

О подходах к оценке показателя текущего состояния защиты информации в соответствии с Методикой оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Докладчик: Щёкотов Дмитрий Геннадиевич
начальник 9 отдела
Управления ФСТЭК России по Уральскому федеральному округу





УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" и в Положение, утвержденное этим Указом

1. Внести в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137; 2014, № 36, ст. 4833; № 44, ст. 6041; 2015, № 4, ст. 641; 2016, № 1, ст. 211; 2017, № 48, ст. 7198; 2018, № 20, ст. 2818; 2019, № 24, ст. 3057; 2020, № 35, ст. 5554; 2021, № 21, ст. 3552; № 50, ст. 8526; 2023, № 22, ст. 3919) и в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное этим Указом, следующие изменения:

а) в пункте 6 Указа:

в подпункте 1 слова "в количестве 260 единиц" заменить словами "в количестве 289 единиц";

в подпункте 2 слова "в количестве 1012 единиц" заменить словами "в количестве 1101 единицы";

б) в Положении:

дополнить пунктом 6¹ следующего содержания:

"6¹. ФСТЭК России обеспечивает в пределах своей компетенции создание информационной автоматизированной системы для управления деятельностью по технической защите информации



Положение о Федеральной службе по техническому и экспортному контролю, утверждено Указом Президента Российской Федерации от 16 августа 2004 г. № 1085

Подпункт 6¹ пункта 8 Положения

ФСТЭК России осуществляет в пределах своей компетенции мониторинг текущего состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры



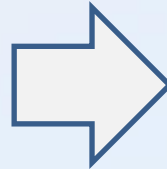
Мониторинг осуществляется по 16 частным показателям безопасности, разделенным на 4 группы

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ И УПРАВЛЕНИЕ ДАННОЙ ДЕЯТЕЛЬНОСТЬЮ

3



**Приказ ФСТЭК России от 11 апреля
2025 г. № 117
«Об утверждении Требований
о защите информации, содержащейся
в государственных информационных
системах, иных информационных
системах государственных органов,
государственных унитарных
предприятий, государственных
учреждений»**



Пункт 31 Приказа

Оценка состояния защиты информации должна проводиться на основе определения оператором (обладателем информации) показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации
(показатель защищенности $K_{зи}$)

Пункт 32 Приказа

Расчет и оценка показателя защищенности $K_{зи}$ должны проводиться оператором (обладателем информации) не реже одного раза в шесть месяцев

Пункт 33 Приказа

По решению руководителя оператора (обладателя информации) разрабатывается план мероприятий по совершенствованию защиты информации, в котором указываются мероприятия, сроки их выполнения, ответственные за их реализацию

МЕТОДИЧЕСКИЙ ДОКУМЕНТ ПО ОЦЕНКЕ ТЕКУЩЕГО СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден
ФСТЭК России
11 ноября 2025 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**Методика
оценки показателя состояния технической защиты
информации в информационных системах и
обеспечения безопасности объектов критической
информационной инфраструктуры Российской
Федерации**

2025

Пункт 16 Методики

Результаты оценки показателя защищенности $K_{зи}$ предоставляются органом (организацией) в ФСТЭК России в целях оценки текущего состояния защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

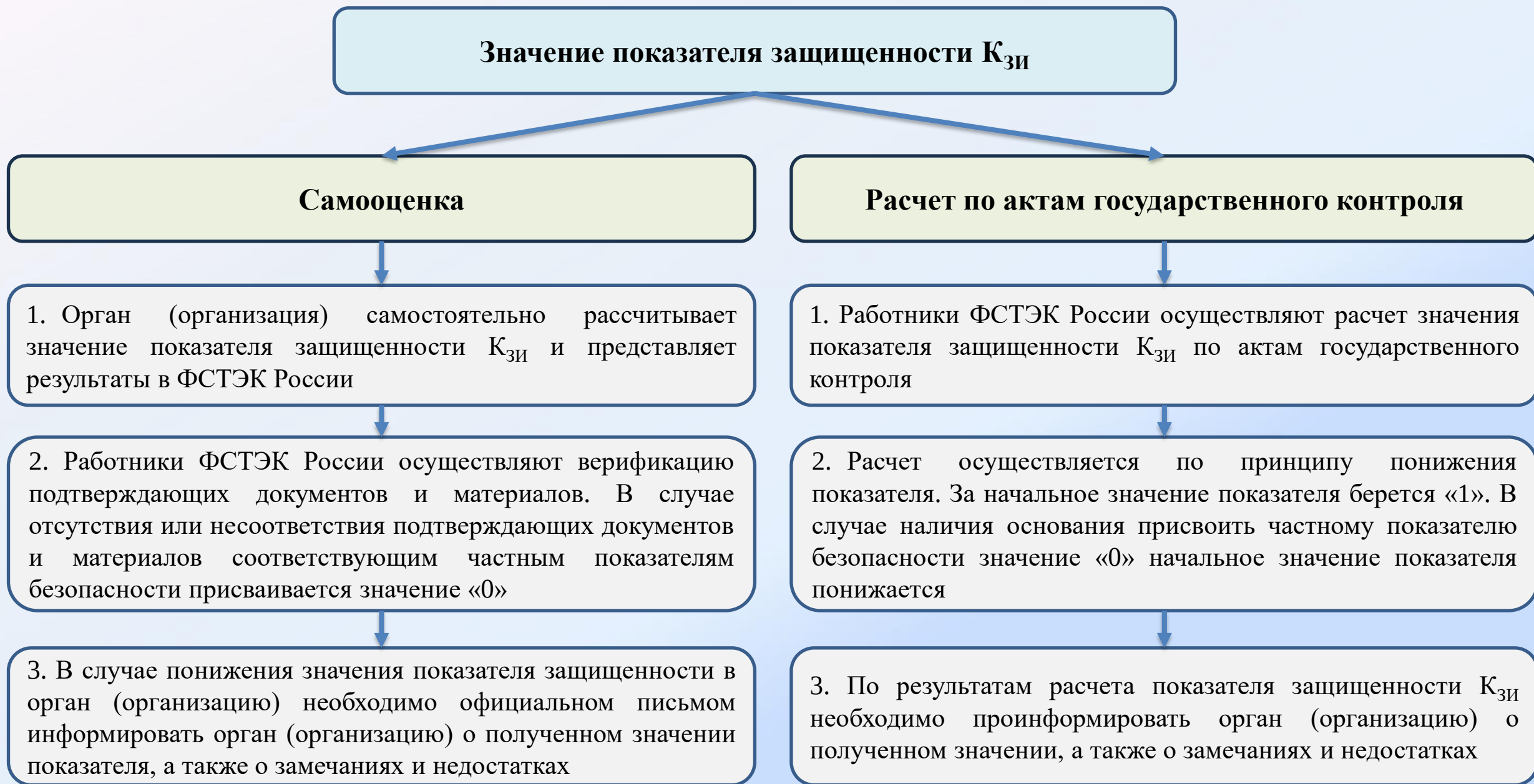
Для подтверждения результатов оценки в ФСТЭК России представляются документы и материалы в соответствии с Приложением к Методике

