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

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

Отчетный период: 01.11.2025 – 30.11.2025 г.

Алматы
2025

Оглавление

1. ОБЩАЯ ИНФОРМАЦИЯ 3
1.1. Ключевые показатели эффективности 3
2. ВВЕДЕНИЕ 3
2.1. Цель отчета 4
2.2. Область действия 4
3. АНАЛИЗ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 4
3.1. Состояние агентов 4
3.2 Оценка соответствие требованием информационной безопасности 6
3.3 План дальнейших мероприятий 7
4. МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 9
4.1. Статистика событий безопасности 9
4.2. Обработка инцидентов 9
4.3. Система уведомлений 10
4.4. Автоматическое реагирование на угрозы 10
5. ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ И АНАЛИЗ УЯЗВИМОСТЕЙ 11
5.1 Пентест 11
5.2 Инструментальное сканирование 11
5.3 Анализ подсети Заказчика с рекомендациями 12
6. **ПЛАТФОРМА АНАЛИЗА УГРОЗ И ЗАЩИТА ОТ ТАРГЕТИРОВАННЫХ АТАК** 14
6.1. OpenCTI — Платформа киберразведки 14
6.2. MISP — Обмен индикаторами компрометации 15
6.3. T-Lab Sandbox — Защита от таргетированных атак 15
6.4 Результаты работы системы за отчетный период: 16
6.4. IOC – Предотвращение утечек данных (safetica) 19
6.4. DLP – Предотвращение утечек данных (safetica) 19
6.5 Checkpoint - межсетевой экран 25
7. РЕАЛИЗОВАННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 28
8. ВЫВОДЫ И РЕКОМЕНДАЦИИ 29
8.1. Общие выводы 29
8.2. Приоритетные планы работ 30
8.3. Рекомендации 30
ПРИЛОЖЕНИЕ 32

1. ОБЩАЯ ИНФОРМАЦИЯ

Настоящий отчет представляет результаты оказания услуг по обеспечению информационной безопасности для Акимата города Алматы (далее - Заказчик) за отчетный период 01.11.2025 – 30.11.2025 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 достигнуты следующие результаты:

- Осуществлена инвентаризация **916** агентов систем SIEM, EDR, DLP и Sysmon, установленных на рабочих станциях и серверах Заказчика;
- Зарегистрировано **68 602** события безопасности различных уровней критичности, поступивших в систему мониторинга;
- Проанализировано и закрыто **51** кейсов, в рамках которых обработано **5 745** события;
- Направлено **18** уведомлений о выявленных инцидентах информационной безопасности, все угрозы своевременно устранены аналитиками Поставщика;
- Обнаружено и нейтрализовано **48** вредоносных файлов посредством системы T-Lab Sandbox в связке с EDR;
- Проведено инструментальное сканирование внутреннего и внешнего периметра, выявлены уязвимости уровней Critical, High и Medium по подразделениям
- Осуществлена интеграция средств защиты информации с SIEM, включая EDR, Check Point, Nessus, DLP, T-Lab Sandbox;
- Проведена оценка соответствия требованиям информационной безопасности согласно **Постановлению №832** и **Приказу №52-НҚ**, сформированы зоны полного и частичного соответствия.
- Политики Check Point корректно применяются на всех шлюзах и обновляются централизованно;
- Зафиксированы множественные срабатывания защитных механизмов (Syslog Message Length Enforcement, Max Ping Size, TCP Invalid Retransmission, Command Injection и др.), подтверждающие активную работу системы;
- Блокировки дополнительно подтверждаются средствами EDR на конечных точках, что обеспечивает сквозную защиту.

2. ВВЕДЕНИЕ

Настоящий отчет подготовлен в соответствии с пунктом 4.5 технической спецификации на услуги по обеспечению информационной безопасности и охватывает период 01.11.2025 – 30.11.2025 года.

2.1. Цель отчета

Целью настоящего отчета является предоставление Заказчику комплексной информации о:

- Текущем состоянии систем мониторинга и защиты информационной безопасности;
- Выявленных инцидентах безопасности и принятых мерах реагирования;
- Результатах проведенного тестирования и сканирования на уязвимости;
- Статистике обработанных событий и уведомлений;
- Рекомендациях по повышению уровня защищенности инфраструктуры.

2.2. Область действия

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

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

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

3. АНАЛИЗ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

3.1. Состояние агентов

В ноябре Поставщиком был выполнен ручной обход рабочих станций и произведён перезапуск EDR-агентов. Необходимость ручного вмешательства была обусловлена тем, что часть инфраструктуры Заказчика функционирует на операционной системе **Windows 11** Home, не поддерживающей корпоративные механизмы централизованного управления, доставки политик безопасности и перезапуска агентов. В рамках данного обхода из **217** рабочих станций, включённых в план, удалось вручную обработать **102** устройства **(47%),** тогда как оставшиеся **115** рабочих станций не были доступны для обслуживания из-за отсутствия сотрудников (отпуска, командировки, отсутствие на рабочих местах), что временно ограничило физический доступ к оборудованию. Работы проводились на объектах инфраструктуры Заказчика, включая аппарат акима города, **15** управлений акимата и территориальные подразделения (районные акиматы).

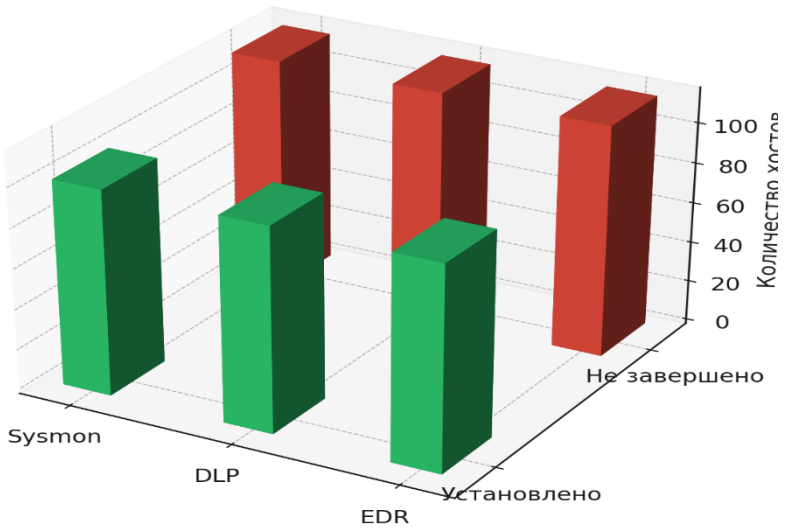

Рисунок 1. Агенты

Диаграмма отражает равномерное распределение трёх типов агентов безопасности – Sysmon, DLP и EDR - установленных на рабочих станциях в ноябре. Каждый из агентов занимает **33.3%,** что соответствует **102** обработанным рабочим станциям для каждого решения.

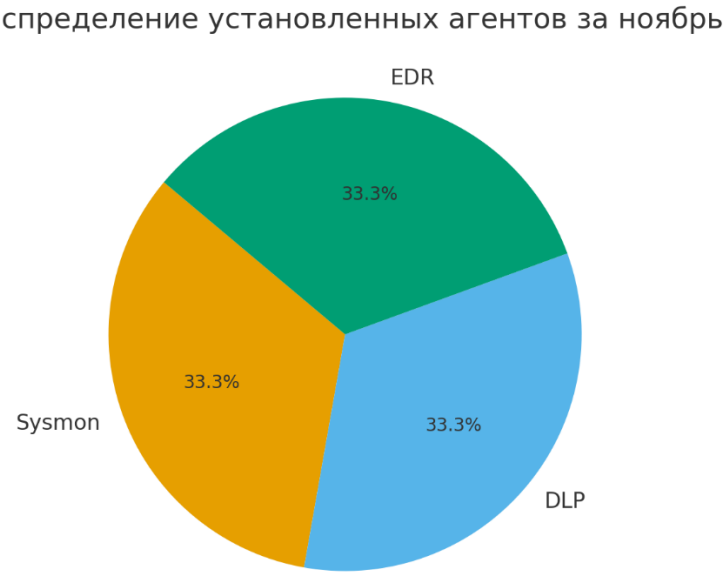

Рисунок 2. Равномерное распределение трёх типов агентов

Таблица 1 отражает хосты, на которых в ноябре успешно установлены все три агента безопасности - Sysmon, DLP и EDR. Эти устройства входят в состав **102** обработанных рабочих станций, охваченных в рамках работ в аппарате акима города, 15 управлениях и районных акиматах.

Таблица 1. Успешно установленные агенты

№	Наименование хоста	sysmon	DLP	EDR
1	ONFMD3V	да	да	да
2	HQHRP8F	да	да	да
3	6VCF7F0	да	да	да
4	DESKTOP-7PQ9JGE	да	да	да
5	AKYLZHAN	да	да	да
6	AIGUL	да	да	да
7	ULBOLSYN	да	да	да
8	DESKTOP-9NI4RVE	да	да	да
9	DESKTOP-N9EPV9O	да	да	да
10	DESKTOP-6BNCNOU	да	да	да

Примечание: Полная таблица установленных агентов указаны в приложений 1.

3.2 Оценка соответствие требованием информационной безопасности

В соответствии с Едиными требованиями в области ИКТ и обеспечения информационной безопасности (ПП РК № 832) и требованиями Приказа № 52-НҚ Поставщиком проведена оценка соответствия инфраструктуры установленным нормам. В рамках работ были проверены средства защиты, состояние рабочих станций, корректность функционирования установленных компонентов безопасности, полнота передачи телеметрии и соблюдение требований по эксплуатации ИКТ-среды. Результаты проведённой оценки представлены в таблице 2.

