# О методическом подходе к оценке текущего состояния защиты информации в информационных системах и обеспечения безопасности объектов критической информационной инфраструктуры в органах государственной власти и организациях

**Жиров Павел Валентинович**

Начальник управления ФСТЭК России

# МОНИТОРИНГ ТЕКУЩЕГО СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

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

**Указ Президента Российской Федерации от 8 ноября 2023 г. № 846 «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»**

**Мониторинг текущего состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры**

**Показатель состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры**

**Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации, утвержденная ФСТЭК России 11 ноября 2025 г.**

# ЗАЩИТА ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ, ИНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ГОСУДАРСТВЕННЫХ УНИТАРНЫХ ПРЕДПРИЯТИЙ, ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ

**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»**

Проведение оценки показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации Кзи

32. Расчет и оценка показателя защищенности Кзи должны проводиться оператором (обладателем информации) **не реже одного раза в шесть месяцев.**

Представление результатов расчета показателя защищенности органами государственной власти и организациями **в 2026 году – август, декабрь**

# МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ТЕКУЩЕГО СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

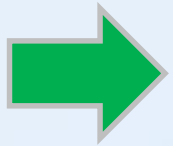
ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден
ФСТЭК России
2 мая 2024 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

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

2024



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

# МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ТЕКУЩЕГО СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ 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

## ЦЕЛЬ ПРИМЕНЕНИЯ:

Оценка степени достижения ОГВ и СКИИ минимально необходимого (базового) уровня защиты информации и обеспечения безопасности значимых объектов КИИ от актуальных угроз безопасности информации

## ОЦЕНИВАЕМЫЙ ПАРАМЕТР:

Показатель состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ ($К_{ЗИ}$ )

## ЭТАПЫ ОЦЕНКИ:

- ✓ Сбор и анализ исходных данных, необходимых для оценки
- ✓ Определение значений частных показателей безопасности
- ✓ Расчет показателя состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ и его сравнение с нормированным значением

# МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ТЕКУЩЕГО СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

| ГРУППА ПОКАЗАТЕЛЕЙ | ВЕСОВОЙ КОЭФФИЦИЕНТ | НАИМЕНОВАНИЕ ПОКАЗАТЕЛЯ | ЗНАЧЕНИЕ |
|---|---|---|---|
| **1. Организация и управление** | 0,10 | 1. На заместителя руководителя органа (организации) возложены полномочия ответственного лица за обеспечение информационной безопасности органа (организации) и определены его обязанности | 0,30 |
| | | 2. Определены функции (обязанности) структурного подразделения (или отдельных работников), ответственного за обеспечение информационной безопасности органа (организации) | 0,40 |
| | | 3. К подрядным организациям, имеющим доступ к информационным системам с привилегированными правами, в договорах установлены требования о реализации мер по защите от угроз через информационную инфраструктуру подрядчика | 0,30 |

# МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ТЕКУЩЕГО СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

| ГРУППА ПОКАЗАТЕЛЕЙ | ВЕСОВОЙ КОЭФФИЦИЕНТ | НАИМЕНОВАНИЕ ПОКАЗАТЕЛЯ | ЗНАЧЕНИЕ |
|---|---|---|---|
| **2. Защита пользователей** | 0,25 | 1. 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 | 0,30 |
| | | 2. Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор) | 0,30 |
| | | 3. Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию | 0,20 |
| | | 4. Отсутствуют активные учетные записи работников органа (организации) и работников, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения | 0,20 |

# МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ТЕКУЩЕГО СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

| ГРУППА ПОКАЗАТЕЛЕЙ | ВЕСОВОЙ КОЭФФИЦИЕНТ | НАИМЕНОВАНИЕ ПОКАЗАТЕЛЯ | ЗНАЧЕНИЕ |
|---|---|---|---|
| **3. Защита информационных систем** | 0,35 | 1. 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) | 0,20 |
| | | 2. 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 | 0,20 |
| | | 3. 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 | 0,10 |
| | | 4. Обеспечена проверка вложений в электронных письмах электронной почты на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств) | 0,10 |
| | | 5. 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 | 0,15 |
| | | 6. Реализована очистка входящего из сети Интернет сетевого трафика от компьютерных атак, направленных на отказ в обслуживании, на уровне L3/L4 (заключен договор с провайдером) | 0,15 |

# МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ТЕКУЩЕГО СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

| ГРУППА ПОКАЗАТЕЛЕЙ | ВЕСОВОЙ КОЭФФИЦИЕНТ | НАИМЕНОВАНИЕ ПОКАЗАТЕЛЯ | ЗНАЧЕНИЕ |
|---|---|---|---|
| **4. Мониторинг информационной безопасности и реагирование** | 0,30 | 1. Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей | 0,40 |
| | | 2. Реализован централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с сетью «Интернет» | 0,35 |
| | | 3. Утвержден документ, определяющий порядок реагирования на компьютерные инциденты | 0,25 |

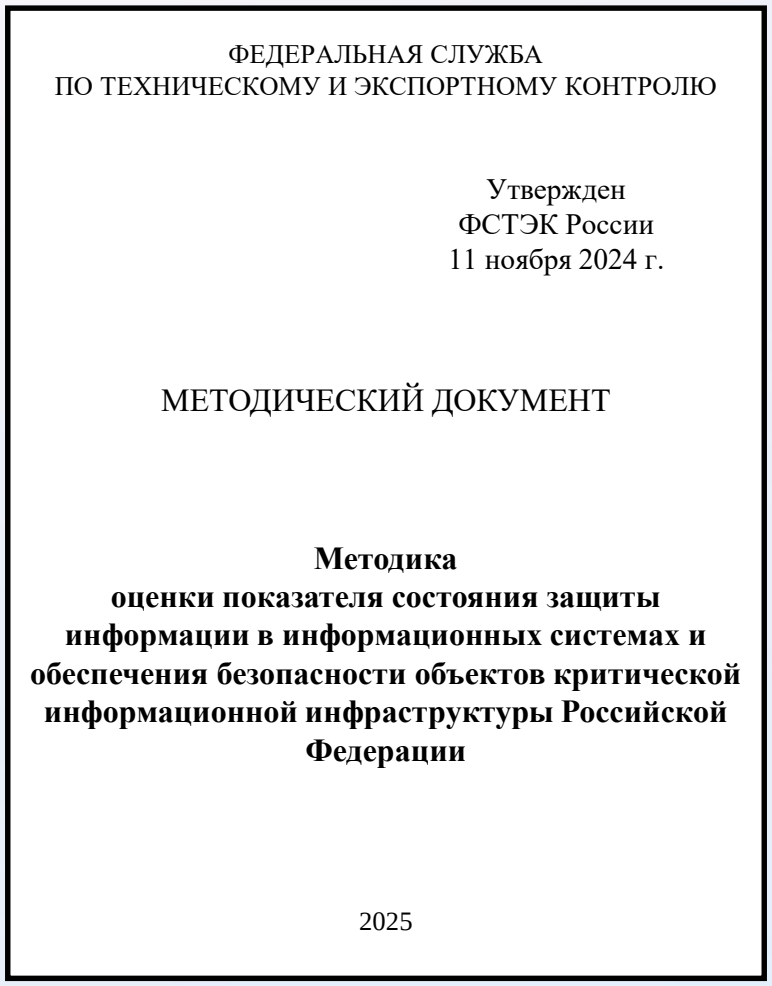
# РАСЧЕТ ПОКАЗАТЕЛЯ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ

$$К_{ИБ}=(k_{11}+ k_{21}+ \ldots k_{i1})*R_1+(k_{12}+ k_{22}+ \ldots k_{i2})*R_2+\ldots(k_{14}+ k_{24}+ \ldots k_{i4})*R_4$$