Документы и материалы,
предоставляющиеся по
запросу ФСТЭК России*

Документы и материалы,
предоставляющиеся с
результатами оценки

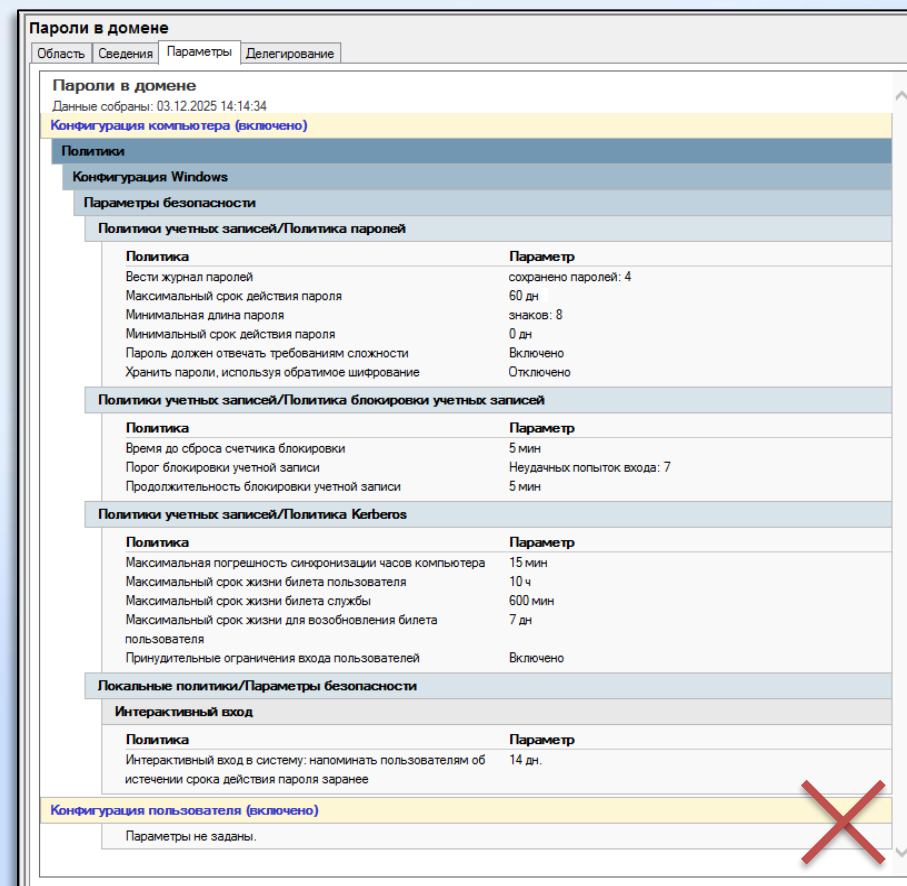
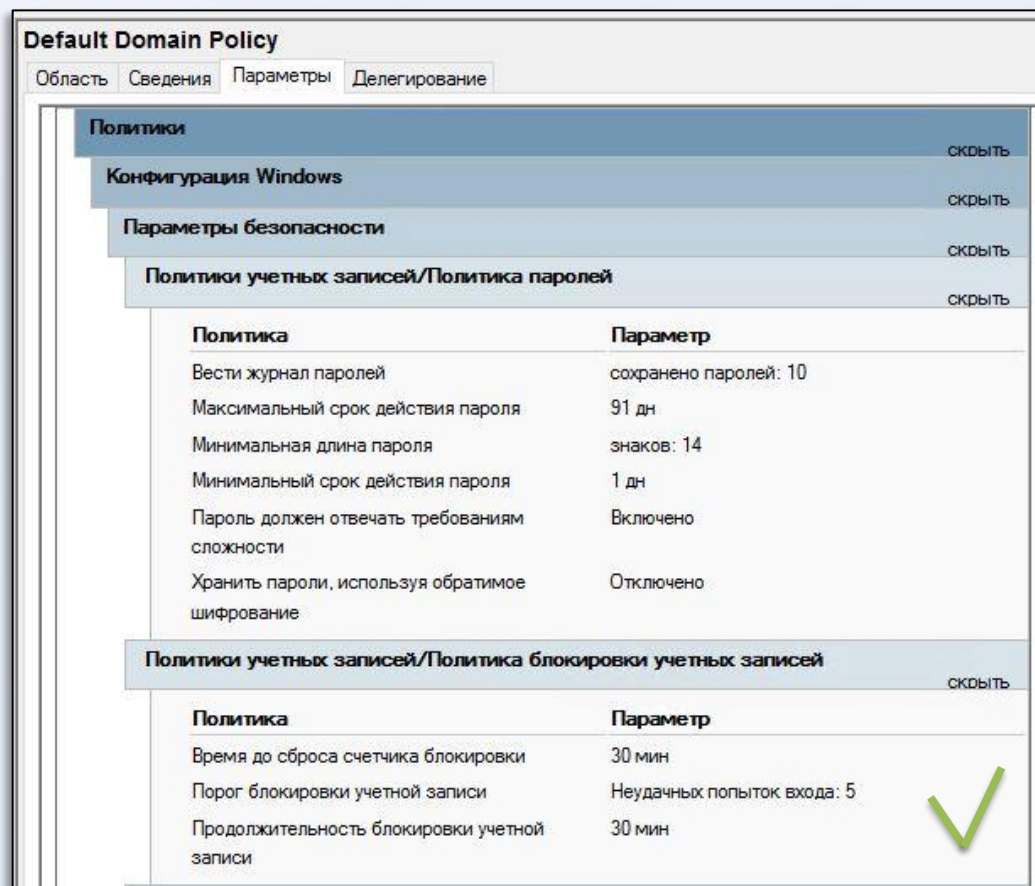
* запрашиваются в случае возникновения инцидентов информационной безопасности при достигнутом минимальном уровне защиты от типовых актуальных УБИ ($K_{зи} = 1$)

СПОСОБЫ ПОЛУЧЕНИЯ РЕЗУЛЬТАТОВ ОЦЕНКИ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ $K_{ЗИ}$



Частный показатель безопасности k21 «Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике. В случае отсутствия технической возможности обеспечения требуемой сложности паролей реализованы компенсирующие меры»

С результатами оценки предоставляется снимок экрана, отображающий установленные на средстве реализации парольной политики настройки для паролей учетных записей пользователей информационных систем органа (организации), подтверждающий соответствие настроек паролей учетных записей пользователей информационных систем органа (организации) парольной политике.



Частный показатель безопасности k21 «Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике. В случае отсутствия технической возможности обеспечения требуемой сложности паролей реализованы компенсирующие меры»

С результатами оценки предоставляется отчет, сформированный средством анализа защищенности или иным инструментальным средством, позволяющим выявить пароли, не соответствующие установленным требованиям (например, сетевой аудит паролей в Сканер-ВС, MaxPatrol VM, RedCheck).


ОТЧЁТ

№ отчёта	5821fed1-9a3b-487d-843e-65a6a3380afa
Профиль	Compliance
Задание	Аудит конфигураций rein-as-dc
Начало/завершение сканирования	15.12.2025 15:37:38 / 15.12.2025 15:39:17
Формирование отчёта	16.12.2025 15:56:10
Имя	Audit_pass_Linux
Хосты [2]	rein-as-dc3.rein.lan, rein-as-dc1.rein.lan

Astra Linux SE и CE / ALT / RED OS 7.3 – Аудит безопасности критической информационной инфраструктуры - ФСТЭК №239 (версия: 9, профиль: 3 категория значимости)

✔ Соответствие (19)

✔ Управление доступом (УПД)

✔ Управление учетными записями пользователей (УПД.1)

✔ Проверка правильности хранения и существования хэшей паролей

✔ Проверка на скрытость хэшей паролей во всех аккаунтах
Критичность: Средний

✔ Убедиться, что нет символа '+' в файле /etc/passwd, /etc/shadow, /etc/group
Критичность: Низкий

✔ Разделение полномочий (ролей) пользователей (УПД.4)

✔ Ограничение входа суперпользователя в виртуальную консоль
Критичность: Средний

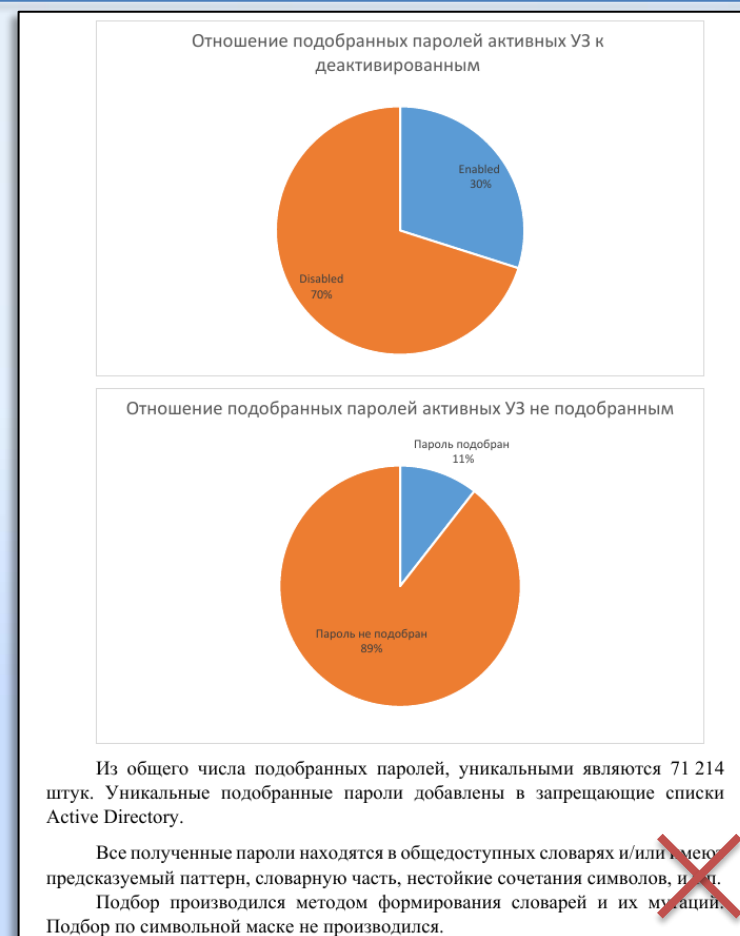
✔ Ограничение входа суперпользователя через последовательный порт
Критичность: Низкий

✔ Проверка, что только у суперпользователя UID 0
Критичность: Средний

✔ Управление действиями пользователей до идентификации и аутентификации (УПД.11)