Таблица 2. Оценка соответствие

№	Перечень требований	Фактическое состояние	Оценка соответствия
1	Подключение к Единому шлюзу доступа к Интернету (ЕШД)	Проверены внешние IP-адреса 89.218.12.50, 88.204.143.162, 78.142.250.198, 46.34.147.70, 78.142.250.239, 217.11.70.102 — не подключены к ЕШД.	Не соответствует
2	Оповещение НКЦИБ об инцидентах ИБ	Процесс реализован в соответствии с п.38 и 41 Постановления №832. Критических инцидентов не зафиксировано. Оповещение осуществляется ТОО «MSSP.GL» и ОЦИБ.	Соответствует
3	Применение средств идентификации и управления доступом	Внедрена система учётных записей Windows AD частично. EDR установлены вручную, без интеграции с AD.	Частично соответствует

№	Перечень требований	Фактическое состояние	Оценка соответствия
4	Мониторинг обеспечения ИБ объектов информатизации	Реализован договором с ТОО «MSSP.GL» используется SIEM, EDR, T-Lab Sandbox.	Соответствует
5	Наличие антивирусных средств и обновлений ОС	EDR агенты установлены вручную, в том числе на Windows Home Edition. ОС требует обновления до Windows 11 Pro.	Частично соответствует
6	Наличие подразделения или ответственного за ИБ	Назначен ответственный сотрудник по ИБ, обучение подтверждено. Дополнительно функции выполняет ОЦИБ.	Соответствует
7	Наличие нормативно-технической документации по ИБ	В наличии Политика ИБ, Правила идентификации активов, Методика оценки рисков. Документы утверждены на казахском и русском языках.	Соответствует
8	Применение многофакторной аутентификации (МФА)	МФА не реализована для доступа к критическим системам. Аутентификация только через пароль AD.	Не соответствует
9	Внесение обязанностей по ИБ в должностные инструкции	В должностных инструкциях сотрудников ИБ и администраторов отражены функции по обеспечению ИБ. ОЦИБ контролирует выполнение.	Соответствует

Примечание: Полная таблица оценки соответствие указаны в приложений 2.

3.3 План дальнейших мероприятий

В рамках выполнения требований ПП РК № 832 и Приказа № 52-НҚ, а также обеспечения завершения актуализации и сопровождения инфраструктуры Заказчика, планируется проведение следующих мероприятий:

1. Завершение охвата оставшихся рабочих станций

- повторный обход 115 рабочих станций, ранее недоступных по причине отсутствия сотрудников;
- установка и проверка работы компонентов безопасности на данных устройствах.

2. Контроль корректности работы агентов безопасности

- регулярная проверка функционирования EDR, DLP и Sysmon;
- устранение выявленных отклонений и восстановление телеметрии при необходимости.

3. Усиление мониторинга через SIEM

- анализ полноты и качества поступающих событий;
- корректировка интеграции и обновление правил корреляции.

4. Актуализация политик безопасности

- обновление политик DLP, EDR и Sysmon с учётом выявленных инцидентов и рисков;
- обеспечение доставки политик на все рабочие станции.

4. МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Статистика событий безопасности

В рамках мониторинга системы обнаружения и предотвращения угроз за отчетный период было зарегистрировано 153 и отработано **68 602событий (alerts)** различного уровня критичности. Детальное распределение событий по уровням критичности указаны в Таблице 3.

Таблица 3. Распределение событий безопасности по уровням критичности

Уровень критичности	Количество	Доля (%)
Critical (Критический)	32	0.05%
High (Высокий)	60265	87.87%
Medium (Средний)	845	1.23%
Low (Низкий)	7460	10.88%
ИТОГО	**68602**	

Примечание. Количество обработанных событий можно посмотреть в приложений 3.

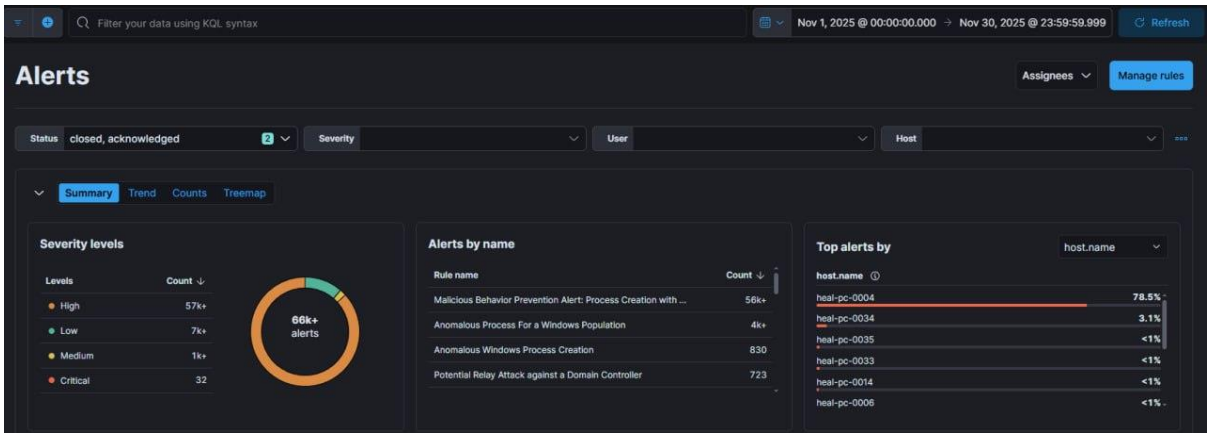

Рисунок 3. Свод по выявленным и проверенным отчетам

4.2. Обработка инцидентов

За отчётный период Поставщиком проанализировано и закрыто **51** кейсов, в рамках которых было обработано **5 745** события информационной безопасности, из них критический – **14**, высокий – **1 041**, средний – **5 35**, низкий – **4 155**.

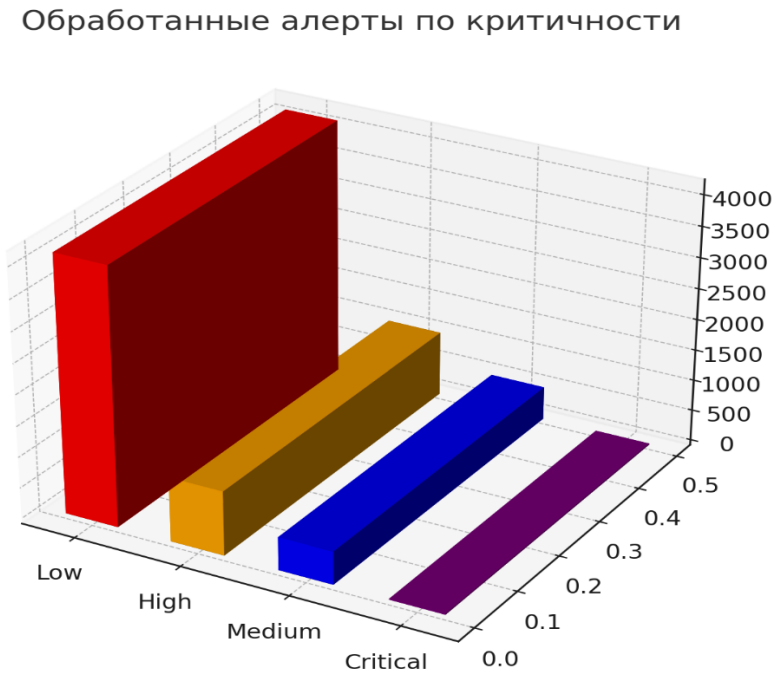

Рисунок 4. Свод по выявленным и проверенным отчета в разрезе уровней критичности

4.3. Система уведомлений

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

За отчётный период Заказчику направлено **18** уведомлений о зафиксированных инцидентах, по каждому из которых аналитиками Поставщика были выполнены мероприятия по реагированию и инциденты были устранены.

4.4. Автоматическое реагирование на угрозы

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

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

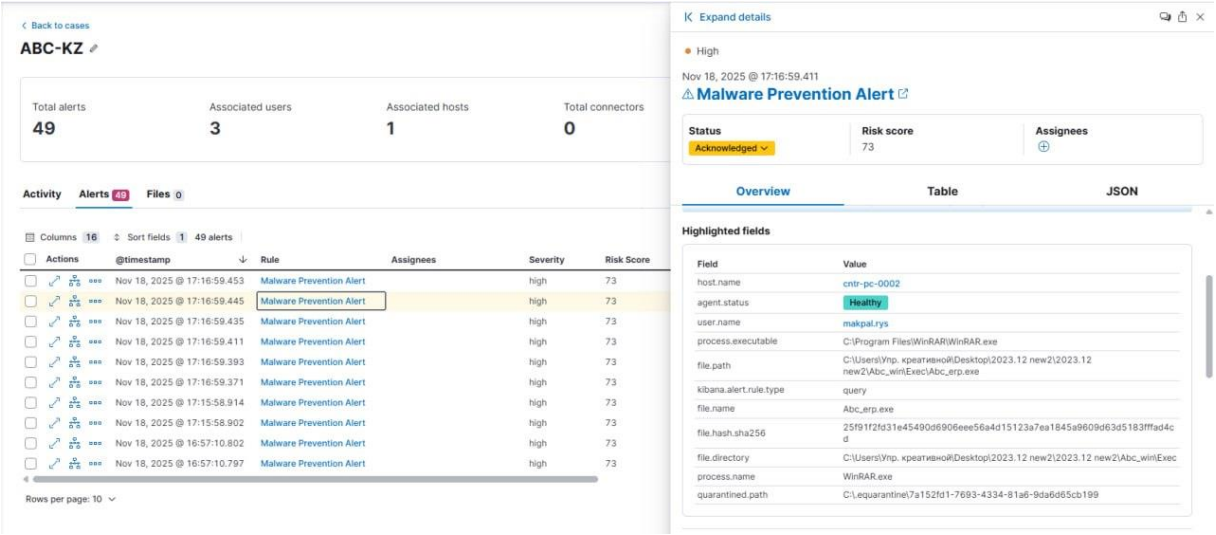

Рисунок 5. Пример направленного изолированного хоста cntr-pc-0002

5. ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ И АНАЛИЗ УЯЗВИМОСТЕЙ

5.1 Пентест

В соответствии с требованиями технической спецификации (пункт 1.1.18), тестирование на проникновение (пентест) должно проводиться не реже двух раз в год. Поставщиком в настоящий момент проводится пентест, который длится в период с ноября по декабрь 2025 года.

5.2 Инструментальное сканирование

Помимо этого, ежемесячно проводится комплексное инструментальное сканирование внутреннего и внешнего периметра сети. Работы выполняются в строгом соответствии с технической спецификацией Акимата города Алматы и включают анализ на наличие уязвимостей, отклонений в конфигурациях и потенциальных точек компрометации. Проведение регулярного сканирования позволяет поддерживать высокий уровень защищённости инфраструктуры, своевременно выявлять риски и обеспечивать их оперативную обработку. Результаты внутреннего сканироваия сети указаны в таблице 4.