Где:
$R_j$ – весовой коэффициент группы частных показателей безопасности
$k_{ij}$ – значение частного показателя безопасности

| | |
|---|---|
| $К_{ИБ}=1$ | обеспечивается минимально необходимый уровень безопасности от актуальных угроз безопасности информации. Уровень обеспечения безопасности – минимальный базовый («зеленый») |
| $0,75<К_{ИБ}<1$ | минимально необходимый уровень безопасности от актуальных угроз безопасности информации не обеспечивается, имеются предпосылки реализации актуальных угроз безопасности информации. Уровень обеспечения безопасности – низкий («оранжевый») |
| $К_{ИБ}\leq 0,75$ | минимально необходимый уровень безопасности от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности информации. Уровень обеспечения безопасности – критический («красный») |

# ОЦЕНКА СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден
ФСТЭК России
11 ноября 2024 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

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

2025

**Недостатки**

- Отсутствие многофакторной аутентификации привилегированных пользователей
- Наличие не устраненных критических уязвимостей на периметре и внутри информационной инфраструктуры
- Наличие установленных по умолчанию паролей учетных записей привилегированных пользователей
- Отсутствие мониторинга событий безопасности и реагирования на них
- Непринятие мер по защите от распределенных атак, направленных на приведение систем в состояние «отказ в обслуживании»

Проведена оценка более **2000 органов государственной власти и организаций**

# ИЗМЕНЕНИЯ В МЕТОДИКЕ ОЦЕНКИ ТЕКУЩЕГО СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

Порядок расчета показателя текущего состояния защиты информации в информационных системах и обеспечения безопасности значимых объектов КИИ для множества информационных систем и объектов КИИ

Учет мероприятий по оценке защищенности информационной инфраструктуры (тестирования на проникновение, учений, тренировок в области защиты)

Перечень подтверждающих документов и материалов, на основании которых показателю присваивается полученное по результатам значение

Исключение частного показателя «Обеспечен документальный или автоматизированный учет пользовательских устройств, серверов и сетевых устройств (не менее 80% устройств и серверов учтено в документах (ведомостях, паспортах, эксплуатационной документации) или в автоматизированных системах (CMDB)»

# ИЗМЕНЕНИЯ В МЕТОДИКЕ ОЦЕНКИ ТЕКУЩЕГО СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

| *УСЛОВИЕ:* | *ГРУППА ЧАСТНЫХ ПОКАЗАТЕЛЕЙ:* | *ЗНАЧЕНИЕ:* |
|---|---|---|
| Получен первоначальный доступ к информационной системе с использованием учетных записей пользователей такой системы | 2. Защита пользователей | 0 |
| Первоначальный доступ к информационной системе получен с использованием уязвимостей программного и программно-аппаратного обеспечения | 3. Защита информационных систем | 0 |
| Подтверждена возможность реализации недопустимых событий | 2. Защита пользователей<br>3. Защита информационных систем | 0 |

# ДОКУМЕНТЫ И МАТЕРИАЛЫ, ПОДТВЕРЖДАЮЩИЕ РЕЗУЛЬТАТЫ РАСЧЕТА ЗНАЧЕНИЙ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ, КОТОРЫЕ ПРЕДСТАВЛЯЮТСЯ В ФСТЭК РОССИИ ПО ЗАПРОСУ

| № п/п | Документы и материалы |
|---|---|
| 1 | Утвержденный руководителем или иным уполномоченным лицом органа (организации) приказ (распоряжение) или иной ОРД о назначении одного из заместителей руководителя ответственным за организацию работ по ИБ органа (организации) |
| 2 | Должностной регламент (инструкция) или иной документ, определяющий должностные обязанности (трудовые функции) по обеспечению ИБ органа (организации) заместителя руководителя органа (организации), ответственного за организацию работ по ИБ |
| 3 | Утвержденное руководителем или иным уполномоченным лицом органа (организации) положение (иной ОРД) о структурном подразделении по обеспечению ИБ или о возложении обязанностей по обеспечению ИБ органа (организации) на отдельных работников, содержащее обязанности (трудовые функции) по обеспечению ИБ структурного подразделения или отдельных работников органа (организации) |
| 4 | Договор, на основании которого привлекаемые подрядные организации (при их наличии) имеют доступ к информационным системам органа (организации), содержащий требования по реализации в инфраструктуре подрядчика мер по защите информации |
| 5 | Утвержденный руководителем или иным уполномоченным лицом органа (организации) ОРД, определяющий парольную политику органа (организации) |
| 6 | Сведения о количестве привилегированных пользователей (которые осуществляют удаленное подключение) информационной системы органа (организации), а также о количестве привилегированных пользователей, в отношении которых реализована многофакторная аутентификация |
| 7 | Утвержденный руководителем или иным уполномоченным лицом органа (организации) ОРД, содержащий требования о необходимости удаления учетных записей работников органа (организации) и работников, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения |
| 8 | Сведения о количестве пользовательских устройств и серверов, а также перечень интерфейсов (IP-адреса, доменные имена, физические интерфейсы (порты)), доступных из сети «Интернет» |
| 9 | Перечень реализованных компенсирующих мер, в случае отсутствия технической возможности устранения уязвимостей уровня «критический», и материалы, подтверждающие их реализацию |
| 10 | Отчет, сформированный средством антивирусной защиты, используемом для защиты электронной почты, содержащий сведения о количестве устройств, на которых функционируют средства антивирусной защиты, обеспечивающие проверку вложений в электронных письмах электронной почты на наличие вредоносного программного обеспечения |
| 11 | Отчет, сформированный средством централизованного управления антивирусной защиты информации |
| 12 | Перечень событий ИБ, в отношении которых осуществляется сбор информации |
| 13 | Отчет, сформированный системой (средством) мониторинга ИБ, содержащий сведения о зарегистрированных ранее событиях ИБ |
| 14 | Утвержденный руководителем или иным уполномоченным лицом органа (организации) ОРД, определяющий порядок реагирования на компьютерные инциденты |

# ДОКУМЕНТЫ И МАТЕРИАЛЫ, ПОДТВЕРЖДАЮЩИЕ РЕЗУЛЬТАТЫ РАСЧЕТА ЗНАЧЕНИЙ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ, КОТОРЫЕ ПРЕДСТАВЛЯЮТСЯ В ФСТЭК РОССИИ С РЕЗУЛЬТАТАМИ ОЦЕНКИ