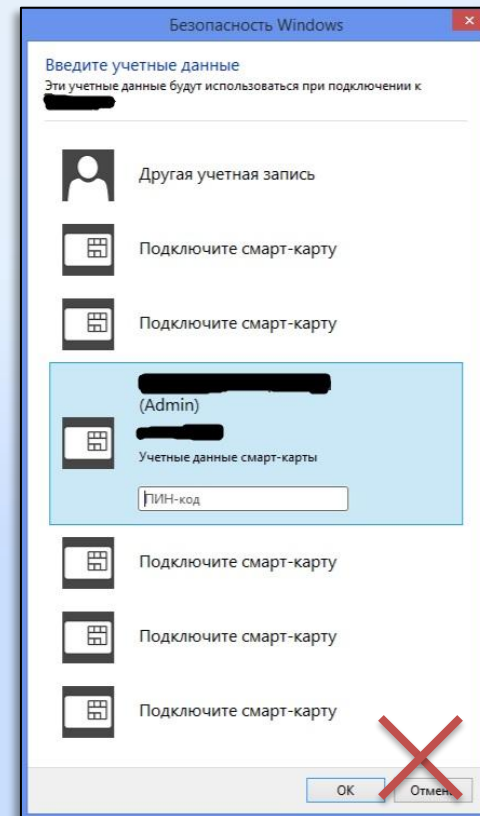
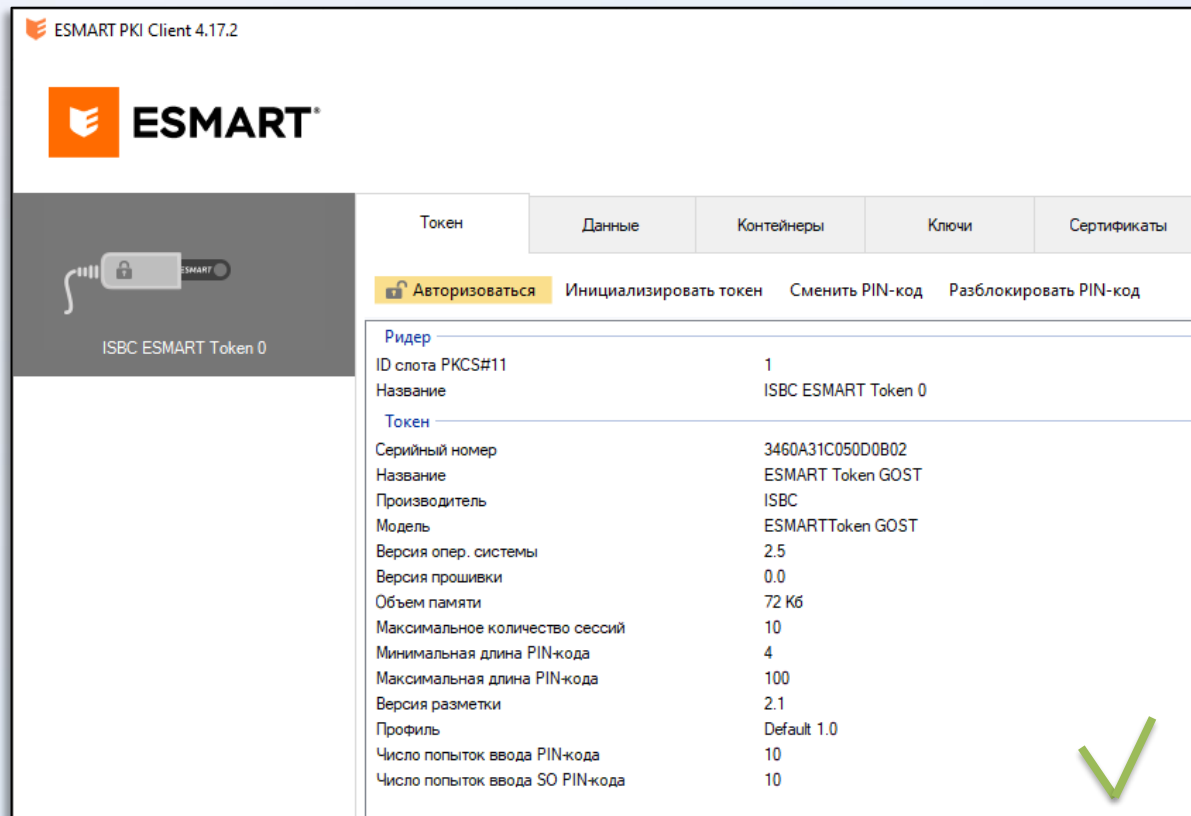
✔ Предотвращение входа в аккаунт с пустым паролем
Критичность: Высокий

✔



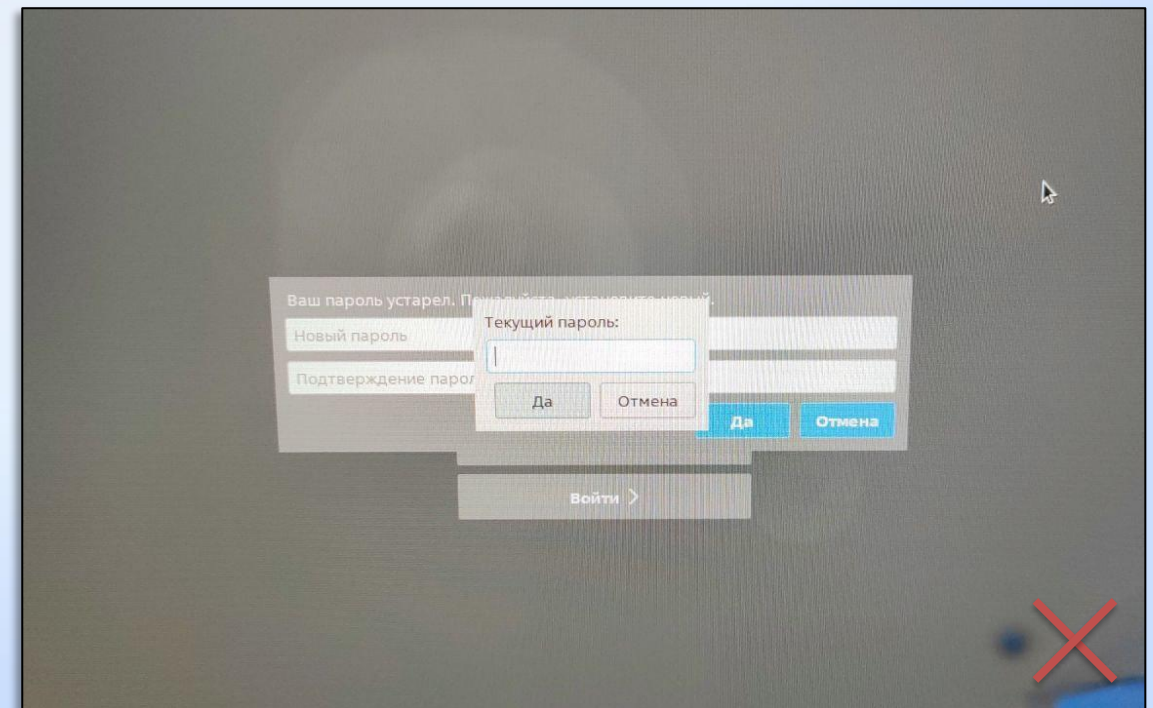
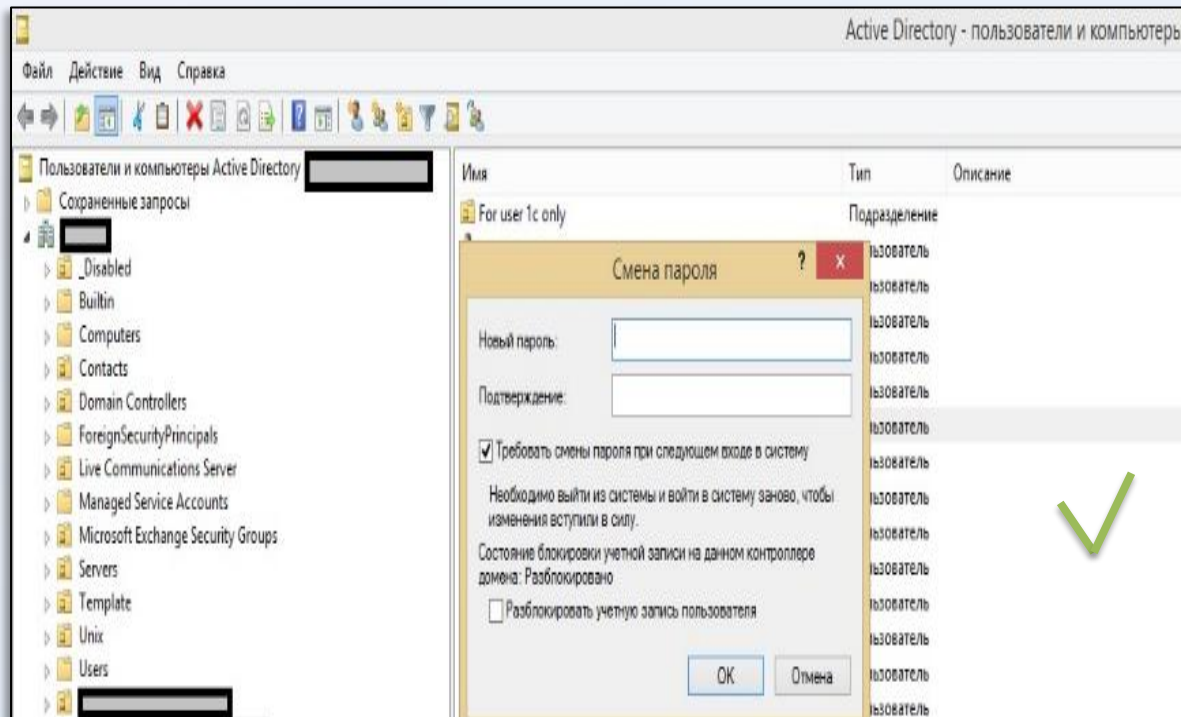
Частный показатель безопасности k22 «Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)»

С результатами оценки предоставляются сведения о программном, программно-аппаратном средстве (снимок экрана панели управления средства), с использованием которого осуществляется многофакторная аутентификация привилегированных пользователей органа (организации).



Частный показатель безопасности k23 «Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию»

С результатами оценки предоставляется снимок экрана, отображающий установленные на средстве реализации парольной защиты (политики) настройки сброса пароля после первой аутентификации для используемых в информационной системе сервисных учетных записей и учетных записей разработчиков.



Частный показатель безопасности k23 «Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию»

С результатами оценки предоставляется отчет, сформированный средством анализа защищенности или иным инструментальным средством, позволяющим выявить установленные по умолчанию пароли учетных записей пользователей (например, сетевой аудит паролей в Сканер-ВС, MaxPatrol VM, RedCheck).