Таблица 4. Инструментальное сканирование внутренней сети

№	Подразделение (полное название)	Critical	High	Medium
1	**Управление градостроительного контроля**	0	0	2
2	**Аппарат акима Алатауского района**	1	5	11

№	Подразделение (полное название)	Critical	High	Medium
3	**Серверная сеть акимата г. Алматы**	1	1	8
4	**Аппарат акима Турксибского района**	0	0	4
5	**Аппарат акима Наурызбайского района**	1	3	8
6	**Управление городского планирования и урбанизации**	5	5	12
7	**Управление предпринимательства и инвестиций**	2	7	15
8	**Управление по делам религий**	0	0	1
9	**Управление сейсмической безопасности и мобилизационной подготовки**	0	0	1
10	**Управление земельных отношений**	0	0	3

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

5.3 Анализ подсети Заказчика с рекомендациями

По результатам анализа выявлены следующие компоненты с критическими и высокими уязвимостями, требующие немедленного внимания (детальная таблица представлена в Приложении 5), также предоставлена диаграмма топ -6 Количество критических уязвимостей.

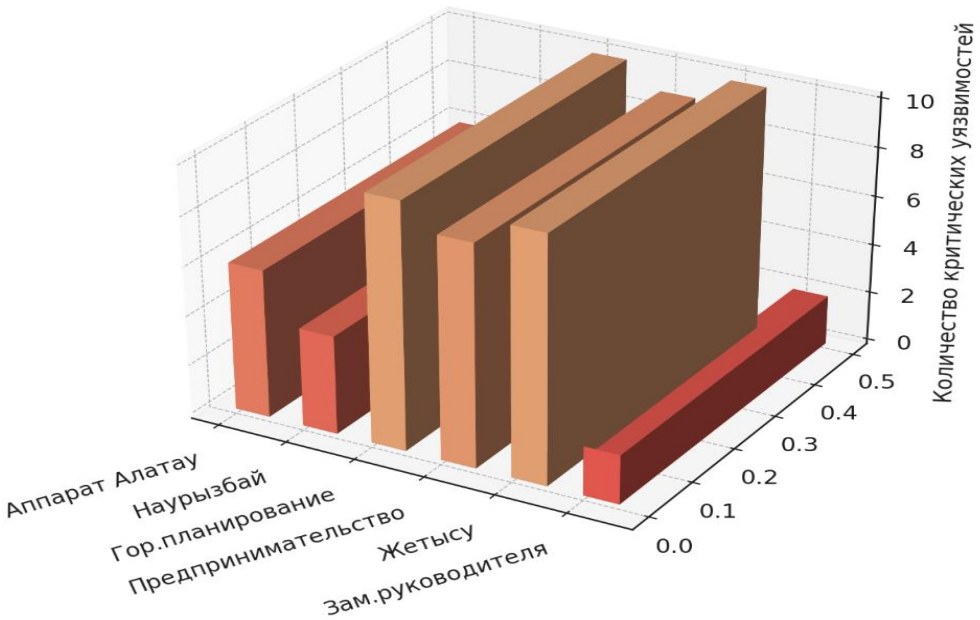

Рисунок 5. Количество критических уязвимостей

Аппарат Наурызбайского района, являющийся структурным подразделением Акимата города Алматы, был включён в перечень объектов, подлежащих инструментальному обследованию. В ноябре в его адресной подсети проведена проверка с целью выявления и последующего предоставления Заказчику информации о потенциальных угрозах информационной безопасности.

Таблица 5. Аппарат Наурызбайского района

№	Уязвимость	IP/Домен	Критичность
1	SNMP Agent Default Community Name (public)	192.168.158.2	Высокая
2	SSL Version 2 and 3 Protocol Detection	192.168.158.11	Критичная
3	SSL Certificate Signed Using Weak Hashing Algorithm	192.168.158.11	Высокая
4	SSL Medium Strength Cipher Suites Supported (SWEET32)	192.168.158.11	Высокая

Примечание: Полная таблица оценки соответствие указаны в приложений 4.

Примечание:
Результаты внутреннего сканирования уязвимостей представлены в ***Приложении 5****, а результаты внешнего сканирования — в* ***Приложении 6****.*

6. ПЛАТФОРМА АНАЛИЗА УГРОЗ И ЗАЩИТА ОТ ТАРГЕТИРОВАННЫХ АТАК

6.1. OpenCTI — Платформа киберразведки

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

- Индикаторы компрометации (IoC);
- Тактики и техники атак в соответствии с фреймворком MITRE ATT&CK;
- Информацию о киберпреступных группировках и вредоносных кампаниях.

Рисунок 6. OpenCTI

6.2. MISP — Обмен индикаторами компрометации

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

За отчетный период угроз информационной безопасности не выявлено.

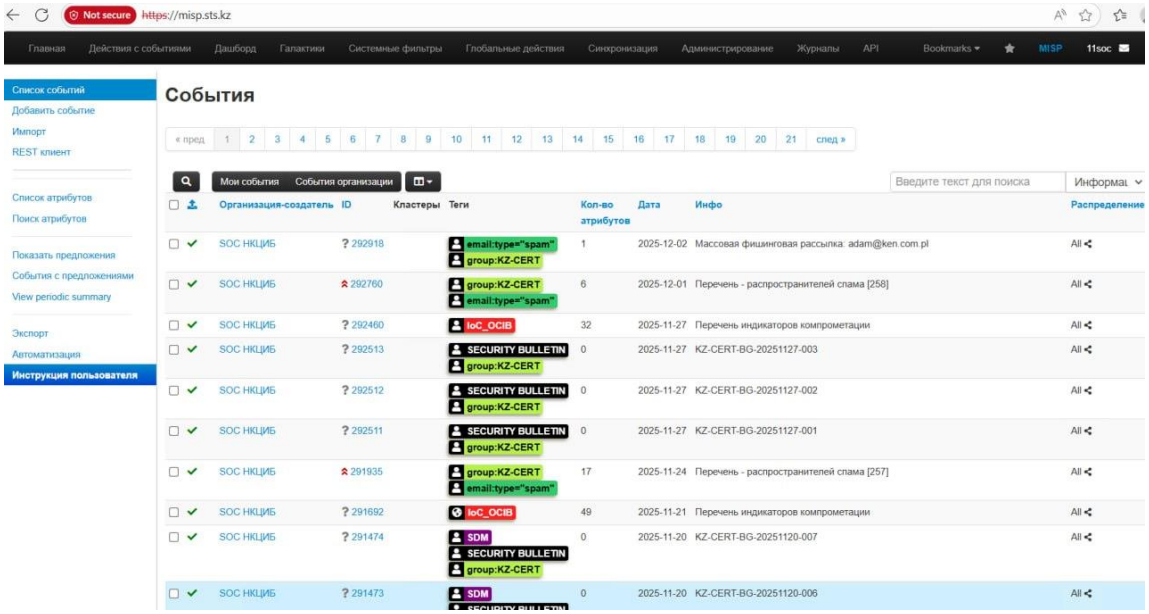

Рисунок 7. MISP

6.3. T-Lab Sandbox — Защита от таргетированных атак

Поставщиком реализованы меры защиты от таргетированных кибератак и угроз нулевого дня с использованием системы динамического и статического анализа **T-Lab Sandbox**. Система позволяет проводить поведенческий анализ подозрительных объектов, выявлять и блокировать вредоносную активность, а также интегрирована с SIEM и EDR для централизованного реагирования.

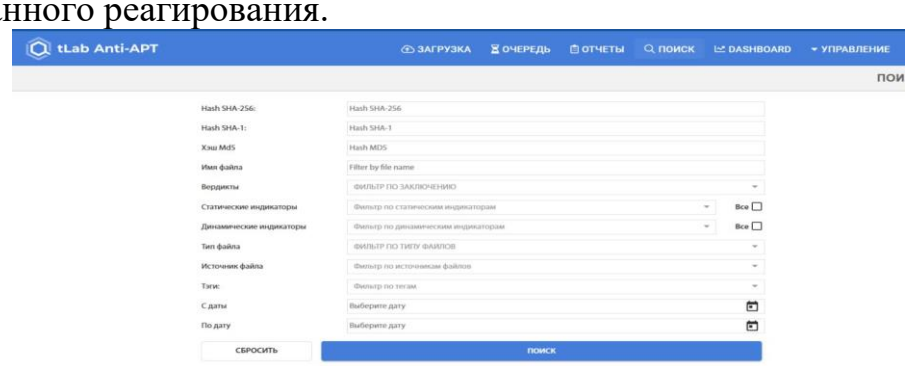

Рисунок 8. T-Lab

6.4 Результаты работы системы за отчетный период:

В отчетном периоде Поставщиком выполнялся постоянный анализ потенциальных угроз, включающих вредоносные и подозрительные события. Согласно динамике на графике, в первой половине месяца наблюдались пиковые значения, после чего активность снизилась до минимального уровня.

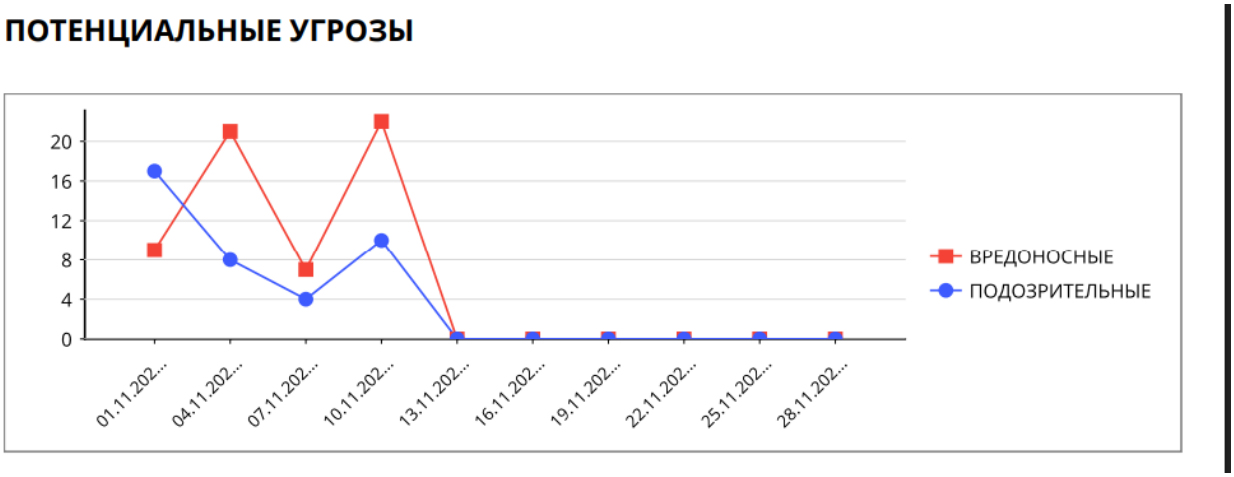

Рисунок 9. Потенциальные угрозы

Поставщиком:

- Проанализировано все файлы, поступивших на проверку через систему защиты от таргетированных атак;
- Из них **48 файла** классифицированы как вредоносное программное обеспечение;
- Обнаруженные угрозы заблокированы на периметре средствами EDR;
- Результаты анализа переданы администраторам информационной безопасности для принятия корректирующих мер.