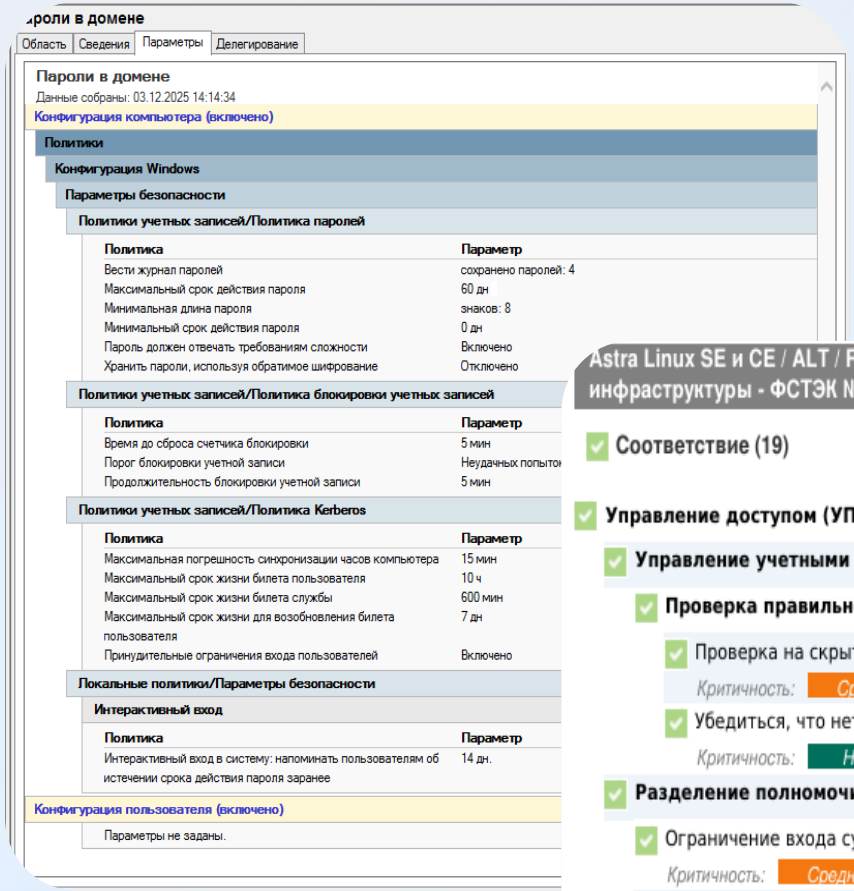
| № п/п | Документы и материалы |
|---|---|
| 1 | Снимок экрана, отображающий установленные на средстве реализации парольной политики настройки для паролей учетных записей пользователей информационных систем органа (организации), подтверждающий соответствие настроек паролей учетных записей пользователей информационных систем органа (организации) парольной политике |
| 2 | Отчет, сформированный средством анализа защищенности или иным инструментальным средством, позволяющим выявить пароли, не соответствующие установленным требованиям |
| 3 | Сведения о программном, программно-аппаратном средстве (снимок экрана панели управления средства), с использованием которого осуществляется многофакторная аутентификация привилегированных пользователей органа (организации) |
| 4 | 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 |
| 5 | Отчет, сформированный средством анализа защищенности или иным инструментальным средством, позволяющим выявить установленные по умолчанию пароли учетных записей пользователей |
| 6 | 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» |
| 7 | 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), а также результаты сканирования пользовательских устройств и серверов органа (организации) на наличие уязвимостей уровня «критический» |
| 8 | Сведения о применяемых средствах антивирусной защиты (снимок экрана панели управлении средством) |
| 9 | Снимок экрана страницы настройки средства централизованного управления антивирусной защиты информации, отображающий количество автоматизированных рабочих мест, которые находятся под его управлением |
| 10 | Копия договора (выписки) с оператором связи (иной организацией), в который включены работы по очистке входящего из сети «Интернет» трафика на уровне L3/L4 |
| 11 | Снимок экрана с вкладки настроек системы (средства) мониторинга информационной безопасности, отображающий установленные настройки оповещения о неудачных попытках входа для всех привилегированных учетных записей |
| 12 | Снимок экрана с вкладки настроек системы (средства) мониторинга информационной безопасности, отображающий количество автоматизированных рабочих мест, с которых осуществляется централизованный сбор событий безопасности |

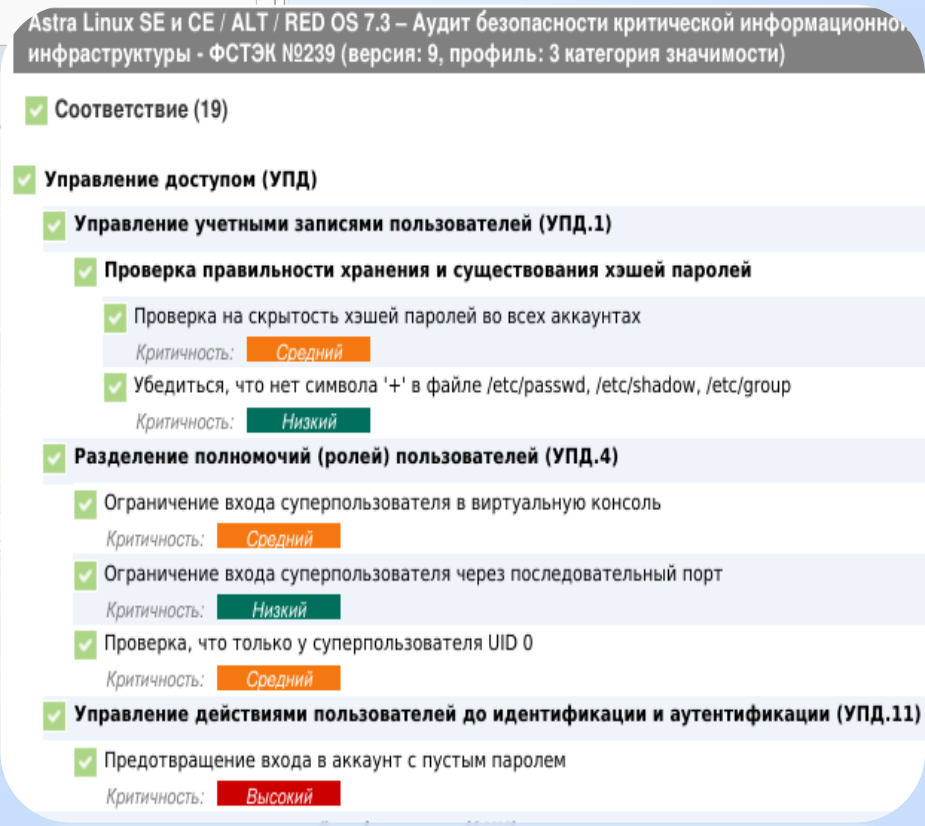
# Частный показатель безопасности k21 «Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике. В случае отсутствия технической возможности обеспечения требуемой сложности паролей реализованы компенсирующие меры»

С результатами оценки предоставляются следующие подтверждающие документы и материалы:

- ✓ 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;
- ✓ 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).