Подбор паролей

Настройки задачи

Пользователи

Пароли

Название задачи

подбор паролей esxv-vegv

24/100

Цели

Введите цели

Импортировать

Сервис

Порт

Закончить подбор при первом положительном результате

Выберите хотя бы один из параметров подбора

Словари

Топ 15 (en) Топ 25 женских имен (en) Топ 25 мужских имен (en)

Пользователи

Пусто

Введите логин пользователя

Выберите хотя бы один из параметров подбора

Словари

Цифры Женские имена (en) Клавиатурные сочетания (en)

Пароли

Пусто

Введите пароль

☒ Проверить пустой пароль

☒ Проверить пароль, совпадающий с логином

☒ Проверить пароль, совпадающий с логином в обратном порядке

Сканер-ВС

анализ защищенности

7

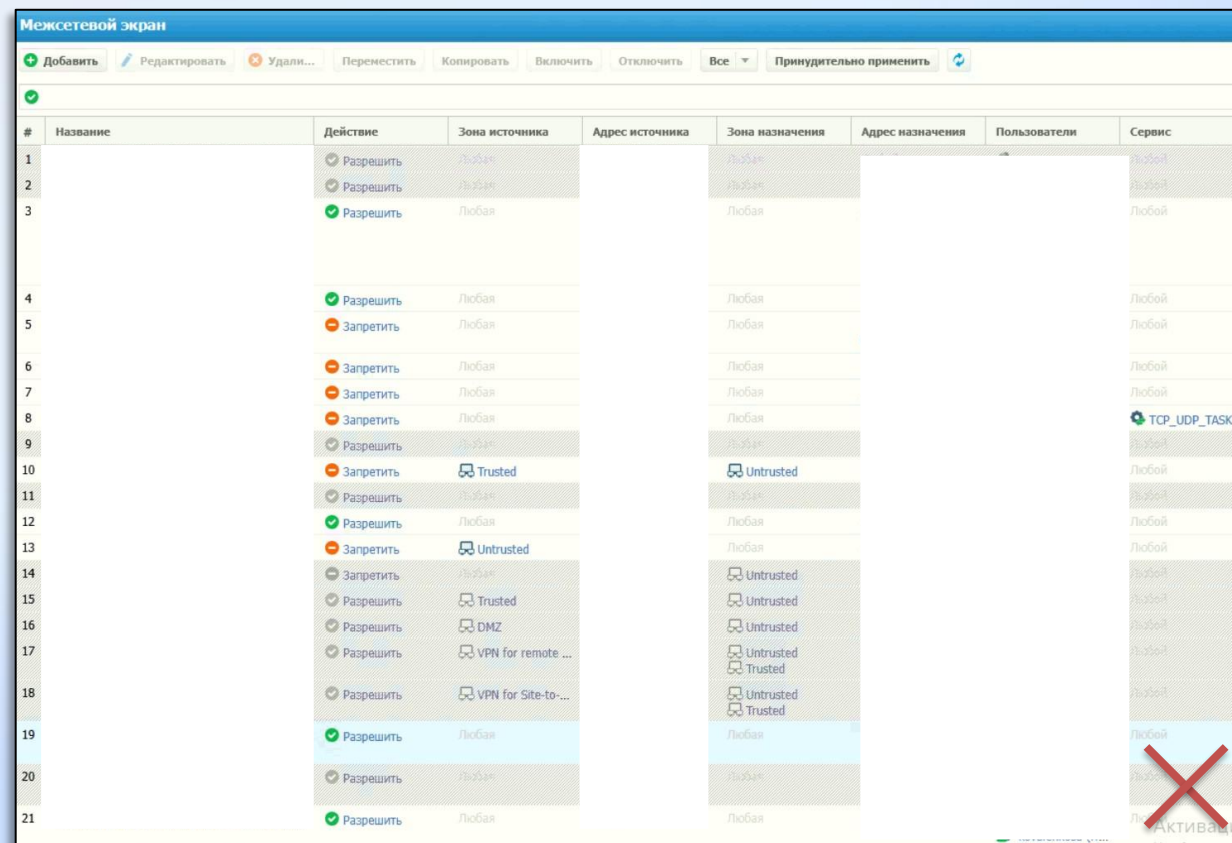
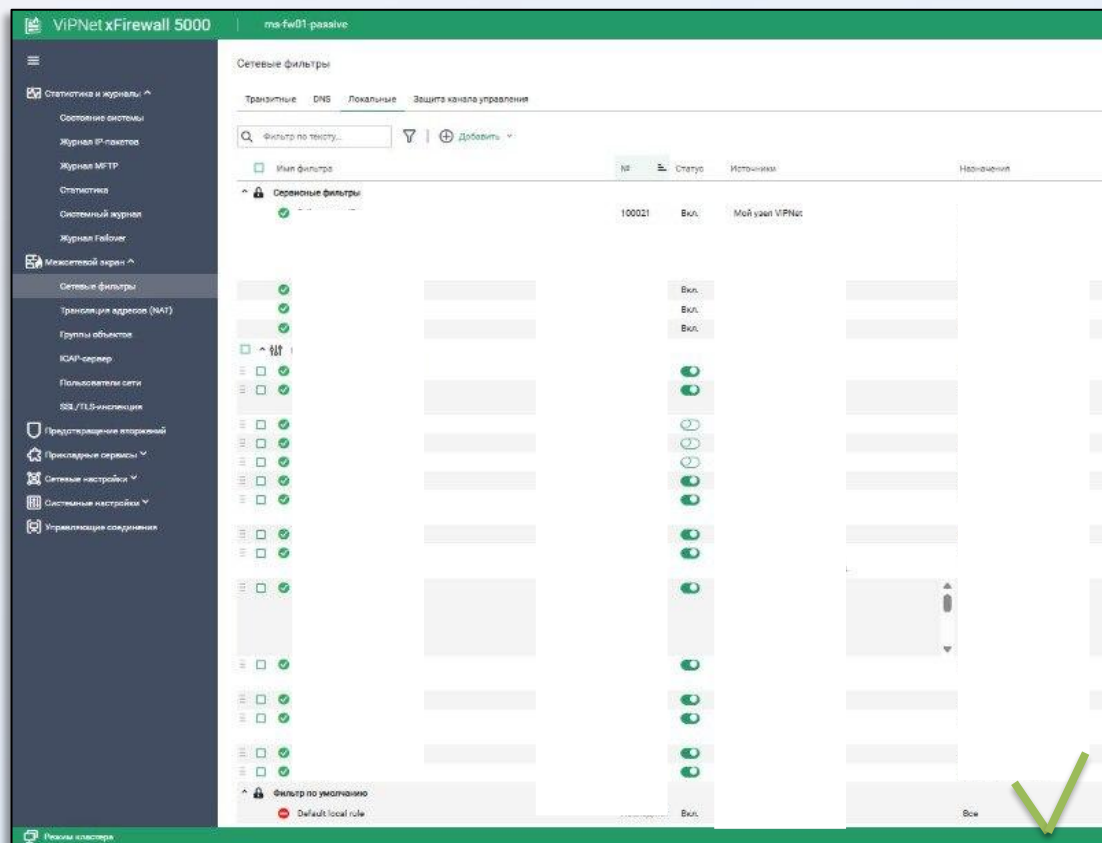
3. Подобранные пароли

Перечень учетных записей отсутствует: задача подбора пароля не проводилась, либо не имеет результата.

	A	B	C	D	E	F
1	@Host	Host.OsName	Host.@CreationTime	Host.@UpdateTime	login	password
2		Debian	01.10.2024	25.12.2025		
3		Debian	08.10.2025	25.12.2025		
4		Debian	05.09.2025	25.12.2025		
5		Astra	09.10.2025	25.12.2025		
6		Astra	08.10.2025	25.12.2025		
7		Debian	08.10.2025	25.12.2025		
8		Astra	08.10.2025	25.12.2025		
9		Astra	09.10.2025	25.12.2025		
10			25.12.2025	25.12.2025		
11		Debian	02.07.2025	25.12.2025		
12		Debian	08.10.2025	25.12.2025		
13		Astra	08.10.2025	25.12.2025		
14		Debian	09.10.2025	25.12.2025		
15		Astra	08.10.2025	25.12.2025		
16		Astra	08.10.2025	25.12.2025		
17		Debian	01.10.2024	25.12.2025		
18		ESXi	25.03.2025	25.12.2025		
19		Debian	09.10.2025	25.12.2025		
20			25.12.2025	25.12.2025		
21			25.12.2025	25.12.2025		
22		Astra	08.10.2025	25.12.2025		
23		Debian	08.10.2025	25.12.2025		
24		ESXi	01.10.2024	25.12.2025		
25		Debian	28.11.2024	25.12.2025		
26		Debian	01.10.2024	25.12.2025		

Частный показатель безопасности кз1 «На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет, контролируется межсетевыми экранами уровня L3/L4)»

С результатами оценки предоставляются сведения о применяемых средствах межсетевого экранирования уровня L3/L4 и снимки экрана панели управления средств межсетевого экранирования, содержащие настройки правил доступа к сервисам (службам), доступным из сети «Интернет».