Таблица 6. Проанализированные файлы

№	дата	наименование файла
1	1 ноября 2025 г., 0:11	eicar.com
2	1 ноября 2025 г., 0:24	5a9557bb4265dad84c1d065afd072b41b756e267416309de8d6b56551d2fe3f7.bin
3	1 ноября 2025 г., 19:39	zzAntiRansomElastic-DO-NOT-TOUCH-dab6d40c-a6a1-442c-adc4-9d57a47e58d7.scr
4	3 ноября 2025 г., 8:23	F1Ldck1UeGMeKBxei4.exe
5	3 ноября 2025 г., 1:24	FUkMUX3wwwTJCQ7Vb8.exe
6	3 ноября 2025 г., 10:09	download.ps1

№	дата	наименование файла
7	3 ноября 2025 г., 10:09	seederexe.exe
8	4 ноября 2025 г., 8:14	FAtEc1jhq2ZrKOLhe
9	4 ноября 2025 г., 8:46	FrVonV1TUdCSxtpuK
10	4 ноября 2025 г., 9:42	Fz5qYJ2AM2Es4b2V89
11	4 ноября 2025 г., 10:24	FyDR6oYMvWANaA9zg
12	4 ноября 2025 г., 11:30	FKcrmR2pjgu43a3ydk
13	4 ноября 2025 г., 13:22	FQI88E1lm9qKvbahR4
14	4 ноября 2025 г., 12:53	F8qrI9bjkGwCTaAdj
15	6 ноября 2025 г., 6:21	FlsAGTHpSh273Qkbe
16	6 ноября 2025 г., 3:23	FT4Hsn1fIUwMRhtpR9
17	6 ноября 2025 г., 7:44	FlcHkfFnceCFxofCd
18	6 ноября 2025 г., 8:14	FtU8X688Spn7oqdrl
19	6 ноября 2025 г., 8:14	FOPOYoZ34XxMBXL7k
20	6 ноября 2025 г., 10:12	Fn1eVh3HQXXe1UmEUi
21	6 ноября 2025 г., 9:52	FDhbVo4ushCiPD4b4e
22	7 ноября 2025 г., 3:09	F00EwQ1RvX27ixJP8a
23	7 ноября 2025 г., 8:44	FxfHVdGcjBPj6ybFf
24	7 ноября 2025 г., 7:34	FmhcML3opgAjQziGm4
25	7 ноября 2025 г., 6:30	FxdsXQ3OUqHWKBbFGa
26	7 ноября 2025 г., 6:17	FqKloO2X5SYVJkHx56
27	7 ноября 2025 г., 13:38	FTi5o431fBu5tl45Kd

№	дата	наименование файла
28	9 ноября 2025 г., 12:16	FYKDaAhTndiSGlMF9.exe
29	10 ноября 2025 г., 11:58	FMkMPs1ufK3GgfeZRl.exe
30	11 ноября 2025 г., 6:01	F3SV3o2Nu5Dl1Se3uj
31	11 ноября 2025 г., 6:24	FLBqmlkEEFZBDoW37
32	11 ноября 2025 г., 6:38	FOX0pe2UpAYsZMtiae
33	11 ноября 2025 г., 9:35	FkWxQRhjdnS0uYci2
34	11 ноября 2025 г., 9:21	F4KOiP3dghDvHasPld
35	11 ноября 2025 г., 8:41	FhXbb61kZxeVIy7JR3
36	11 ноября 2025 г., 8:01	Fcb0QZ3N2XvIIlQyf9
37	11 ноября 2025 г., 9:51	FRjVvT2NcSqkuaKVZi
38	11 ноября 2025 г., 10:38	FspW9i34Ewwk5JNlb6
39	12 ноября 2025 г., 8:38	Fnzm551zZKtnvSAIKj
40	12 ноября 2025 г., 6:29	Fcu7Hi3ILIhOwR7zE2
41	12 ноября 2025 г., 0:32	FyJhUj4cT1VV02sSof
42	12 ноября 2025 г., 9:38	FL0G5l3oWlRnRvi1h5
43	12 ноября 2025 г., 9:37	FJeCAB4xFwg3CHcjQ
44	12 ноября 2025 г., 9:27	FmADpc3xClKjwaS3x1
45	12 ноября 2025 г., 9:24	FkQxXG1iMS5gxri992
46	12 ноября 2025 г., 11:54	FiOG163LSZ22bwhIsf
47	12 ноября 2025 г., 11:45	FzAQ4C4BRB6vdlUYy4
48	12 ноября 2025 г., 10:25	Fvt6Ge4ch9Jn2cWp15

Примечание: Полный анализ можно посмотреть в приложений 7

6.4. IOC – Предотвращение утечек данных (safetica)

В ходе анализа IOC за период 01–12 ноября 2025 года выявлено **48** вредоносных и **39** подозрительных файлов, при этом активность угроз наблюдалась только в первой половине месяца, с пиками 03.11, 04.11 и 12.11, после чего полностью прекратилась. Основной вектор угроз связан с фишинговыми и скриптовыми объектами (TEXT, MS Office, PDF, EXE), что указывает на попытки первоначального доступа через социальную инженерию. T-Lab Sandbox выделил ТОП-10 наиболее опасных хэшей, которые необходимо внести в block-list всех средств защиты, однако источник доставки угроз в отчёте не определяется и требует дополнительной проверки почтовых логов, proxy и телеметрии EDR/Sysmon. Все выявленные вредоносные объекты были корректно заблокированы системой, и их дальнейшее распространение не зафиксировано

Таблица 7. Хэш сумма вредоносных файлов

№	hash -сумма вредоносных файлов
1	7650464c2215c6ecccd11fbbdca783b47c596aea01456f167e3b7261dc39bbe
2	35585d12899435e13e186490fcf1d270adbe3c74a1e0578b3d9314858bf2d797
3	1cddb0aaee3746cd3277f03ff2b49e82736e5719fe73698f01ad0585a841917
4	ccef0b59cec8235e9d6d284f6cb6992b0eed7ae0dc1583fd14d78e87dfc75796
5	9a9557bb4265dad84c1d05afd072b41b756e267461309de8d6b56551d2fe3f7
6	c263574b0f6987dd34de1b82513828f6dbf99fd693aaa99d701d9c23bb7e679
7	03cf2f5522b84c9566e3fb753e57448e02a0ad3385e786d460005d074e045d90
8	5b3e1974e722987ba9482e92630ad56dc2c3153e3260c536dee0775c5e6ba14
9	5d73d51c5b1164b1e8f5bc4632a5eadd02ee0039a9f4ce98b40d57cdaa6053d
10	7e389079878fae6efe916b9d0925c4c9976d84e55f0d4ceff2e049a42071779

6.4. DLP – Предотвращение утечек данных (safetica)

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

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

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

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

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

Рисунок 10. Распределение операционных система

Показывает частоту входов пользователей. Повышенная активность может указывать на повышенную нагрузку, а также потенциальные риски нарушения политик ИБ.

Рисунок 11. Активность отрпавки телеметрии по часам

Таблица 8. Активность устройств и пользователей

№	Устройство	Операционная система	Последний раз входил в систему	Защита обновлена	Записи отправлены	Последний ответ
1	DESKTOP-0EPGF17	Windows 10	Аппарат Акима@DESKTOP-0EPGF17	2025-12-04 01:06:45	2025-12-04 01:06:45	2025-12-04 01:06:15
2	SRV-DLP	Windows Server 2022	Administrator@SRV-DLP	2025-12-04 00:00:45	2025-12-04 01:05:45	2025-12-04 01:05:15

№	Устройство	Операционная система	Последний раз входил в систему	Защита обновлена	Записи отправлены	Последний ответ
3	354k	Windows 11	aika_@354k	2025-12-04 00:00:45	2025-12-04 01:05:15	2025-12-04 01:05:15
4	PINF-PC-0003	Windows 10	Gaziz Dulatbekov	2025-12-04 00:59:45	2025-12-04 01:03:45	2025-12-04 01:02:15
5	ALMA-PC-0002	Windows 11	Rustem Doskozha	2025-12-04 00:00:45	2025-12-04 00:55:45	2025-12-04 01:05:15
6	CNTR-PC-0018	Windows 10	Ainur Ybyraeva	2025-12-04 00:55:15	2025-12-04 00:55:15	2025-12-04 00:55:45
7	DESKTOP-QP7T2OK	Windows 11	УГМ@DESKTOP-QP7T2OK	2025-12-04 00:47:45	2025-12-04 00:47:45	2025-12-04 00:47:45
8	PSPS-PC-0012	Windows 11	Nurdaulet Sanabay	2025-12-04 00:31:45	2025-12-04 00:46:45	2025-12-04 01:05:15
9	DESKTOP-VTU0A9E	Windows 11	User@DESKTOP-VTU0A9E	2025-12-04 01:05:45	2025-12-04 00:45:45	2025-12-04 01:05:15
10	DESKTOP-APPR32	Windows 10	Аппарат Акима@DESKTOP-APPR32	2025-12-04 00:37:45	2025-12-04 00:39:15	2025-12-04 01:05:15

Примечание: Полный анализ активности пользователя можно посмотреть в приложений 8