*В случае отсутствия технической возможности выполнения требований к паролям подтверждающим документом является перечень реализованных в информационной системе компенсирующих мер, и материалы, подтверждающие их реализацию.*

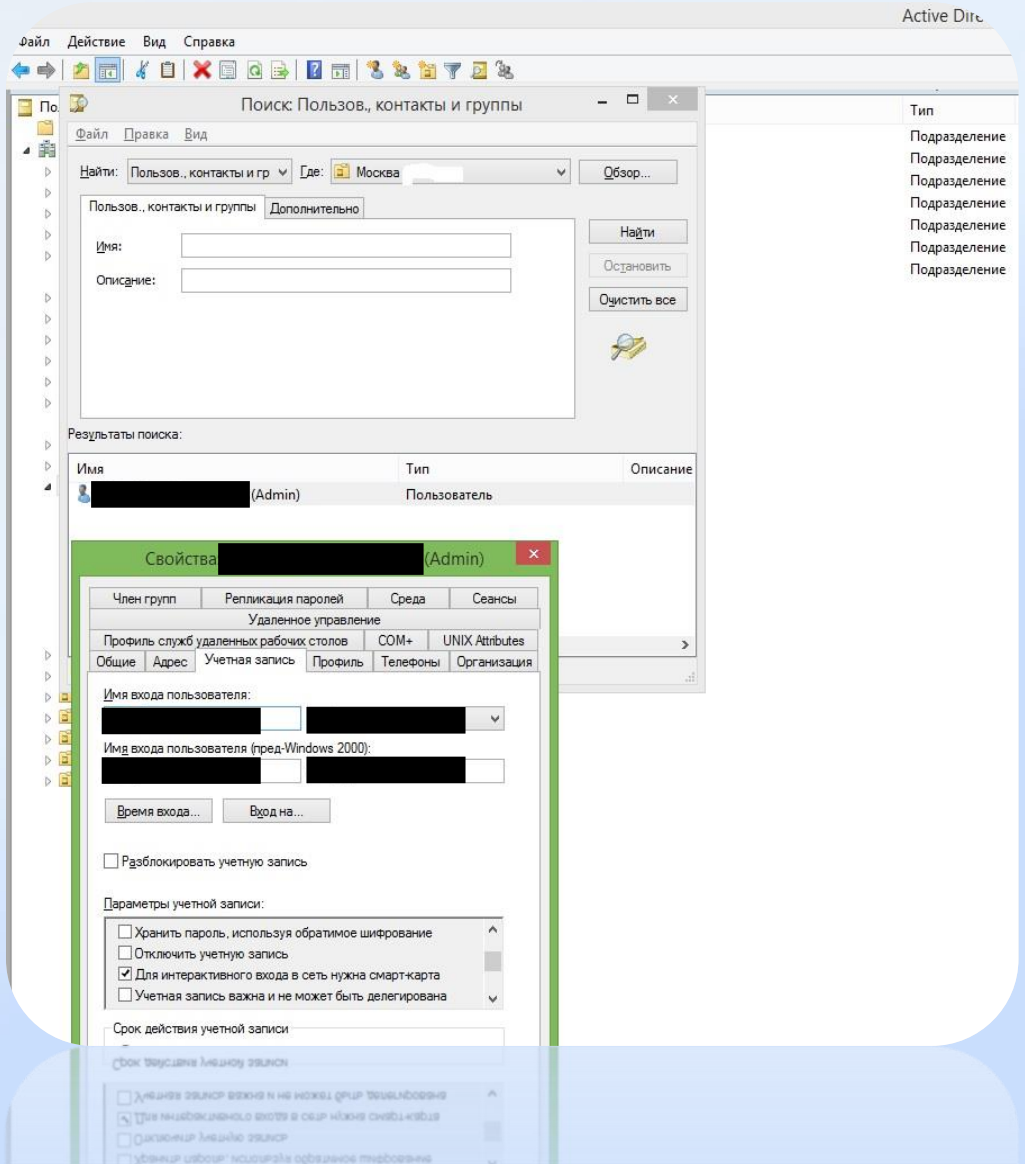


# Частный показатель безопасности k22 «Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)»

С результатами оценки предоставляются следующие подтверждающие документы и материалы:

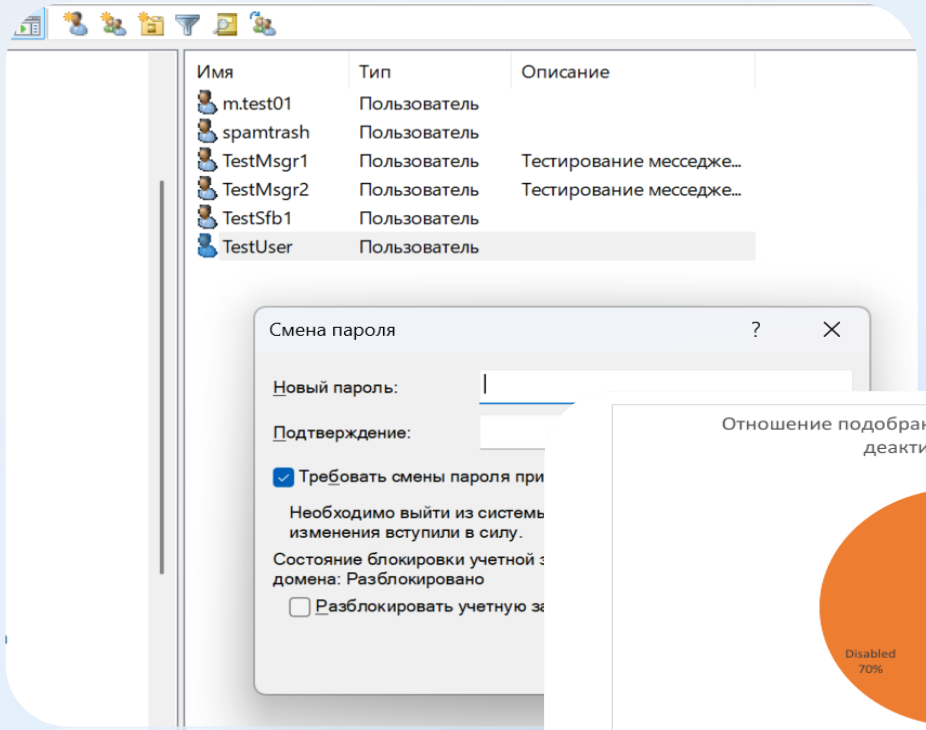
- ✓ сведения о программном, программно-аппаратном средстве (снимок экрана панели управления средства), с использованием которого осуществляется многофакторная аутентификация привилегированных пользователей органа (организации).

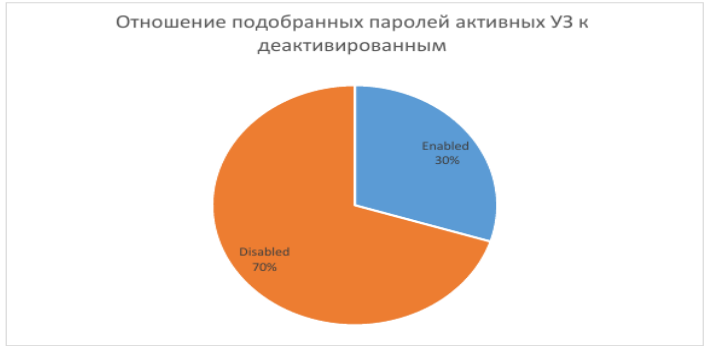


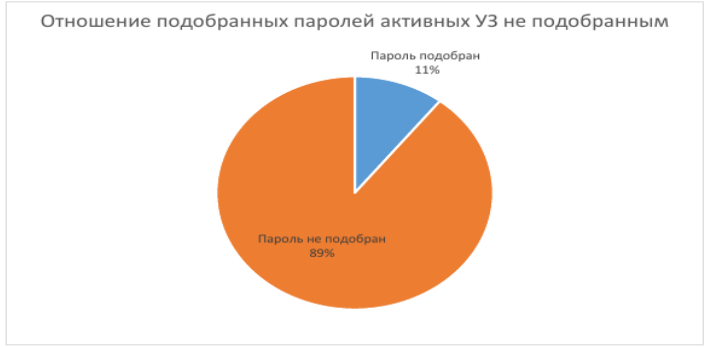
# Частный показатель безопасности k23 «Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию»

С результатами оценки предоставляются следующие подтверждающие документы и материалы:

- ✓ 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;
- ✓ 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).




