, агентам, аудиту ИБ, проблемным вопросам по хостам и уведомлению о плановых технических работах. Материалы используются как подтверждение организационного взаимодействия и исполнения процессных пунктов ТС.
Регламент взаимодействия	Предоставлен Регламент взаимодействия между ТОО «MSSP.GL» и Заказчиком, закрепляющий порядок оказания услуг, маршруты эскалации, SLA и каналы коммуникаций. Подтверждает исполнение пунктов ТС 1.2.2, 1.2.7–1.2.8, 5.1 (регламенты, SLA, планы работ и порядок взаимодействия).
Схемы сети (L3)	Предоставлены логические L3-схемы сети: основная площадка Акимата. Схемы подтверждают архитектуру сегментации, периметровые шлюзы Check Point, L3-коммутацию MikroTik и VPN-связность управлений (ТС 11.1–11.3). Рисунок 10 отчета содержит схему основной сети.

21. Выводы и рекомендации

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.

Отдельно сформирован перечень пунктов, учтенных при корректировке отчета и комплекта подтверждающих материалов. В перечень включены замечания по полноте мониторинга, доступности MDR, управлению уязвимостями, контролю привилегированного доступа, обучению и процессам

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000201301F66B3

информационной безопасности. Детальная матрица замечаний, статусов и подтверждающих материалов приведена в разделе 20 (Таблица 25).

21.1. Общие выводы

На отдельных шлюзах фиксировалось использование приложений удаленного доступа, VPN и P2P-обмена, включая BitTorrent Protocol, ZeroTier One, AnyDesk. Выявленные вредоносные объекты своевременно блокировались средствами Check Point. IPS фиксировала типовые сценарии сетевого воздействия, при этом признаков успешной эксплуатации уязвимостей не выявлено. Под мониторингом находилось 693 активных агентов; offline - 268, нестабильных/требующих проверки - 53. За отчетный период зарегистрировано 383 событий уровня high/critical. По данным Nessus в отчетном периоде выявлено 41 критических и 157 высоких уязвимостей.

21.2. Приоритетные планы работ

Продолжить актуализацию и оптимизацию правил корреляции в SIEM с учетом 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, ZeroTier One, AnyDesk в инфраструктуре Заказчика. Проведение тестирование на проникновения в октябре 2026 года.

21.3. Рекомендации

Продолжить контроль и актуализацию политик Check Point NGFW с акцентом на risky applications, VPN и P2P-категории. Перепроверить необходимость использования приложений BitTorrent Protocol, ZeroTier One, AnyDesk 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 «First Time Seen Removable Device».

DOC ID KZBW2Z120260000201301F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z120260000201301F66B3
Тип документа	Исходящее письмо
Тема	Отчеты за июнь 2026 года
Статус	Отправлен
Рег. Номер:	01-01/258
Рег. Дата:	08.07.2026
Количество страниц	74
Подписи	2

Информация об отправителе

Отправитель	ТОО "MSSP.GL"
IP-адрес	185.143.21.26

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	185.143.21.26
Email	d.salipov@mssp.global
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIW/AYJ...goCE/ZfI=
Дата подписания	08.07.2026 10:08

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Генеральный директор
IP-адрес	185.143.21.26
Email	d.salipov@mssp.global
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIXMgYJ...thdNV59Q=

Дата подписания 08.07.2026 10:09

DOC ID KZBW2Z120260000201301F66B3

DOC ID KZBW2Z120260000201301F66B3
Электронный документ подписан в Documentolog Business