Анализ данных DLP показал, что сотрудники Акимата активно используют мессенджеры WhatsApp и Telegram, а также видеосервис YouTube в рабочее время. Подобная активность повышает риски утечки конфиденциальной информации, поскольку мессенджеры не относятся к контролируемым корпоративным каналам связи. Дополнительно фиксируется увеличение нагрузки на сеть организации из-за потребления видеоконтента, что может негативно влиять на производительность бизнес-сервисов и общую доступность информационных ресурсов

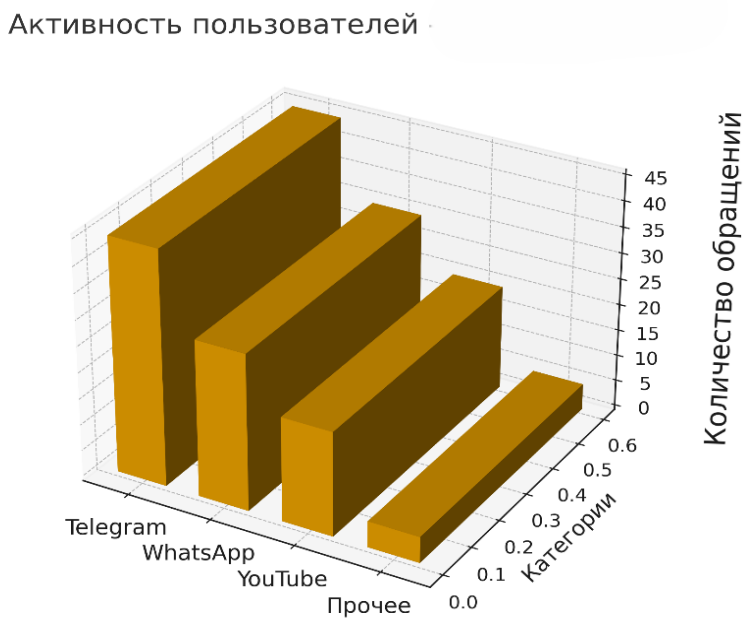

Рисунок 12. Активность пользователей

По результатам анализа интернет-активности установлено, что в течение отчётного периода наиболее значительное время в сети проводят следующие сотрудники, что отражено на диаграмме «Топ-10 пользователей». Данные сотрудники формируют основную нагрузку на интернет-канал, что требует дополнительной оценки характера посещаемых ресурсов и соответствия такой активности рабочим задачам.

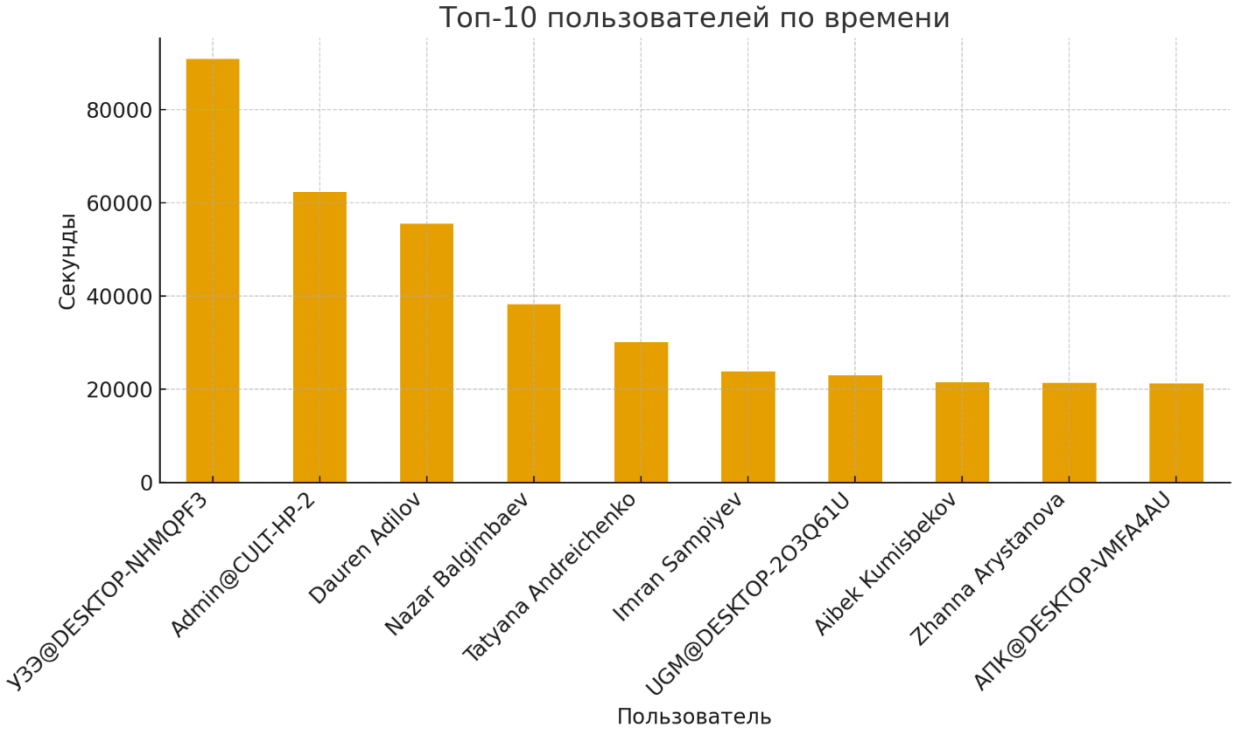

Рисунок 13. Топ-10 пользователей

Анализ посещаемых ресурсов показывает, что наибольшее количество времени сотрудники проводят на сайтах развлекательного характера, что отчётливо видно из диаграммы «Топ-10 сайтов». Господствующее положение занимает видеоплатформа YouTube, что указывает на высокую долю непрофильного трафика и повышенную нагрузку на интернет-канал.

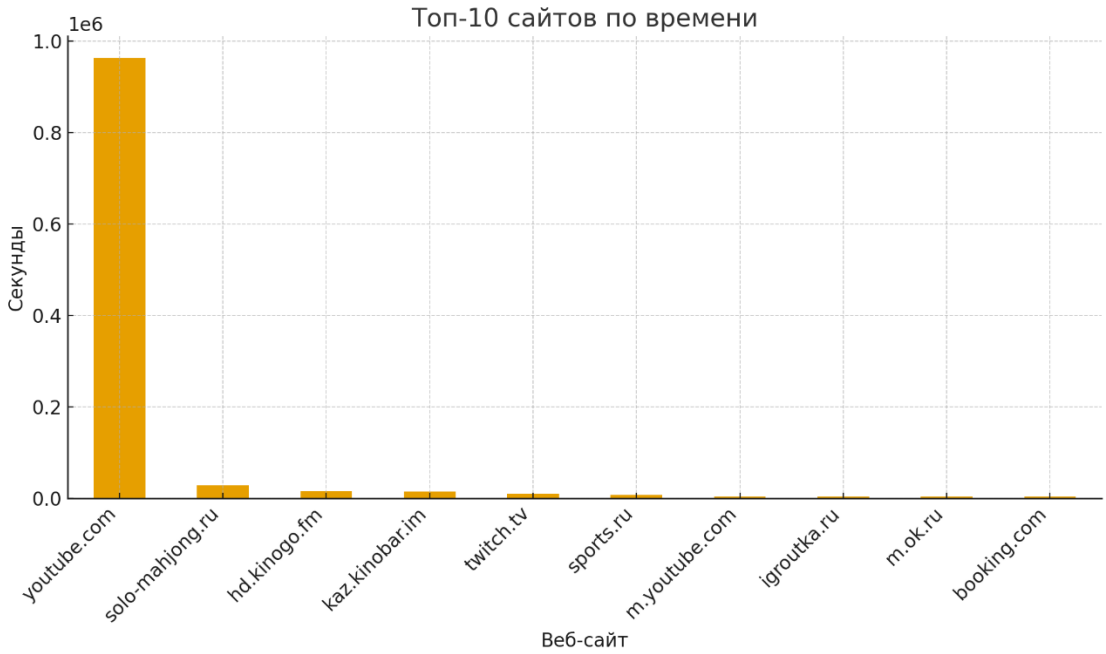

Рисунок 14. Топ-10 сайтов по времени

Круговая диаграмма демонстрирует, что основная часть трафика относится к категории «Досуг», включающей видеосервисы, социальные сети и медиа-платформы. Подобное распределение говорит о преобладании непроизводственной активности, что снижает доступную пропускную способность сети для критически важных сервисов и требует дальнейшей оптимизации политик доступа.

Рисунок 15. Инфографика распределение трафика по категориям

По результатам анализа интернет-активности пользователей установлено, что наибольшее суммарное время в сети провели следующие сотрудники, указанные в таблице ТОП-10. Основная часть их активности связана с доступом к видеоплатформе YouTube, что относится к категории «Досуг» и формирует значительную нагрузку на интернет-канал.

Таблица 9. Топ 10 пользователей, которые сидят в интернете

№	Пользователь	Веб-сайт	Веб-категория	Общее время
1	УЗЭ@DESKTOP-NHMQPF3	youtube.com	Досуг	25ч 14м 13с
2	Admin@CULT-HP-2	youtube.com	Досуг	17ч 16м 18с
3	Dauren Adilov	youtube.com	Досуг	15ч 25м 44с
9	Nazar Balgimbaev	youtube.com	Досуг	10ч 35м 48с
5	Tatyana Andreichenko	solo-mahjong.ru	Финансовый	8ч 1м 25с
6	Imran Sampiyev	youtube.com	Досуг	6ч 24м 21с
7	UGM@DESKTOP-2O3Q61U	youtube.com	Досуг	6ч 23м 53с
8	Zhanna Arystanova	youtube.com	Досуг	5ч 54м 43с
9	УЗЭ@DESKTOP-QV7S0RL	youtube.com	Досуг	5ч 43м 43с
10	Aibek Kumisbekov	youtube.com	Досуг	5ч 27м 24с

Примечание: Полный анализ активности пользователя в интернете можно посмотреть в приложений 9

План дальнейших мероприятий

Актуализация политики использования интернет-ресурсов

- Обновить правила использования корпоративного интернета.
- Определить перечень разрешённых/запрещённых сайтов и сервисов.
- Уведомить сотрудников о требованиях и возможных ограничениях.