Частный показатель безопасности k32 «На устройствах и интерфейсах, доступных из сети Интернет, отсутствуют уязвимости критического уровня опасности с датой публикации обновлений (компенсирующих мер по устранению) в банке данных угроз ФСТЭК России, на официальных сайтах разработчиков, иных открытых источниках более 30 дней или в отношении таких уязвимостей реализованы компенсирующие меры»

С результатами оценки предоставляется отчет, сформированный средством анализа защищенности, содержащий результаты сканирования устройств и интерфейсов, доступных из сети «Интернет», на наличие уязвимостей уровня «критический» (с датой сканирования не ранее 30 дней даты проведения оценки).



Полный отчет по проекту "scan-host"
на
25.12.2025 15:27:51.



Сканер-ВС
анализ защищенности

Оглавление

1. Резюме для руководителя	4
2. Границы проекта	6
3. Хост	7
3.1. Уязвимости	8
4. Хост	8
4.1. Уязвимости	8
5. Хост	8
5.1. Уязвимости	8
6. Хост	9
6.1. Уязвимости	9
7. Хост	9
7.1. Уязвимости	9
8. Хост	10
8.1. Уязвимости	10
9. Хост	10
9.1. Уязвимости	10
10. Хост	10
10.1. Уязвимости	10
11. Хост	11
11.1. Уязвимости	11
12. Хост	11
12.1. Уязвимости	11
13. Хост	11
13.1. Уязвимости	11
14. Хост	12
14.1. Уязвимости	12
15. Хост	12
15.1. Уязвимости	12
16. Хост	13
16.1. Уязвимости	13
17. Хост	13
17.1. Уязвимости	13
18. Хост	14
18.1. Уязвимости	14
19. Хост	14
19.1. Уязвимости	14
20. Хост	14
20.1. Уязвимости	14
21. Хост	15
21.1. Уязвимости	15
22. Хост	15

Дата формирования: 25.12.2025
Имя проекта: scan-host
Количество узлов: 27
Период сканирования: 25.12.2025 - 25.12.2025

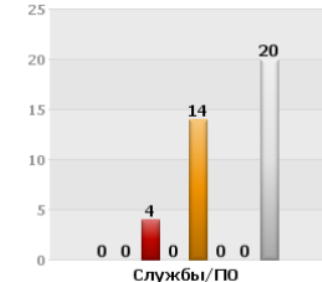
Автор: Администратор Сканер-ВС
Системная группа: -



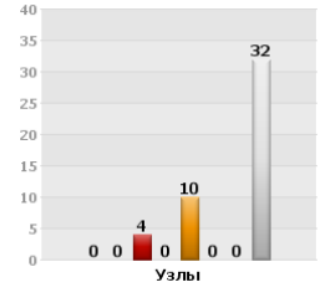
Данные, включенные в отчет

задача	узлов	сканов
ГК Внешние узлы	46	1
Итого:	46	1

Уязвимость объектов



Службы/ПО



Узлы

Уровень	Службы / ПО	Узлы
Критический уровень	0	0
Критический уровень (подозрение)	0	0
Высокий уровень	4	4
Высокий уровень (подозрение)	0	0
Средний уровень	14	10
Средний уровень (подозрение)	0	0
Низкий уровень	0	0
нет уязвимостей	20	32
Итого:	38	46



Частный показатель безопасности кзз «На пользовательских устройствах и серверах отсутствуют уязвимости критического уровня с датой публикации обновления (компенсирующих мер по устранению) более 90 дней (не менее 90% устройств и серверов) или в отношении таких уязвимостей реализованы компенсирующие меры»

С результатами оценки предоставляется отчет, сформированный средством анализа защищенности, содержащий результаты сканирования пользовательских устройств и серверов органа (организации) на наличие уязвимостей уровня «критический».

MAXPATROL

27.11.2025 17:26:56

ЦА Пользовательский сегмент

Отчёт по уязвимостям пользовательского сегмента ЦА

Параметры отчета

Тип отчета	Информация
Тип данных	Уязвимость PenTest
Исходные данные	По скану
Состав описания уязвимостей	Название, Краткое описание, Как исправить, Ссылки
Достоверность результатов	Только высокая
Фильтр уязвимостей по уровню: включить	Уязвимость, серьезная уязвимость, критический уровень
Включить уязвимости, помеченные как ложное срабатывание	Нет
Разбивать отчет на части	Не разбивать отчет
Содержание отчета	Уязвимость узлов

Данные, включенные в отчет

задача	узлов	сканов
ЦА Пользователи все подсети	577	1
Итого:	577	1



Kaspersky Security Center

kaspersky

Отчет об уязвимостях

25 декабря 2025 г. 15:19:16

Отчет об обнаруженных уязвимостях ПО. Отчет формируется для всех групп.

Количество устройств:

- Устройств без уязвимостей: 477
- Устройств с уязвимостями средней критичности: 0
- Устройств с уязвимостями высокой критичности: 0
- Устройств с уязвимостями предельной критичности: 83

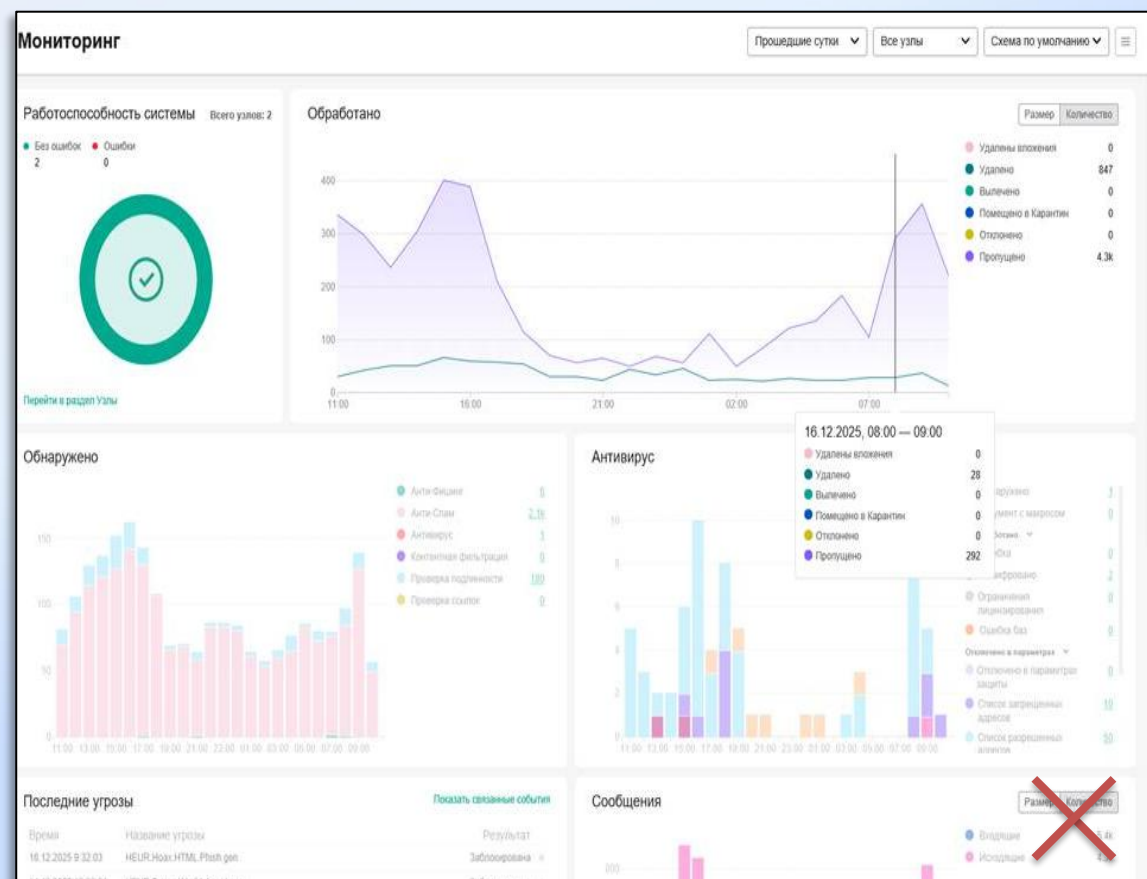
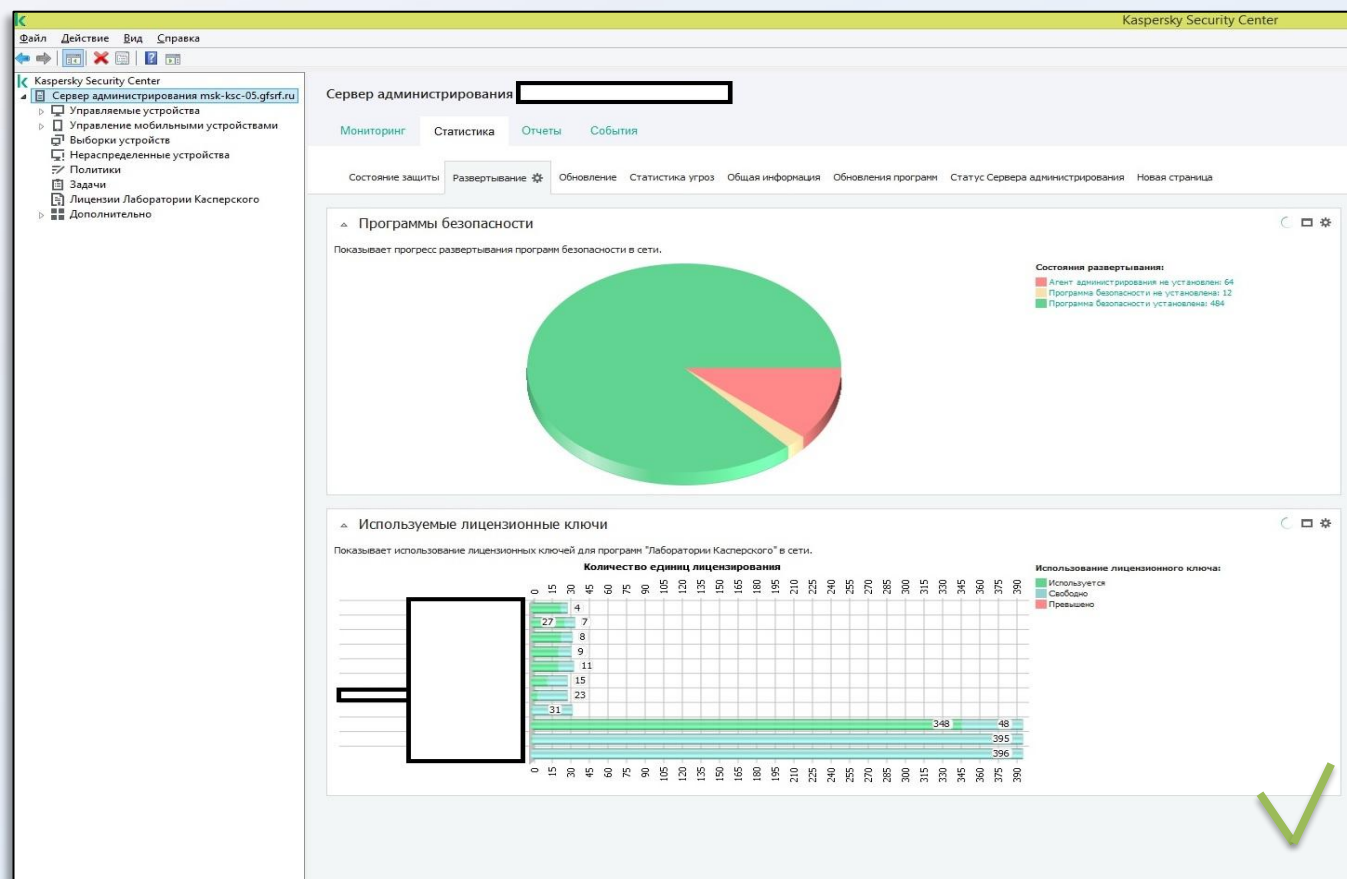
Сводная информация:

Уровень критичности	Уязвимость	Поставщик	Программа	Устройства	Группы
Критическое	KLA10473	Microsoft	Windows 7	1	1
Критическое	KLA10544	Microsoft	Office 2007	1	1
Критическое	KLA10544	Microsoft	Windows 7	5	2
Критическое	KLA10578	Microsoft	Office 2013	6	3
Критическое	KLA10580	Microsoft	Windows 7	14	3
Критическое	KLA10589	Microsoft	Windows 7	14	2
Критическое	KLA10600	Microsoft	Office 2013	51	4
Критическое	KLA10601	Microsoft	Windows 7	19	4
Критическое	KLA10603	Microsoft	Windows 7	9	1



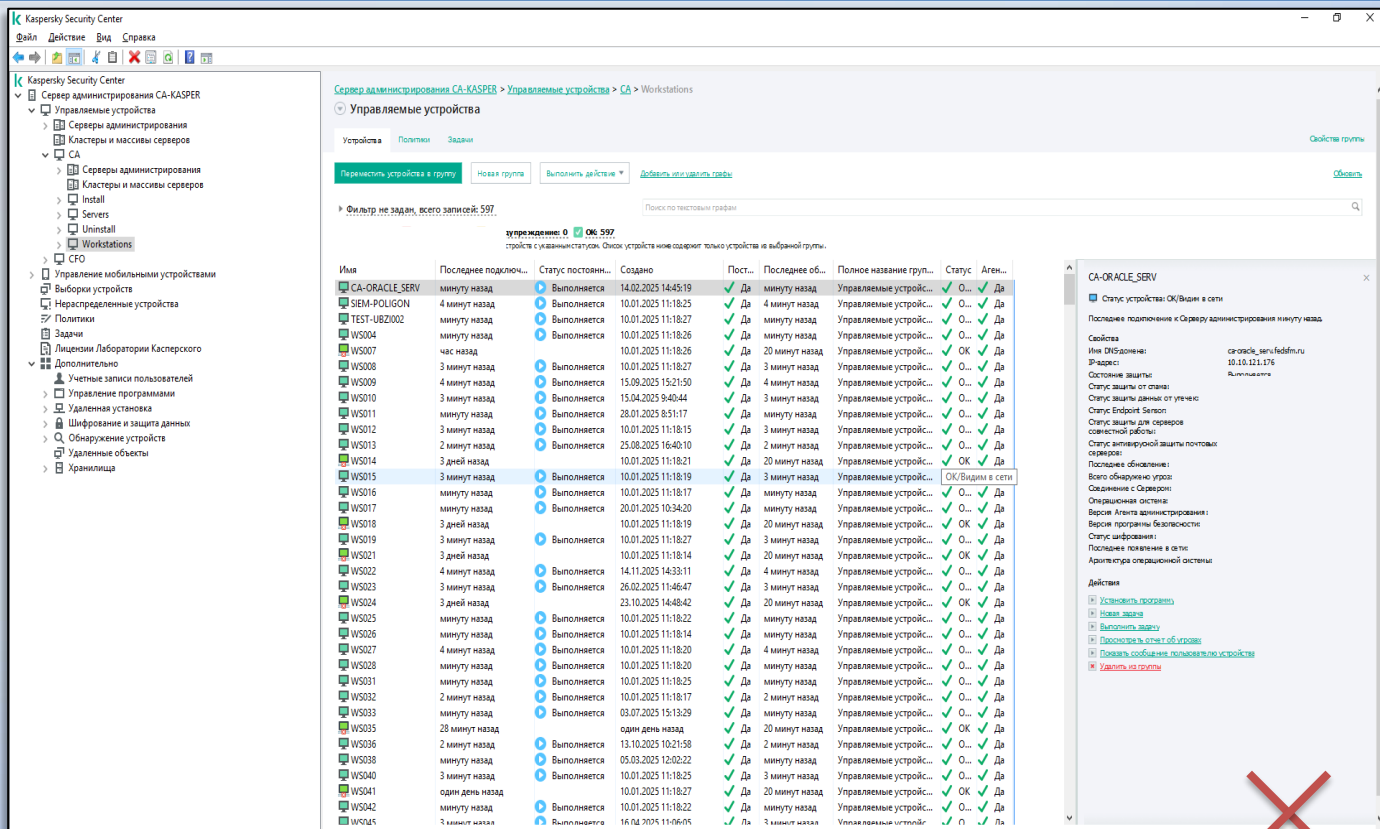
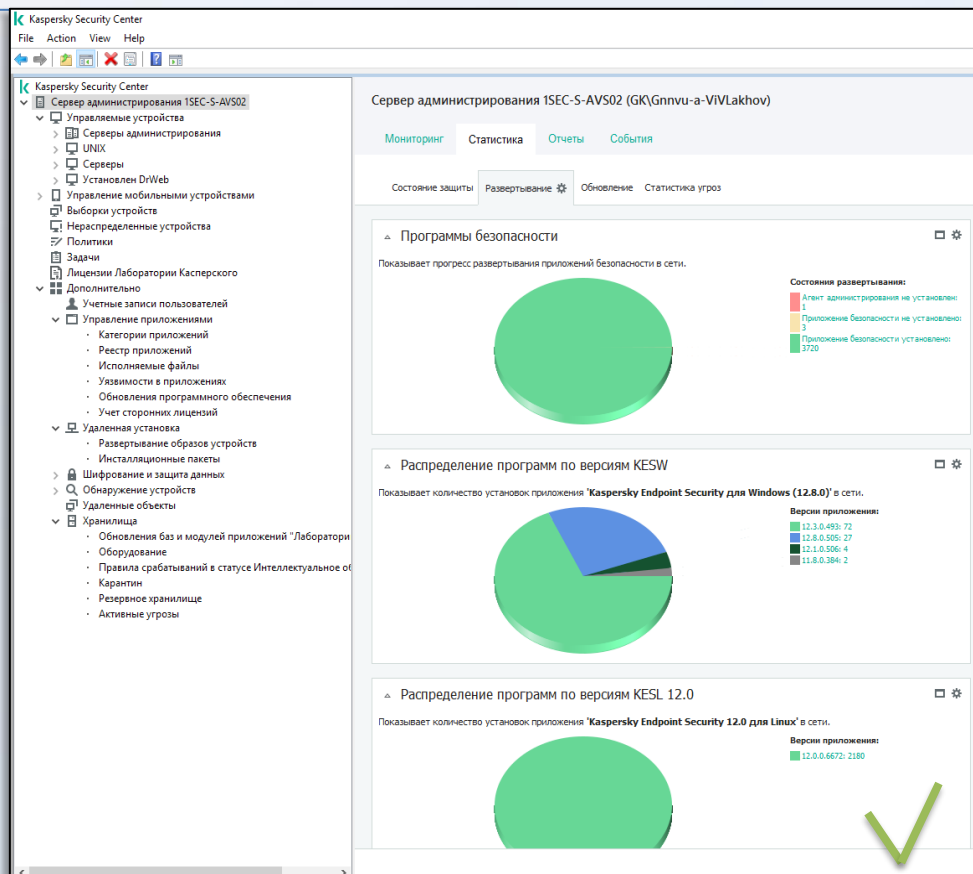
Частный показатель безопасности кз4 «Обеспечена проверка вложений в электронных письмах электронной почты на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств)»

С результатами оценки предоставляются сведения о применяемых средствах антивирусной защиты (снимок экрана панели управления средством).