Из общего числа подобранных паролей, уникальными являются 71 214 штук. Уникальные подобранные пароли добавлены в запрещающие списки Active Directory.

# Частный показатель безопасности $k_{31}$ «На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет7, контролируется межсетевыми экранами уровня L3/L4)»

С результатами оценки предоставляются следующие подтверждающие документы и материалы:

- ✓ 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».

*В случае отсутствия в информационной системе сервисов (служб) доступных из сети «Интернет» (отсутствие взаимодействия с сетью «Интернет») подтверждающим документом являются сведения об их отсутствии.*

| | | | | | | |
|---|---|---|---|---|---|---|
| BLM | BADSITE<br>BADSITE_EOSDO<br>HACK_SOFT_MARKE... | Любой | Любой | Любое | Отбросить | Не задан |
| BLM2 | Любой | BADSITE<br>BADSITE_EOSDO | Любой | Любое | Отбросить | Не задан |
| MARKERS_LOG | Любой | HACK_SOFT_MARKE... | Любой | Любое | Отбросить | Не задан |
| Net_Devices | Любой | Net_Devices_Real_IP | Любой | Любое | Отбросить | Не задан |

Сведения о применяемых средствах межсетевого экранирования

| Наименование ПАК | Версия ПО | Кол-во |
|---|---|---|
| Континент 4 HSEC-4-IPC-R3000-FW-SP1Y | 4.2.1 | 2 |
| Континент 4 HSEC-4-IPC-R3000-FW-SP1Y | 4.2.1 | 2 |
| Континент 4 HSEC-4-IPC-R3000-FW-SP1Y | 4.1.9, 4.2.1 | 6 |
| ViPNet Coordinator HW1000[2] | 4.0 | 2 |
| Континент 4 HSEC-4-IPC-R3000-FW-SP1Y | 4.1.9, 4.2.1 | 6 |
| ViPNet Coordinator HW1000[2] | 4.0 | 2 |

**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»**

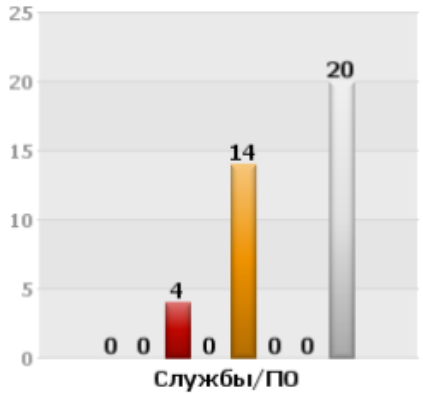
С результатами оценки предоставляются следующие подтверждающие документы и материалы:

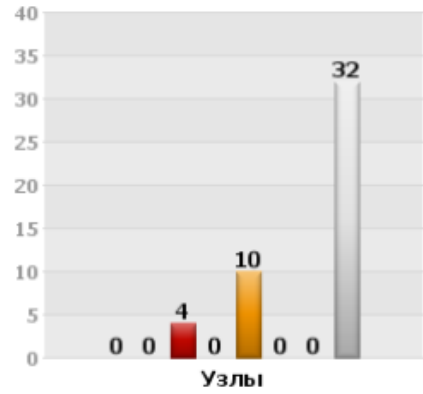
- ✓ отчет, сформированный средством анализа защищенности, содержащий результаты сканирования устройств и интерфейсов, доступных из сети «Интернет», на наличие уязвимостей уровня «критический» (с датой сканирования не ранее 30 дней даты проведения оценки).