Ознакомление сотрудников с политикой ИБ

- Провести рассылку и инструктаж по корректному использованию сетевых ресурсов

Обучение и повышение осведомлённости

- Провести мини-тренинг: «Безопасная работа в интернете».
- Разъяснить риски утечек данных через мессенджеры и социальные сети.

Информационные памятки

- Рассылки с рекомендациями: «Как не стать источником утечки», «Что нельзя делать в рабочее время».

6.5 Checkpoint - межсетевой экран

По данным системы сетевой безопасности, за отчётный период были зафиксированы наиболее частые типы заблокированных или предотвращённых событий. Ниже представлены топ-10 защитных механизмов по количеству срабатываний:

Таблица 10. Топ 10 срабатываний

№	Protection	Sessions	Комментарий
1	Syslog Message Length Enforcement	640K	Массовые попытки отправки некорректных или аномально длинных Syslog-сообщений — система успешно блокирует такие пакеты.
2	140	314K	Высокочастотные сетевые события, классифицированные системой как нарушение профиля трафика.
3	Max Ping Size	75K	Попытки отправки ICMP-пакетов нестандартного размера — возможно разведка.
4	TCP Invalid Retransmission	9.4K	Ошибочные или подозрительные TCP-переотправки, характерные для сканирования.

5	TCP Segment Limit Enforcement	5.7K	Попытки передать слишком большие TCP-сегменты — система блокирует как потенциальный DoS-вектор.
6	Command Injection	550	Попытки внедрения команд в сетевые запросы; заблокировано системой.
7	Non-Compliant IKE	207	Некорректные IKE-пакеты, попытки неправомерного VPN-установления.
8	179	131	Категория защиты с уникальным ID — детект нарушений сетевого протокола.
9	Resource Records Enforcement	113	Попытки некорректных DNS-запросов; предотвращено.
10	33	103	Низкоуровневые сетевые отклонения, блокируемые системой по сигнатурам.

В рамках функционирования системы сетевой безопасности Check Point, были выявлены и заблокированы наиболее распространённые вредоносные объекты. Благодаря встроенным механизмам Threat Prevention (*подробно смотреть в таблице 9*), все попытки заражения и обращения к вредоносным ресурсам были остановлены на уровне межсетевого экрана, а также дополнительно подтверждены и заблокированы средствами EDR на конечных устройствах.

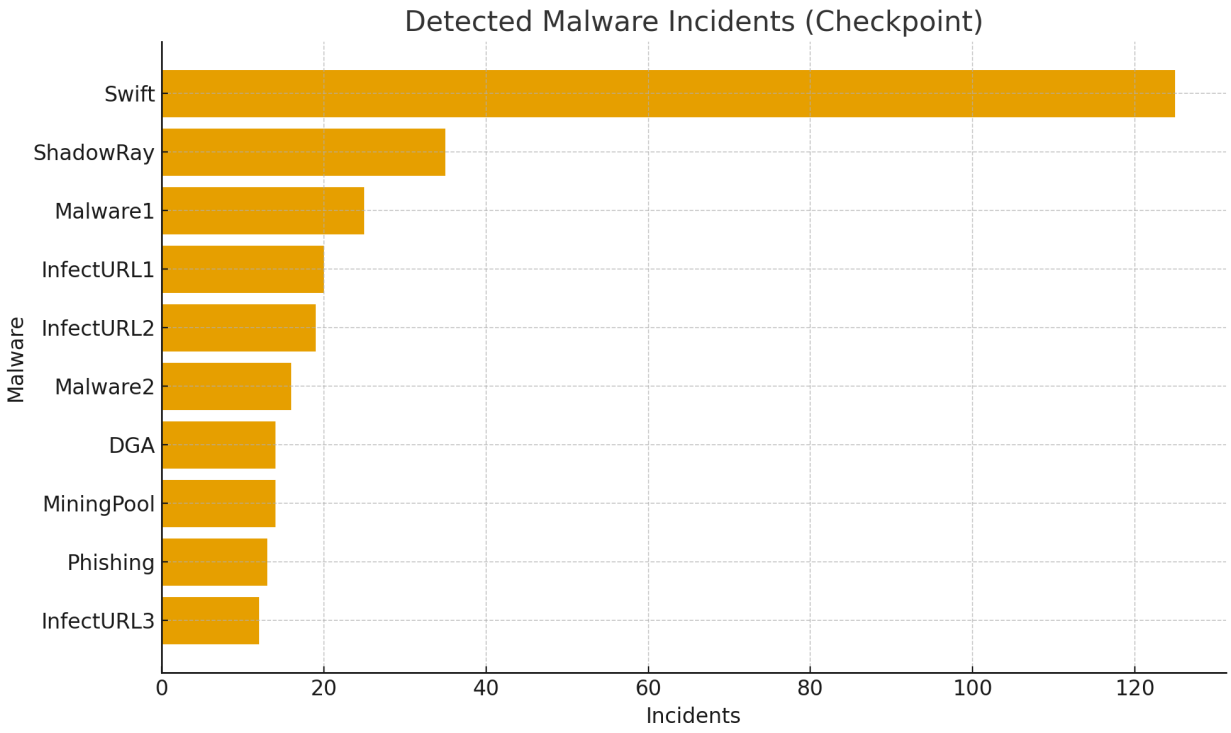

Рисунок 16. Топ-10 заблокированных вредоносных файлов

Таблица 11. Топ – 10 вредоносные файлы

№	Название вредоносного ПО	Критичность / Уровень опасности	попытка распространение
1	Swift.TC.e7e0XsOZ	High	125
2	ShadowRay.TC.1f22YRUa	High	35
3	Malware.TC.11a7qGKr	Medium	25
4	Infecting_URL.RS.TC.bec6FhkZ	Medium	20
5	Infecting_URL.VUP.RS.TC.2e44lngd	Medium	19
6	Malware.TC.6334vlow	Medium	16
7	dga-RzNsG.TC.c75drnbP	Low	14
8	MiningPool.TC.3aa3uhfH	Medium	14
9	Phishing.GS.RS.TC.d90fyotR	Medium	13
10	Infecting_URL.RS.TC.2677bzbU	Medium	12

7. РЕАЛИЗОВАННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Таблица 12. Статус реализации систем информационной безопасности

№	Система	Назначение	Статус реализации
1	**Система контроля привилегированного доступа (PAM)**	Защищенные доступы администраторов через бастион безопасности, аудит действий	✓ Реализовано. Доступ к инфраструктуре через бастион, ведется аудит действий администраторов
2	**Система сканирования уязвимостей (Nessus)**	Сканирование инфраструктуры, управление уязвимостями, формирование отчетов CVSS	✓ Реализовано. Регулярное сканирование, интеграция с SIEM, контроль устранения критичных уязвимостей
3	**Система обнаружения и реагирования (EDR)**	Защита серверов и PC от вредоносных действий, поведенческий анализ	✓ Реализовано. Elastic EDR интегрирован с T-Lab Sandbox и SIEM, обеспечивает автоматическую изоляцию угроз
4	**Система предотвращения утечек (DLP)**	Защита от утечек конфиденциальной информации, контроль каналов передачи	✓ Реализовано. Контроль почтовых, USB и веб-каналов, интеграция с SIEM
5	**Межсетевые экраны нового поколения (Check Point NGFW)**	Защита сетевого периметра от внешних атак, IPS, URL-фильтрация, SSL-инспекция	✓ Реализовано. 15 шлюзов Check Point с активными политиками безопасности, централизованное управление
6	**Система мониторинга событий (SIEM)**	Централизованный сбор и корреляция событий безопасности, формирование отчетов	✓ Реализовано. Интеграция с NGFW, DLP, EDR, PAM, Nessus. Круглосуточный мониторинг
7	**Система оркестрации SOAR**	централизованное управление,	✓ Реализовано. Интеграция с SIEM,

№	Система	Назначение	Статус реализации
		автоматизации и координации процессов реагирования на инциденты информационной безопасности.	Nessus. Круглосуточный мониторинг, корреляция и playbook
8	**Система регистрации инцидентов информационной безопасности**	Централизованного учёта, обработки, классификации и управления инцидентами информационной безопасности	✓ Реализовано. Интеграция с SIEM, Nessus. Круглосуточный мониторинг, регистрация карточек инцидента информационной безопасности

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

8. ВЫВОДЫ И РЕКОМЕНДАЦИИ

8.1. Общие выводы

1. Выявлены критические и высокие уязвимости в компонентах инфраструктуры, требующие незамедлительного устранения;
2. Достигнут высокий уровень покрытия инфраструктуры средствами защиты подключено **916** агента на рабочих станциях и серверах Заказчика;
3. Проведена работа с **102** рабочими станциями, однако часть оборудования остаётся без актуальной обработки и контроля из-за недоступности пользователей и особенностей ОС (Windows Home/11 Home);
4. Обнаруженные вредоносные файлы и попытки атак блокируются на уровне Check Point и EDR, файлы изолируются, результаты анализа передаются администраторам для принятия мер;
5. Обеспечено своевременное выявление и нейтрализация вредоносного программного обеспечения - заблокировано **48** вредоносных файла средствами EDR и системы защиты от таргетированных атак;
6. Основной объём составляет **High**-события, связанные со сканированием уязвимостей и сетевой активностью; критических инцидентов немного, и они отработаны без эскалации ущерба;
7. Значительная часть трафика относится к категории «Досуг» (YouTube, развлекательные ресурсы), что увеличивает нагрузку на канал и повышает риск утечек через неконтролируемые мессенджеры.
8. В отчётный период осуществлена комплексная оценка соответствия инфраструктуры требованиям ИБ, установленным Постановлением Правительства №832 и Приказом №52-НҚ. Проверка включала анализ технических, организационных и эксплуатационных мер

безопасности, состояние рабочих станций, полноту работы систем защиты и корректность применения политик ИБ.