Частный показатель безопасности k35 «Обеспечено централизованное управление средствами антивирусной защиты (не менее чем 80% пользовательских устройств и серверов контролируются средствами антивирусной защиты с централизованным управлением). При этом обеспечены контроль и установка обновлений баз данных признаков вредоносного программного обеспечения не реже чем 1 раз в месяц»

С результатами оценки предоставляется снимок экрана страницы настройки средства централизованного управления антивирусной защиты информации, отображающий количество автоматизированных рабочих мест, которые находятся под его управлением.



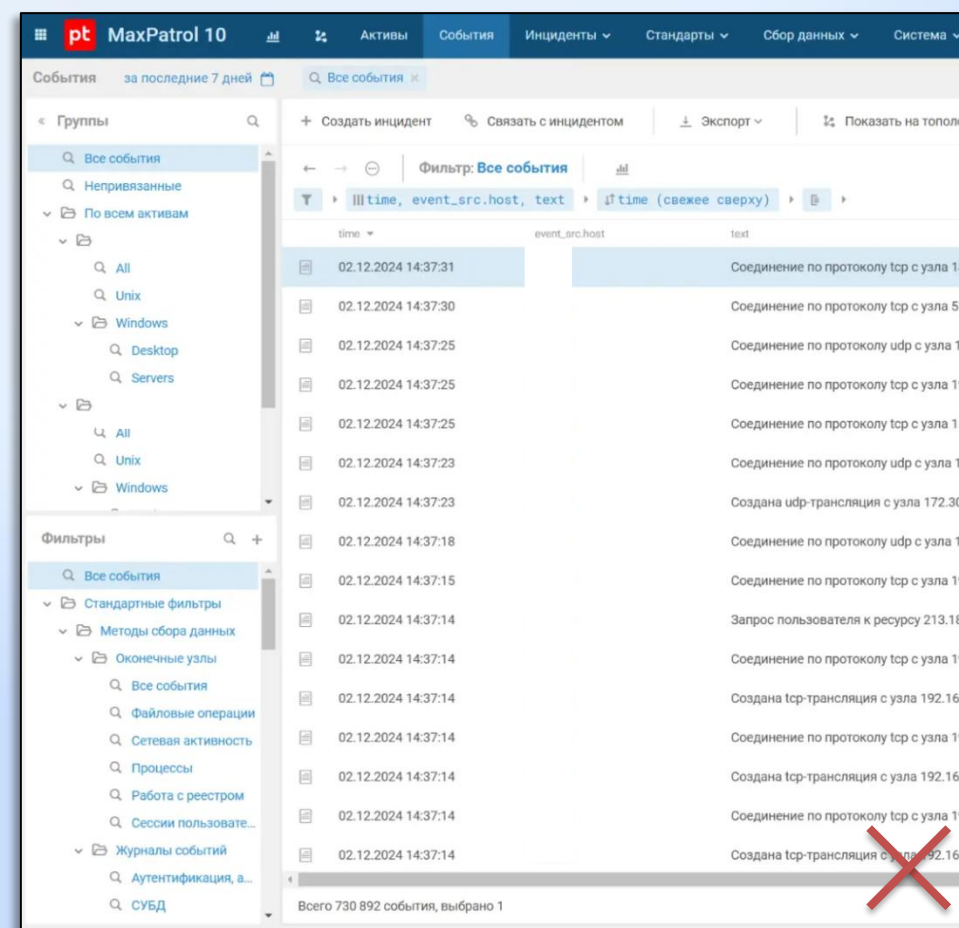
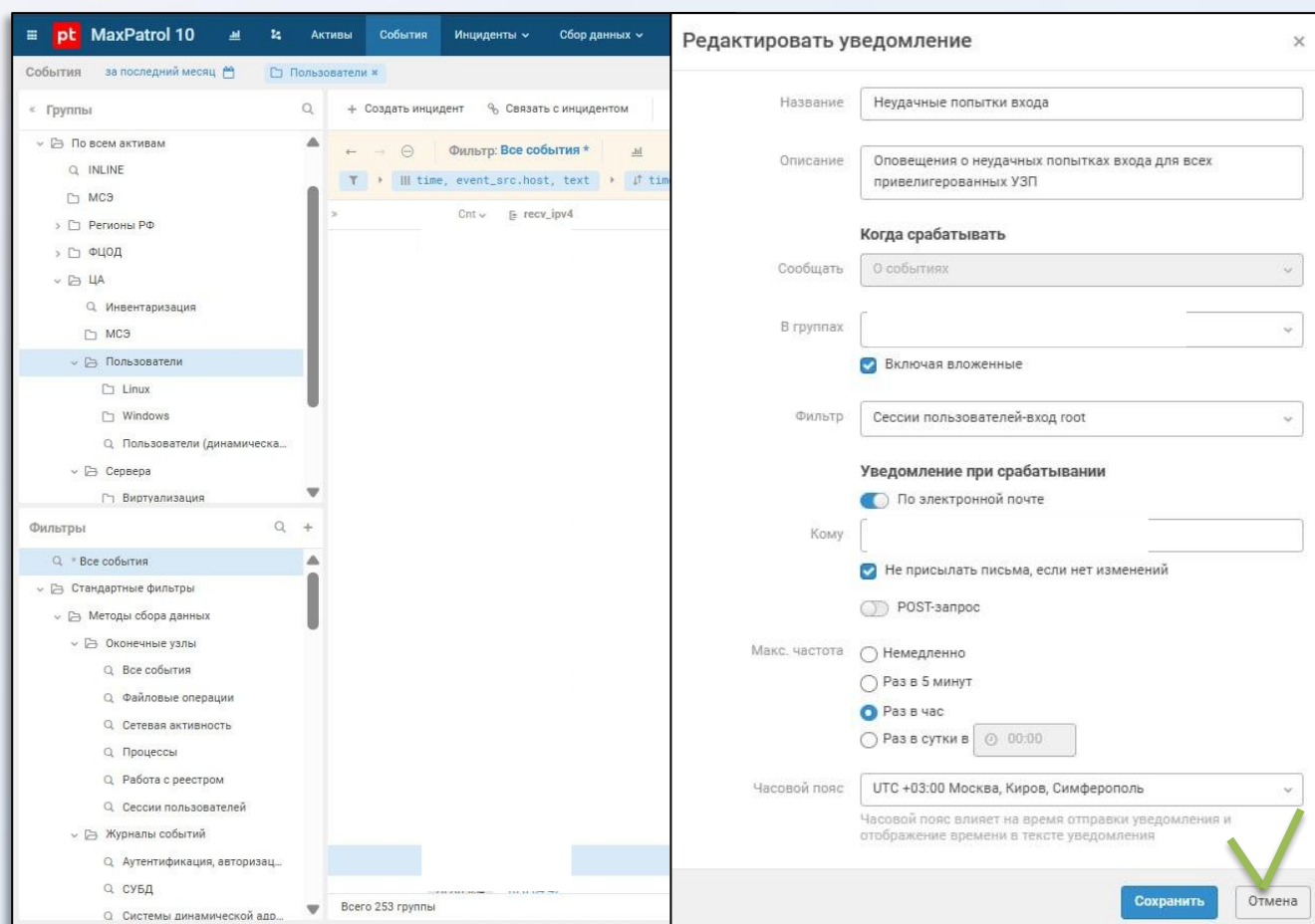
Частный показатель безопасности к36 «Реализована очистка входящего из сети Интернет сетевого трафика от компьютерных атак, направленных на отказ в обслуживании, на уровне L3/L4 (заключен договор с провайдером)»

С результатами оценки предоставляется копия договора (выписки) с оператором связи (иной организацией), в который включены работы по очистке входящего из сети «Интернет» трафика на уровне L3/L4.