**Данные, включенные в отчет**

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

**Уязвимость объектов**



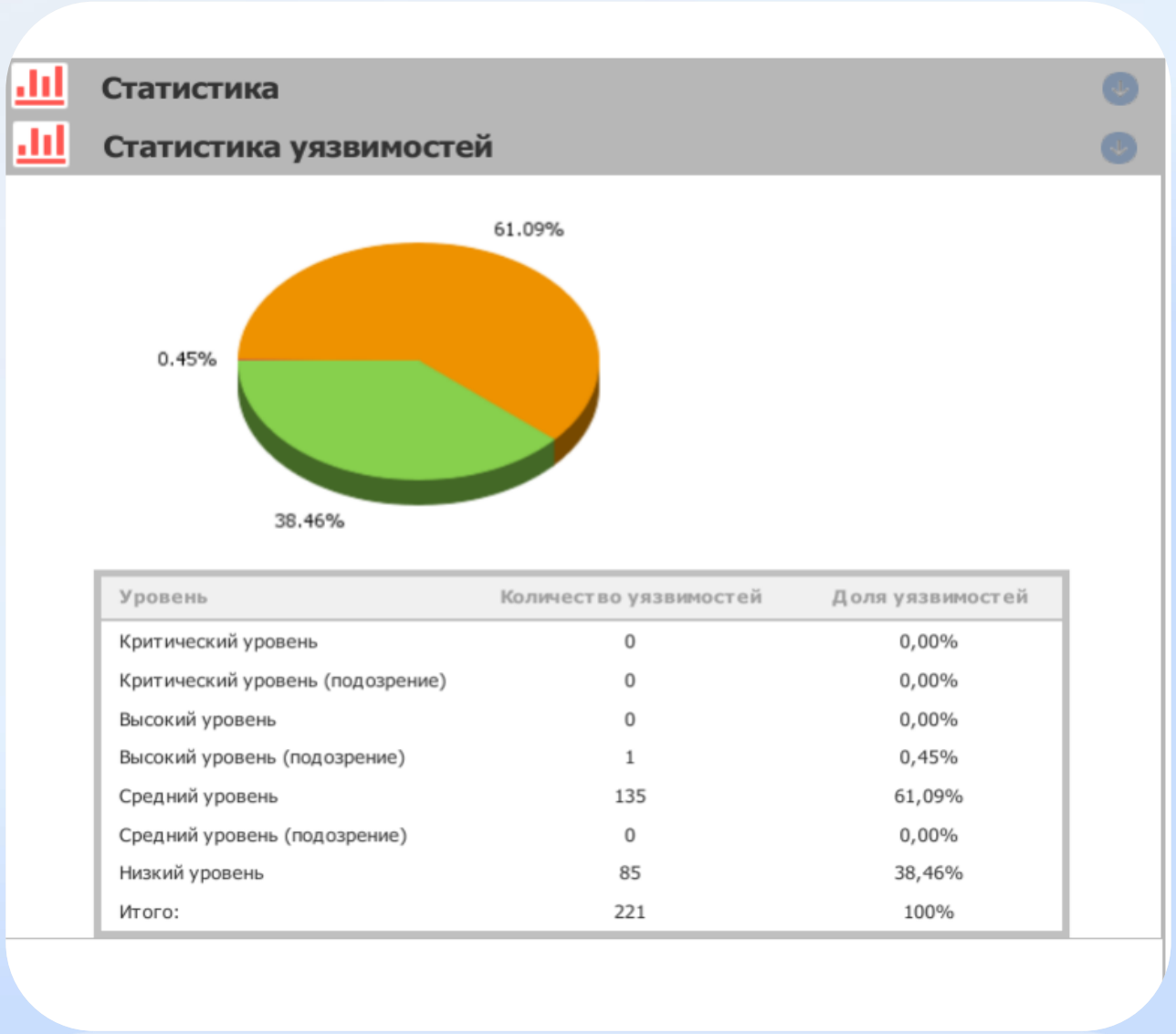




| Уровень | Службы/ПО | Узлы |
|---|---|---|
| Критический уровень | 0 | 0 |
| Критический уровень (подозрение) | 0 | 0 |
| Высокий уровень | 4 | 4 |
| Высокий уровень (подозрение) | 0 | 0 |
| Средний уровень | 14 | 10 |
| Средний уровень (подозрение) | 0 | 0 |
| Низкий уровень | 0 | 0 |
| нет уязвимостей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

**Частный показатель безопасности kзз «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 предоставляются следующие подтверждающие документы и материалы:

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

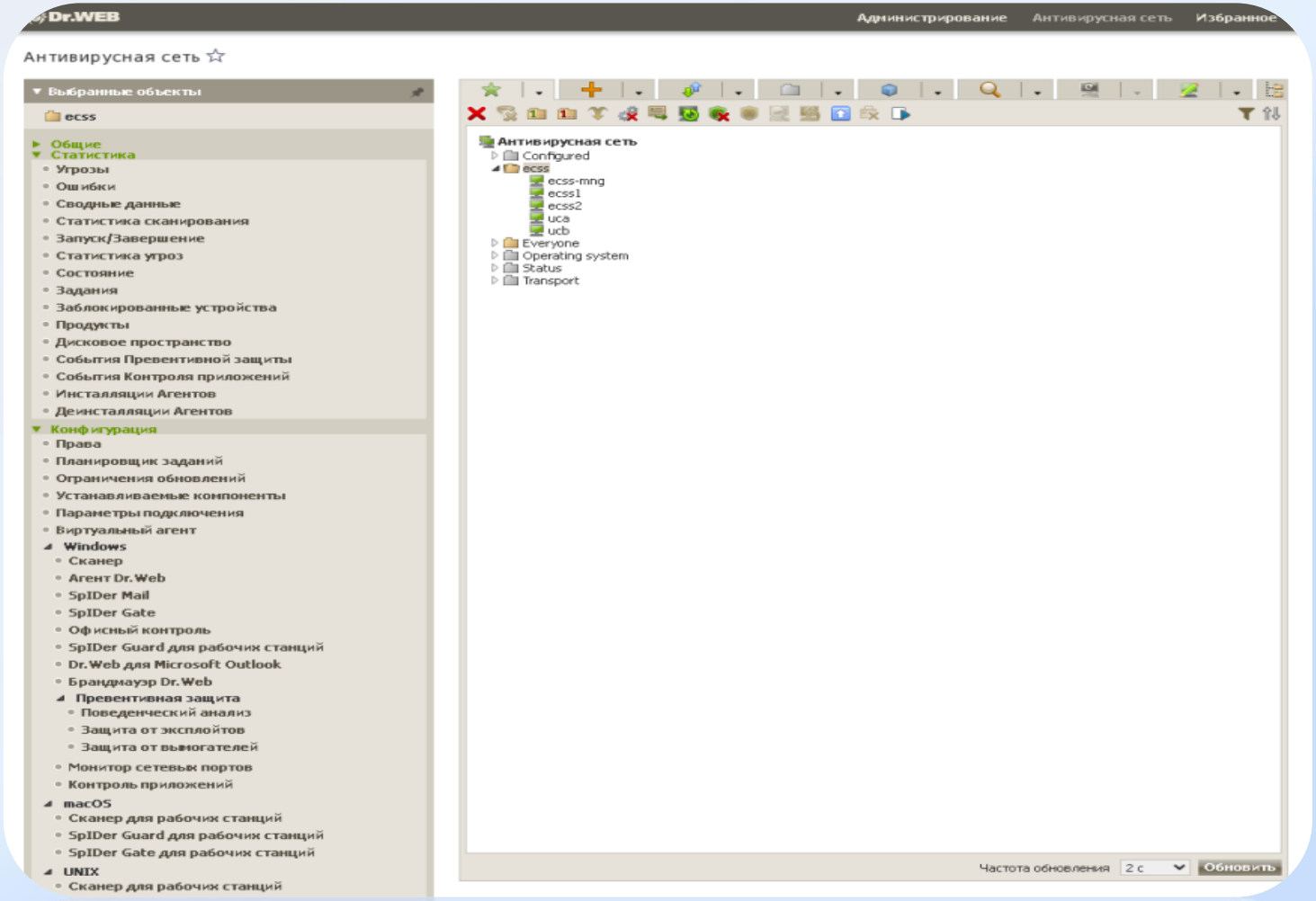



| Уровень | Количество уязвимостей | Доля уязвимостей |
|---|---|---|
| Критический уровень | 0 | 0,00% |
| Критический уровень (подозрение) | 0 | 0,00% |
| Высокий уровень | 0 | 0,00% |
| Высокий уровень (подозрение) | 1 | 0,45% |
| Средний уровень | 135 | 61,09% |
| Средний уровень (подозрение) | 0 | 0,00% |
| Низкий уровень | 85 | 38,46% |
| Итого: | 221 | 100% |

# Частный показатель безопасности k34 «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 следующие подтверждающие документы и материалы:

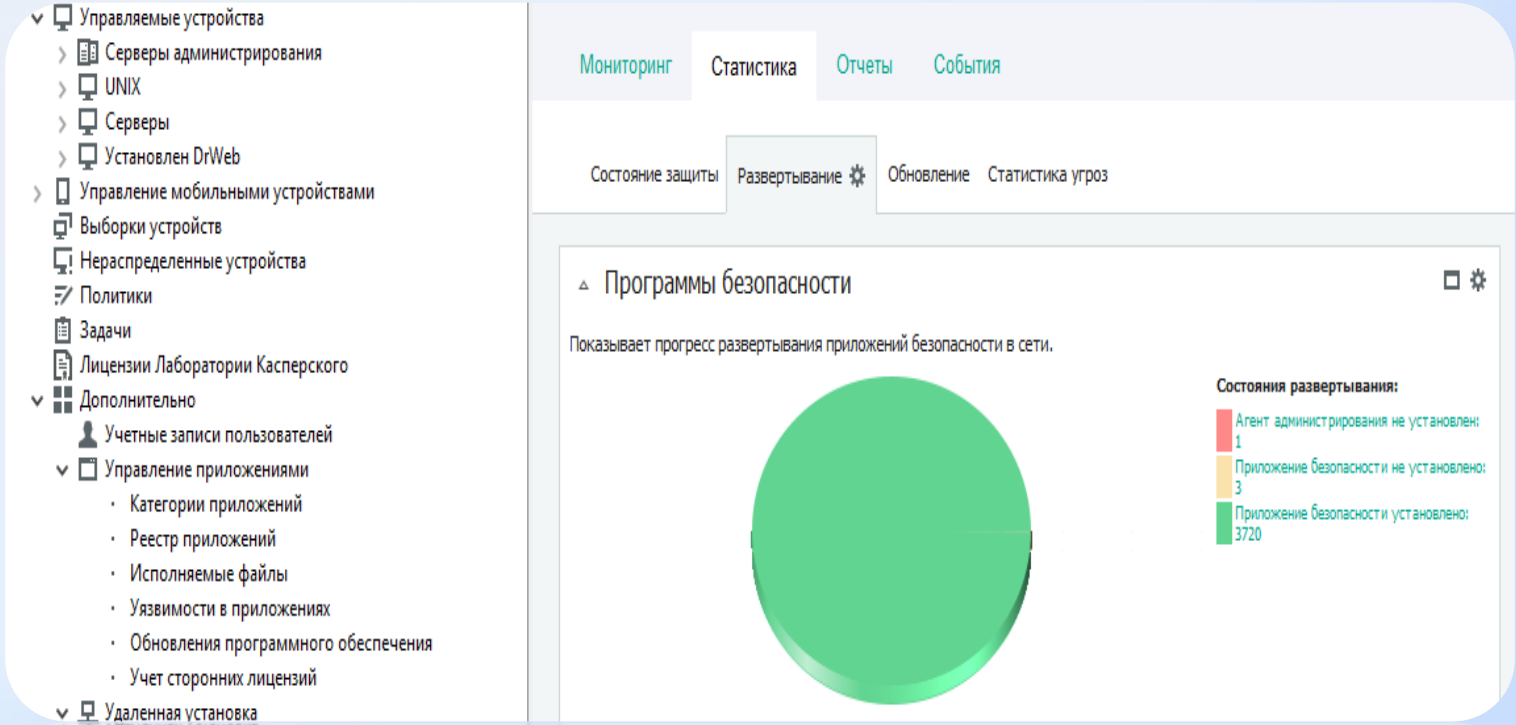
- ✓ сведения о применяемых средствах антивирусной защиты (снимок экрана панели управлении средством).



**Частный показатель безопасности $k_{35}$ «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 предоставляются следующие подтверждающие документы и материалы:

- ✓ снимок экрана страницы настройки средства централизованного управления антивирусной защиты информации, отображающий количество автоматизированных рабочих мест, которые находятся под его управлением.



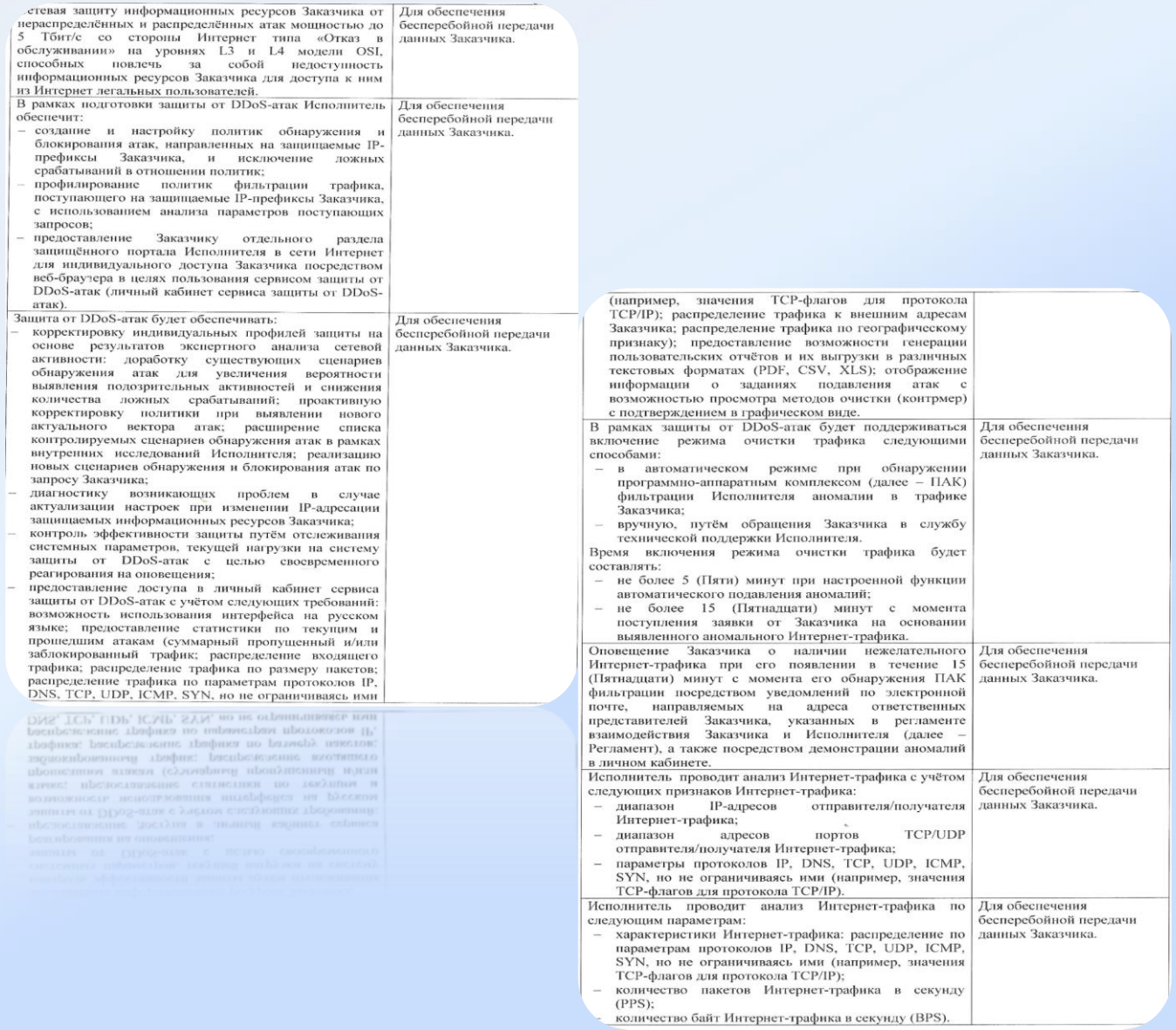
# Частный показатель безопасности $k_{36}$ «Реализована очистка входящего из сети Интернет сетевого трафика от компьютерных атак, направленных на отказ в обслуживании, на уровне L3/L4 (заключен договор с провайдером)»

С результатами оценки предоставляются следующие подтверждающие документы и материалы:

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

*В случае самостоятельной блокировки органом (организацией) входящего сетевого трафика подтверждающим документом являются сведения о применяемых в органе (организации) методах и средствах защиты от атак типа «отказ в обслуживании».*

*В случае отсутствия веб-сайтов, служб или иных сервисов, доступных из сети «Интернет» и подлежащих защите подтверждающим документом являются сведения, предусмотренные для показателя k31.*