9. Обеспечено круглосуточный мониторинг событии информационной безопасности средствами защиты информации и дежурной смены Поставщика в режиме 24/7

8.2. Приоритетные планы работ

1. Установить и проверить работу EDR, DLP и Sysmon на оставшихся 115 хостах.
2. Провести контроль подключения к ЕШД и устранить использование внешних IP-адресов, не соответствующих требованиям.
3. Оптимизировать правила SIEM, расширить автоматизацию SOAR и обеспечить постоянный контроль телеметрии агентов.
4. Закрыть выявленные критические уязвимости (CVE), выполнить повторное инструментальное сканирование и ограничить трафик категории «Досуг» и некорпоративных мессенджеров.
5. Предоставить итоговый отчёт по пентесту внешнего периметра.
6. Организовать обучение сотрудников по вопросам информационной безопасности, включая безопасное использование интернет-ресурсов, предотвращение утечек данных и соблюдение корпоративных политик

8.3. Рекомендации

1. Рассмотреть необходимость внедрения предложенных мер информационной безопасности, изложенных в итоговом отчёте, и утвердить план их реализации.
2. Обеспечить установку и корректную работу всех защитных агентов (EDR, DLP, Sysmon) на оставшихся рабочих станциях, чтобы гарантировать полный охват инфраструктуры телеметрией.
3. Организовать обновление программного обеспечения и устранение уязвимостей, указанных в перечне Приложения 4, включая критические и высокие CVE.
4. Усилить контроль за использованием интернет-ресурсов, в том числе ограничить категории «Досуг» и некорпоративные мессенджеры для снижения вероятности фишинговых инцидентов.
5. Рассмотреть внедрение дополнительных мер фильтрации почтового и веб-трафика, так как идентифицированные IOC указывают на активное использование фишинговых и скриптовых методов атаки.
6. Организовать обучение сотрудников Акимата по вопросам кибер-гигиены и безопасной работе с электронными документами, чтобы минимизировать риск успешного фишинга.

7. Провести дополнительную проверку сетевых журналов и журналов почты за период зафиксированных атак (03–12 ноября) для уточнения возможных каналов доставки вредоносного контента.
8. Принять к сведению результаты анализа IOC и T-Lab Sandbox и обеспечить внесение выявленных индикаторов в механизмы защиты, используемые в Акимате.
9. Привести процессы и инфраструктуру информационной безопасности в соответствие требованиям законодательства, включая:
   - Приказ №52-НҚ («Требования по обеспечению ИБ в ГБД/ГИС») – обеспечение регистрации событий, контроль доступа, ограничение трафика, управление уязвимостями.
   - Постановление №832 («Правила мониторинга и реагирования на инциденты ИБ») — обеспечение своевременного обнаружения, классификации, регистрации и обработки инцидентов, а также корректное предоставление отчётности.

ПРИЛОЖЕНИЕ

Приложение 1. Успешно установленные агенты

№	Наименование хоста	sysmon	DLP	EDR
1	ONFMD3V	да	да	да
2	HQHRP8F	да	да	да
3	6VCF7F0	да	да	да
4	DESKTOP-7PQ9JGE	да	да	да
5	AKYLZHAN	да	да	да
6	AIGUL	да	да	да
7	ULBOLSYN	да	да	да
8	DESKTOP-9NI4RVE	да	да	да
9	DESKTOP-N9EPV9O	да	да	да
10	DESKTOP-6BNCNOU	да	да	да
11	DESKTOP-MH0J2Q7	да	да	да
12	DESKTOP-H8HNE82	да	да	да
13	DESKTOP-C187F6G	да	да	да
14	DESKTOP-O6H7LQG	да	да	да
15	DESKTOP-MVAUDIA	да	да	да
16	DESKTOP-B4JQSQQ	да	да	да
17	DESKTOP-MQIC7R3	да	да	да
18	DESKTOP-7POB5LS	да	да	да
19	DESKTOP-4VPO3O4	да	да	да
20	DESKTOP-7NGLS2A	да	да	да
21	DESKTOP-B1MA7BI	да	да	да
22	DESKTOP-K0VKNJN	да	да	да
23	DESKTOP-AUKCRS0	да	да	да
24	ENRG-PC-0029	да	да	да
25	OVG-1	да	да	да
26	DESKTOP-8N5OSS5	да	да	да
27	DESKTOP-7Q75ME4	да	да	да
28	HEAL-PC-0019	да	да	да
29	DESKTOP-CULT5	да	да	да
30	DESKTOP-CULT1	да	да	да
31	DESKTOP-CULT60	да	да	да
32	CULT-HP-2	да	да	да
33	DESKTOP-LA6F3BM	да	да	да
34	CULT-PC-0010	да	да	да
35	CULT-PC-0017	да	да	да
36	DESKTOP-E9G3I7B	да	да	да
37	DESKTOP-EIPEA03	да	да	да
38	DESKTOP-24NQHNS	да	да	да

№	Наименование хоста	sysmon	DLP	EDR
39	DESKTOP-EOPKGAU	да	да	да
40	DESKTOP-QV7S0RL	да	да	да
41	DESKTOP-IQ2LFU8	да	да	да
42	DESKTOP-4KGULFP	да	да	да
43	DESKTOP-7K82JQC	да	да	да
44	DESKTOP-RJU5PID	да	да	да
45	DESKTOP-N3ARAQL	да	да	да
46	DESKTOP-28DSOT9	да	да	да
47	DESKTOP-OPQD1MJ	да	да	да
48	DESKTOP-CO6FS19	да	да	да
49	DESKTOP-L06BB02	да	да	да
50	DESKTOP-2VM9KM5	да	да	да
51	DESKTOP-MLQ5RLG	да	да	да
52	DESKTOP-34886QN	да	да	да
53	DESKTOP-1450DBF	да	да	да
54	DESKTOP-AJKO4DH	да	да	да
55	Lawyer	да	да	да
56	DESKTOP-KERVJRP	да	да	да
57	DESKTOP-6L825P7	да	да	да
58	UO-2022	да	да	да
59	DESKTOP-UQ6NS5G	да	да	да
60	SPORT-56-1	да	да	да
61	Sport1	да	да	да
62	Sport5	да	да	да
63	sport464	да	да	да
64	SPORT-66-2	да	да	да
65	SPORT-PC1	да	да	да
66	DESKTOP-OMLGVDK	да	да	да
67	DESKTOP-2SI92MJ	да	да	да
68	DESKTOP-8H6ORVI	да	да	да
69	DESKTOP-UVRH5LA	да	да	да
70	DESKTOP-GCRTSIJ	да	да	да
71	DESKTOP-C6KVP4D	да	да	да
72	DESKTOP-5LK01I9	да	да	да
73	DESKTOP-IV65PMK	да	да	да
74	DESKTOP-FL3RB84	да	да	да
75	DESKTOP-MB08JT6	да	да	да
76	DESKTOP-4LH9VES	да	да	да
77	DESKTOP-MKVUSJV	да	да	да
78	DESKTOP-OSN7JUO	да	да	да
79	DESKTOP-2O3Q61U	да	да	да
80	DESKTOP-P3OSI15	да	да	да

№	Наименование хоста	sysmon	DLP	EDR
81	DESKTOP-26FSAF4	да	да	да
82	DESKTOP-OVQ7SJE	да	да	да
83	DESKTOP-67A1CGR	да	да	да
84	DESKTOP-AN8SHTD	да	да	да
85	DESKTOP-IQ2LFU8	да	да	да
86	DESKTOP-2SI92MJ	да	да	да
87	DESKTOP-GCRTSIJ	да	да	да
88	DESKTOP-2O3Q61U	да	да	да
89	DESKTOP-67A1CGR	да	да	да
90	DESKTOP-GF86AKS	да	да	да
91	DESKTOP-AUKCRS0	да	да	да
92	BAKOW	да	да	да
93	DESKTOP-0DEUENJ	да	да	да
94	DESKTOP-EBCPBJP	да	да	да
95	DESKTOP-AAFCT8U	да	да	да
96	DESKTOP-FMBEGSB	да	да	да
97	DESKTOP-P3OSI15	да	да	да
98	BUH	да	да	да
99	UO-2022	да	да	да
100	DESKTOP-L06BB02	да	да	да
101	DESKTOP-AJKO4DH	да	да	да
102	DESKTOP-CULT27	да	да	да

Приложение 2. Основная таблица аудита (пункты 1–66) с критерий оценки соответствия

№	Перечень требований	Фактическое состояние	Оценка соответствия
1	Подключение к Единому шлюзу доступа к Интернету (ЕШД)	Проверены внешние IP-адреса 89.218.12.50, 88.204.143.162, 78.142.250.198, 46.34.147.70, 78.142.250.239, 217.11.70.102 — не подключены к ЕШД.	Не соответствует
2	Оповещение НКЦИБ об инцидентах ИБ	Процесс реализован в соответствии с п.38 и 41 Постановления №832. Критических инцидентов не зафиксировано. Оповещение осуществляется ТОО «MSSP.GL» и ОЦИБ.	Соответствует
3	Применение средств идентификации и управления доступом	Внедрена система учётных записей Windows AD частично. EDR установлены вручную, без интеграции с AD.	Частично соответствует
4	Мониторинг обеспечения ИБ объектов информатизации	Реализован договором с ТОО «MSSP.GL» используется SIEM, EDR, T-Lab Sandbox.	Соответствует
5	Наличие антивирусных средств и обновлений ОС	EDR агенты установлены вручную, в том числе на Windows Home Edition. ОС требует обновления до Windows 11 Pro.	Частично соответствует
6	Наличие подразделения или ответственного за ИБ	Назначен ответственный сотрудник по ИБ, обучение подтверждено. Дополнительно функции выполняет ОЦИБ.	Соответствует
7	Наличие нормативно-технической документации по ИБ	В наличии Политика ИБ, Правила идентификации активов, Методика оценки рисков. Документы утверждены на казахском и русском языках.	Соответствует
8	Применение многофакторной аутентификации (МФА)	МФА не реализована для доступа к критическим системам. Аутентификация только через пароль AD.	Не соответствует
9	Внесение обязанностей по ИБ в	В должностных инструкциях сотрудников ИБ и администраторов отражены функции по обеспечению ИБ. ОЦИБ контролирует выполнение.	Соответствует