СОГЛАШЕНИЕ № о взаимодействии г. Москва 17 апреля 2025 г.	Сетевая защита информационных ресурсов Заказчика от нераспределённых и распределённых атак мощностью до 5 Тбит/с со стороны Интернет типа «Отказ в обслуживании» на уровнях L3 и L4 модели OSI, способных повлечь за собой недоступность информационных ресурсов Заказчика для доступа к ним из Интернет легальных пользователей. Для обеспечения бесперебойной передачи данных Заказчика.
1. Общие положения 1. Соглашение заключено в соответствии со статьёй 65.1 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» и Правилами централизованного управления сетью связи общего пользования, утвержденными постановлением Правительства Российской Федерации от 12 февраля 2020 г. № 127, в целях организации взаимодействия Сторон по вопросам противодействия распределённым атакам, направленным на отказ в обслуживании (DDoS-атакам) (далее соответственно – взаимодействие, DDoS-атаки). 1.2. Предметом Соглашения является взаимодействие между Сторонами при осуществлении противодействия DDoS-атакам, направленное на их предупреждение, выявление и пресечение. 1.3. Взаимодействие Сторон осуществляется на безвозмездной основе и не влечет за собой возникновения каких-либо финансовых обязательств для Сторон. 2. Формы взаимодействия Сторон 2.1. Взаимодействие Сторон осуществляется в следующих формах: а) сбор, обработка и обмен информацией о DDoS-атаках; б) осуществление Владелемьм HСIА комплекса мероприятий, направленных на уменьшение количества нелегитимного трафика из информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») на оборудование Владелца сетевого ресурса (далее – защита от DDoS-атак); в) осуществление комплекса мероприятий, направленных на снижение количества DDoS-атак. 2.2. Объектом защиты является диапазон IP-адресов 2.3. Соглашение не препятствует Сторонам в определении и развитии любых взаимоприемлемых форм взаимодействия, предусмотренных дополнительными соглашениями к Соглашению.	В рамках подготовки защиты от DDoS-атак Исполнитель обеспечит: – создание и настройку политик обнаружения и блокирования атак, направленных на защищаемые IP-префиксы Заказчика, и исключение ложных срабатываний в отношении политик; – профилирование политик фильтрации трафика, поступающего на защищаемые IP-префиксы Заказчика, с использованием анализа параметров поступающих запросов; – предоставление Заказчику отдельного раздела защищённого портала Исполнителя в сети Интернет для индивидуального доступа Заказчика посредством веб-браузера в целях пользования сервисом защиты от DDoS-атак (личный кабинет сервиса защиты от DDoS-атак). Защита от DDoS-атак будет обеспечивать: – корректировку индивидуальных профилей защиты на основе результатов экспертного анализа сетевой активности: доработку существующих сценариев обнаружения атак для увеличения вероятности выявления подозрительных активностей и снижения количества ложных срабатываний; проактивную корректировку политики при выявлении нового актуального вектора атак; расширение списка контролируемых сценариев обнаружения атак в рамках внутренних исследований Исполнителя; реализацию новых сценариев обнаружения и блокирования атак по запросу Заказчика; – диагностику возникающих проблем в случае актуализации настроек при изменении IP-адресации защищаемых информационных ресурсов Заказчика; – контроль эффективности защиты путём отслеживания системных параметров, текущей нагрузки на систему защиты от DDoS-атак с целью своевременного реагирования на оповещения; – предоставление доступа в личный кабинет сервиса защиты от DDoS-атак с учётом следующих требований: возможность использования интерфейса на русском языке; предоставление статистики по текущим и прошедшим атакам (суммарный пропущенный и/или заблокированный трафик; распределение входящего трафика; распределение трафика по размеру пакетов; распределение трафика по параметрам протоколов IP, DNS, TCP, UDP, ICMP, SYN, но не ограничиваясь ими Для обеспечения бесперебойной передачи данных Заказчика.

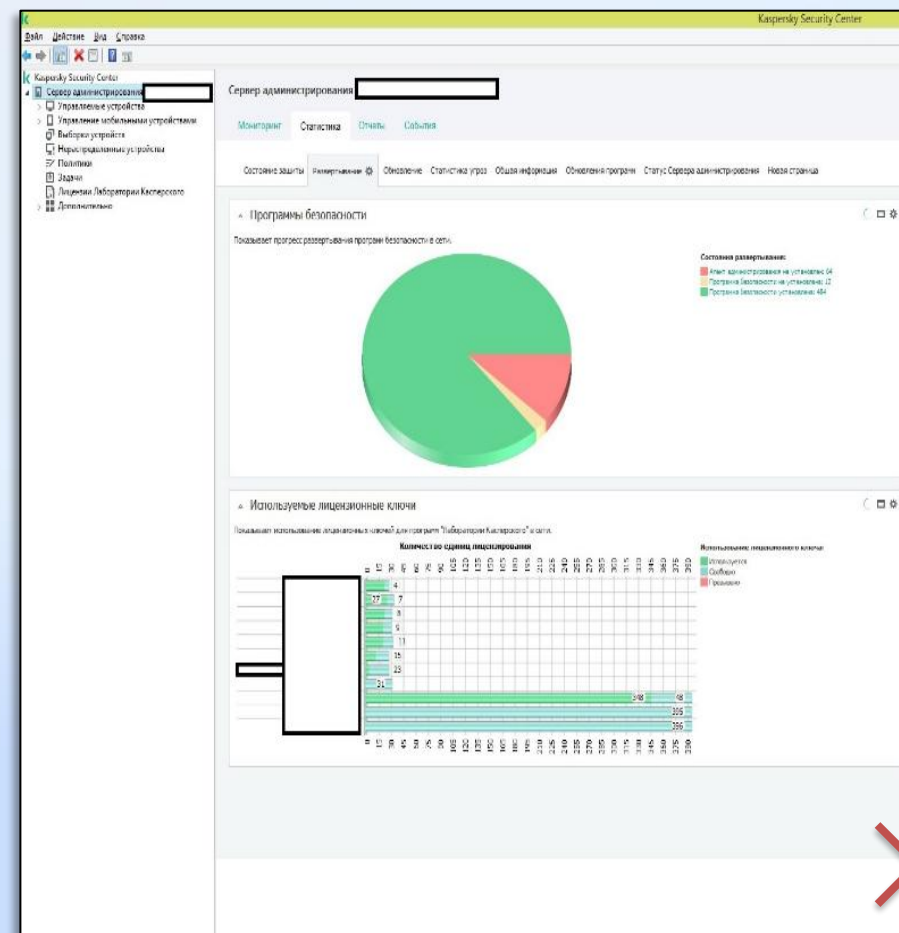
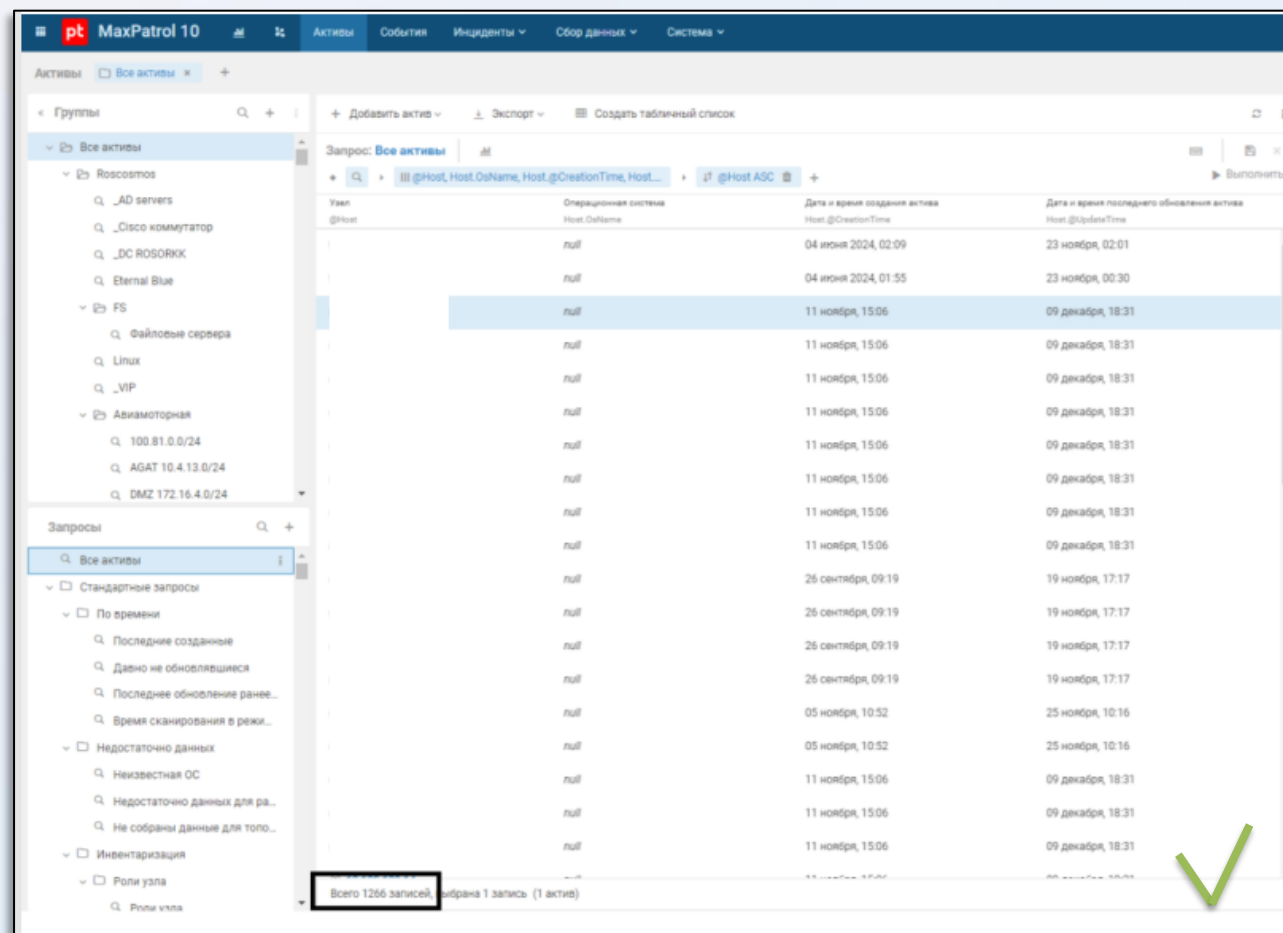
Частный показатель безопасности k41 «Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей»

С результатами оценки предоставляется снимок экрана с вкладки настроек системы (средства) мониторинга информационной безопасности, отображающий установленные настройки оповещения о неудачных попытках входа для всех привилегированных учетных записей.



Частный показатель безопасности k42 «Реализован централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с сетью Интернет»

С результатами оценки предоставляется снимок экрана с вкладки настроек системы (средства) мониторинга информационной безопасности, отображающий количество автоматизированных рабочих мест, с которых осуществляется централизованный сбор событий безопасности.



Спасибо за внимание!