№	Перечень требований	Фактическое состояние	Оценка соответствия
	должностные инструкции		
10	Применение СКЗИ	СКЗИ не задействованы, шифрование выполняется средствами ОС (BitLocker, TLS).	Соответствует
11	Хранение и восстановление государственных ЭИР	Резервное копирование выполняется регулярно средствами ОС и хранилища. Контроль восстановления задокументирован.	Не применимо
12	Применение CMS для защиты ЭИР	Пункт 12 признаётся не применимым к проверяемому объекту, поскольку Акимат г. Алматы не является владельцем или оператором государственных электронных информационных ресурсов (ЭИР), размещённых в публичном интернет-пространстве. Функции по администрированию и защите контента официального интернет-ресурса (в доменной зоне .gov.kz) реализуются централизованно через АО «Национальные информационные технологии» (НИТ), являющееся техническим оператором государственных веб-ресурсов.	Не применимо
13	Применение регистрационных свидетельств для доменов .GOV.KZ и СКЗИ для HTTPS	Домен зарегистрирован через АО НИТ, сертификат безопасности используется.	Соответствует
14	Управление идентификацией при виртуализации	Аутентификация выполняется средствами платформы, федеративная идентификация не реализована.	Частично соответствует
15	Аудит событий ИБ при виртуализации	События фиксируются в SIEM. Хранение журналов обеспечено, проверка корректности ведётся ежемесячно.	Соответствует
16	Регистрация и мониторинг событий ИБ при виртуализации	Реализовано через SIEM. Есть автоматические оповещения о критических событиях.	Соответствует
17	Исполнение процедур системного и сетевого администрирования	Контроль целостности ОС, приложений и сетевых конфигураций выполняется средствами SIEM и антивирусных решений.	Соответствует

№	Перечень требований	Фактическое состояние	Оценка соответствия
18	Обеспечение системы хранения данных системой резервного копирования	Резервное копирование выполняется автоматически, тестирование копий проводится ежеквартально.	Соответствует
19	Применение программно-технических средств защиты с СКЗИ при выделенных каналах связи	Каналы защищены межсетевыми экранами Check Point. СКЗИ не активированы.	Частично соответствует
20	Исключение сопряжения ЛС внутреннего и внешнего контура	Сегментация выполнена. Прямое соединение между контурами отсутствует.	Соответствует
21	Использование ведомственной электронной почты и мессенджеров, размещенных в РК	Используется корпоративная почта и Telegram-канал для взаимодействия, сервера размещены в РК.	Соответствует
22	Наличие бесперебойного электропитания активного оборудования ЛС	ИБП установлены и функционируют в штатном режиме. Есть журнал обслуживания.	Соответствует
23	Физическое отключение неиспользуемых портов ЛС	Ненужные порты деактивированы, контроль осуществляется сетевыми администраторами.	Не соответствует
24	Применение межсетевого экранирования	Межсетевые экраны Check Point используются для фильтрации и защиты. Конфигурации проверяются ТОО «MSSP.GL».	Соответствует

№	Перечень требований	Фактическое состояние	Оценка соответствия
25	Документирование технического сопровождения оборудования	Журналы обслуживания и устранения неисправностей не ведутся в серверном помещение..	Не соответствует
26	Наличие системы контроля и управления доступом в серверном помещении	СКУД реализована, доступ ограничен уполномоченными лицами, ведется журнал посещений.	Соответствует
27	Наличие списка авторизованных лиц для сопровождения объектов ИКИ	Список утверждён приказом, хранится в отделе ИБ и актуализируется ежеквартально.	Соответствует
28	Наличие системы обеспечения микроклимата в серверном помещении	Система кондиционирования и вентиляции установлена, питание осуществляется от ИБП. Автоматическое отключение при пожаре предусмотрено.	Соответствует
29	Наличие системы охранной сигнализации в серверном помещении	Система охранной сигнализации функционирует, сигналы поступают на пульт круглосуточной охраны.	Соответствует
30	Наличие системы видеонаблюдения в серверном помещении	Видеонаблюдение ведётся круглосуточно, архив хранится 30 суток. Камеры покрывают все зоны доступа.	Соответствует
31	Наличие системы пожарной сигнализации в	Установлены температурные и дымовые датчики, сигнал выводится на пульт охраны.	Соответствует

№	Перечень требований	Фактическое состояние	Оценка соответствия
	серверном помещении		
32	Наличие системы пожаротушения в серверном помещении	Установлена автоматическая система газового пожаротушения, независимая от общей системы здания.	Соответствует
33	Наличие системы гарантированного электропитания в серверном помещении	Автомат ввода резерва установлен, электропитание резервируется источниками ИБП.	Соответствует
34	Наличие системы заземления в серверном помещении	Заземление выполнено согласно нормативам, каждая стойка соединена с общей шиной.	Соответствует
35	Отсутствие источников электромагнитных помех в кроссовом помещении	Источники ЭМ-помех отсутствуют, трансформаторы и электродвигатели не размещены рядом.	Соответствует
36	Отсутствие труб и вентилей водоснабжения в кроссовом помещении	Коммуникации водоснабжения отсутствуют, риск затопления минимален.	Соответствует
37	Наличие систем пожарной безопасности в кроссовом помещении	Система пожарной безопасности установлена и интегрирована с общим пультом охраны.	Соответствует

№	Перечень требований	Фактическое состояние	Оценка соответствия
38	Отсутствие легковоспламеняющихся материалов в кроссовом помещении	В помещении отсутствуют деревянные стеллажи и бумажные материалы, используется металлическая мебель.	Соответствует
39	Наличие отдельной линии электропитания в кроссовом помещении	Выделенная линия электропитания имеется, запитана от отдельного автомата.	Соответствует
40	Наличие систем охранной сигнализации и контроля доступа в кроссовом помещении	СКУД установлена, охранная сигнализация функционирует, контроль ведется круглосуточно.	Соответствует
41	Наличие системы кондиционирования в кроссовом помещении	Система кондиционирования установлена и подключена к источнику бесперебойного питания.	Соответствует
42	Использование средств мониторинга и управления инцидентами (SIEM, IDS/IPS)	Внедрены SIEM и IDS/IPS, используется ТОО «MSSP.GL» для мониторинга и реагирования.	Соответствует
43	Создание или использование услуг Оперативного центра ИБ (SOC)	Функции SOC выполняются ТОО «MSSP.GL». Взаимодействие с НКЦИБ реализовано.	Соответствует
44	Размещение Интернет-ресурсов на	Ресурсы размещены на оборудовании, находящемся на территории Республики Казахстан.	Соответствует

№	Перечень требований	Фактическое состояние	Оценка соответствия
	доменах .KZ и .ҚАЗ в пределах РК		
45	Проведение регулярной инвентаризации серверного оборудования	Инвентаризация серверов проводится ежеквартально с фиксацией в акте.	Соответствует
46	Приобретение ПО из реестра доверенного ПО и продукции электронной промышленности	Закупки осуществляются с проверкой в реестре доверенного ПО. При отсутствии — оформляется исключение.	Соответствует
47	Контроль событий нарушений ИБ в организации	Мониторинг событий ИБ выполняется через SIEM и ТОО «MSSP.GL». Журналы синхронизируются, хранятся не менее трёх лет.	Соответствует
48	Наличие соглашения с третьими лицами по вопросам ИБ	Соглашения с подрядчиками содержат условия конфиденциальности и ответственности за нарушение требований ИБ.	Соответствует
49	Управление доступом при увольнении и изменении трудового договора	Процедура отключения учётных записей реализована. При увольнении доступ аннулируется в течение 1 дня.	Соответствует
50	Учёт прохождения обучения по ИБ и информатизации	Сотрудники проходят обучение ИБ не реже 1 раза в год, журналы инструктажа ведутся.	Соответствует
51	Регистрация критических событий ИБ в НКЦИБ	Критические события не зафиксированы. При обнаружении процесс передачи информации реализуется силами ОЦИБ.	Соответствует
52	Проведение аудита ИБ не реже 1 раза в год	Аудит ИБ проводится ежегодно согласно договору с поставщиком услуг ТОО «MSSP.GL».	Соответствует

№	Перечень требований	Фактическое состояние	Оценка соответствия
53	Списание ИС, ПО и сервисов с сохранением структуры БД	Функция резервного копирования и восстановления реализована средствами СУБД. Инструкции подготовлены.	Соответствует
54	Наличие акта испытаний на соответствие требованиям ИБ	Приемочные испытания проводятся при вводе в эксплуатацию систем. Акт хранится в ИБ.	Соответствует
55	Интерфейс прикладного ПО на казахском и русском языках	ПО поддерживает выбор интерфейса на двух языках. Требования соблюдены.	Соответствует
56	Мониторинг действий пользователей и использования ресурсов	Мониторинг выполняется средствами SIEM, агентами EDR и T-Lab Sandbox. Выявленные события анализируются ТОО «MSSP.GL».	Соответствует
57	Наличие технической документации на казахском и русском языках для ПО	Вся эксплуатационная документация на прикладное ПО предоставлена на русском и частично на казахском языке.	Частично соответствует
58	Обеспечение высокой доступности сервера встроенных систем	Реализовано резервирование блоков питания, вентиляторов и дисков. Система уведомляет о сбоях.	Соответствует
59	Наличие средств гарантированного уничтожения информации при выводе носителей из эксплуатации	Используется программное средство очистки дисков (wipe), уничтожение фиксируется актом.	Соответствует
60	Наличие схемы локальной сети	Схема ЛВС имеется в актуальном состоянии, содержит обозначения всех узлов и сегментов.	Соответствует

№	Перечень требований	Фактическое состояние	Оценка соответствия
61	Наличие серверного оборудования, АПК и систем хранения данных в серверном помещении	Серверное оборудование и СХД установлены в соответствии с проектной документацией.	Соответствует
62	Расположение серверного помещения в отдельном, непроходном помещении без оконных проемов	Серверное помещение размещено в отдельном помещении, окна заделаны негорючими материалами.	Соответствует
63	Наличие фальшпола и/или фальшпотолка для размещения кабельных систем	В серверном помещении установлен фальшпол, обеспечивающий скрытую прокладку кабельных трасс.	Соответствует
64	Исключение прохождения транзитных коммуникаций через серверное помещение	Транзитные трубы и коммуникации вынесены за пределы помещения.	Соответствует
65	Размещение основных и резервных серверных помещений в разных зданиях	Основное и резервное серверные помещения расположены в разных зданиях, связь обеспечивается по выделенному каналу.	Соответствует
66	Исключение размещения в одной среде объектов разных классов информатизации	Объекты разных классов ИС размещены на отдельных серверах и в разных виртуальных средах.	Соответствует