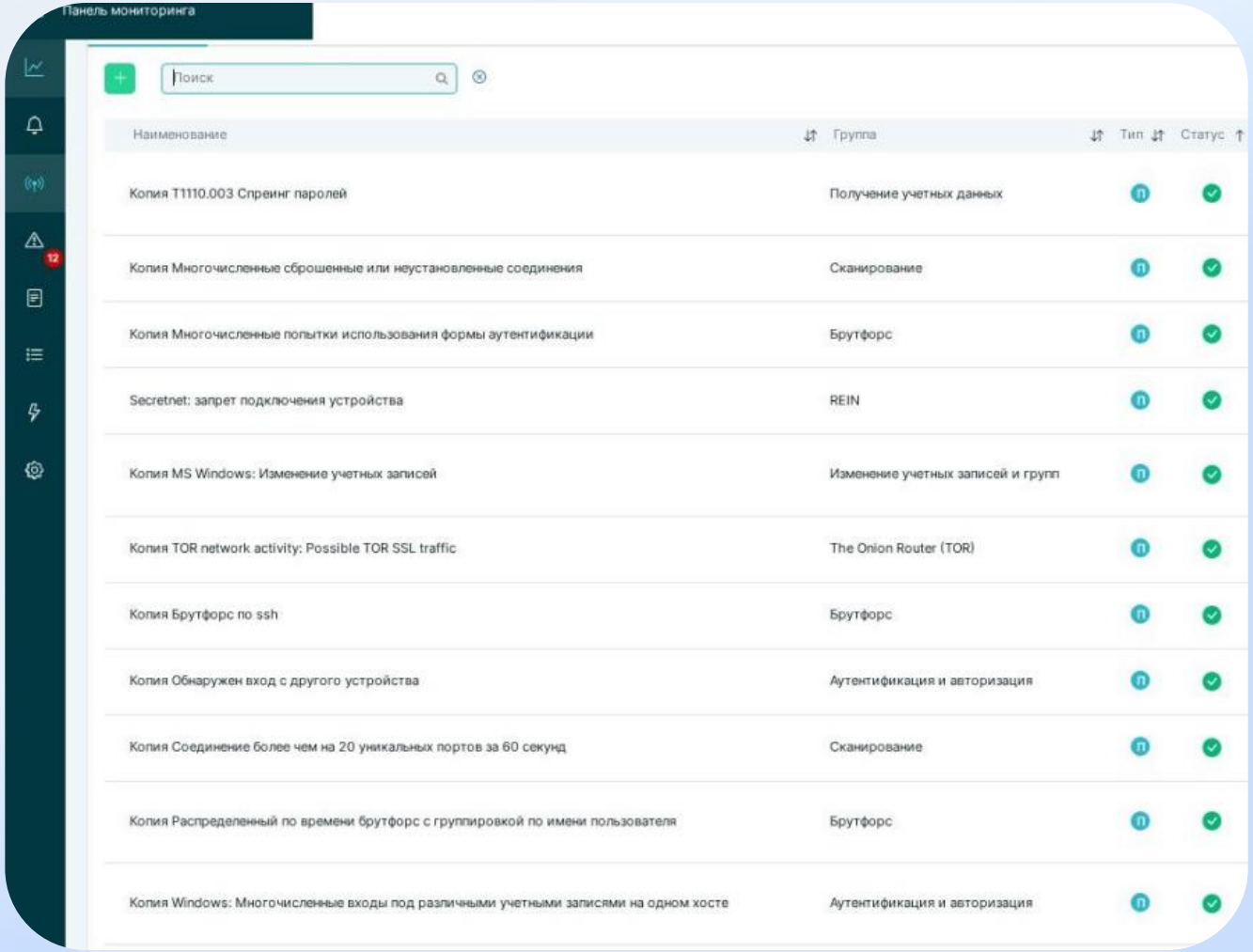


| | |
|---|---|
| сетевая защиту информационных ресурсов Заказчика от нераспределённых и распределённых атак мощностью до 5 Тбит/с со стороны Интернет типа «Отказ в обслуживании» на уровнях L3 и L4 модели OSI, способных повлечь за собой недоступность информационных ресурсов Заказчика для доступа к ним из Интернет легальных пользователей. | Для обеспечения бесперебойной передачи данных Заказчика. |
| В рамках подготовки защиты от DDoS-атак Исполнитель обеспечит:<br>– создание и настройку политик обнаружения и блокирования атак, направленных на защищаемые IP-префиксы Заказчика, и исключение ложных срабатываний в отношении политик;<br>– профилирование политик фильтрации трафика, поступающего на защищаемые IP-префиксы Заказчика, с использованием анализа параметров поступающих запросов;<br>– 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). | Для обеспечения бесперебойной передачи данных Заказчика. |
| Защита от DDoS-атак будет обеспечивать:<br>– 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;<br>– диагностику возникающих проблем в случае актуализации настроек при изменении IP-адресации защищаемых информационных ресурсов Заказчика;<br>– контроль эффективности защиты путём отслеживания системных параметров, текущей нагрузки на систему защиты от DDoS-атак с целью своевременного реагирования на оповещения;<br>– 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. |
| (например, значения TCP-флагов для протокола TCP/IP); распределение трафика к внешним адресам Заказчика; распределение трафика по географическому признаку); предоставление возможности генерации пользовательских отчётов и их выгрузки в различных текстовых форматах (PDF, CSV, XLS); отображение информации о заданиях подавления атак с возможностью просмотра методов очистки (контрмер) с подтверждением в графическом виде. | |
| В рамках защиты от DDoS-атак будет поддерживаться включение режима очистки трафика следующими способами:<br>– в автоматическом режиме при обнаружении программно-аппаратным комплексом (далее – ПАК) фильтрации Исполнителя аномалии в трафике Заказчика;<br>– вручную, путём обращения Заказчика в службу технической поддержки Исполнителя.<br>Время включения режима очистки трафика будет составлять:<br>– не более 5 (Пяти) минут при настроенной функции автоматического подавления аномалий;<br>– не более 15 (Пятнадцати) минут с момента поступления заявки от Заказчика на основании выявленного аномального Интернет-трафика. | Для обеспечения бесперебойной передачи данных Заказчика. |
| Оповещение Заказчика о наличии нежелательного Интернет-трафика при его появлении в течение 15 (Пятнадцати) минут с момента его обнаружения ПАК фильтрации посредством уведомлений по электронной почте, направляемых на адреса ответственных представителей Заказчика, указанных в регламенте взаимодействия Заказчика и Исполнителя (далее – Регламент), а также посредством демонстрации аномалий в личном кабинете. | Для обеспечения бесперебойной передачи данных Заказчика. |
| Исполнитель проводит анализ Интернет-трафика с учётом следующих признаков Интернет-трафика:<br>– диапазон IP-адресов отправителя/получателя Интернет-трафика;<br>– диапазон адресов портов TCP/UDP отправителя/получателя Интернет-трафика;<br>– параметры протоколов IP, DNS, TCP, UDP, ICMP, SYN, но не ограничиваясь ими (например, значения TCP-флагов для протокола TCP/IP). | Для обеспечения бесперебойной передачи данных Заказчика. |
| Исполнитель проводит анализ Интернет-трафика по следующим параметрам:<br>– характеристики Интернет-трафика: распределение по параметрам протоколов IP, DNS, TCP, UDP, ICMP, SYN, но не ограничиваясь ими (например, значения TCP-флагов для протокола TCP/IP);<br>– количество пакетов Интернет-трафика в секунду (PPS);<br>– количество байт Интернет-трафика в секунду (BPS). | 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 предоставляются следующие подтверждающие документы и материалы:

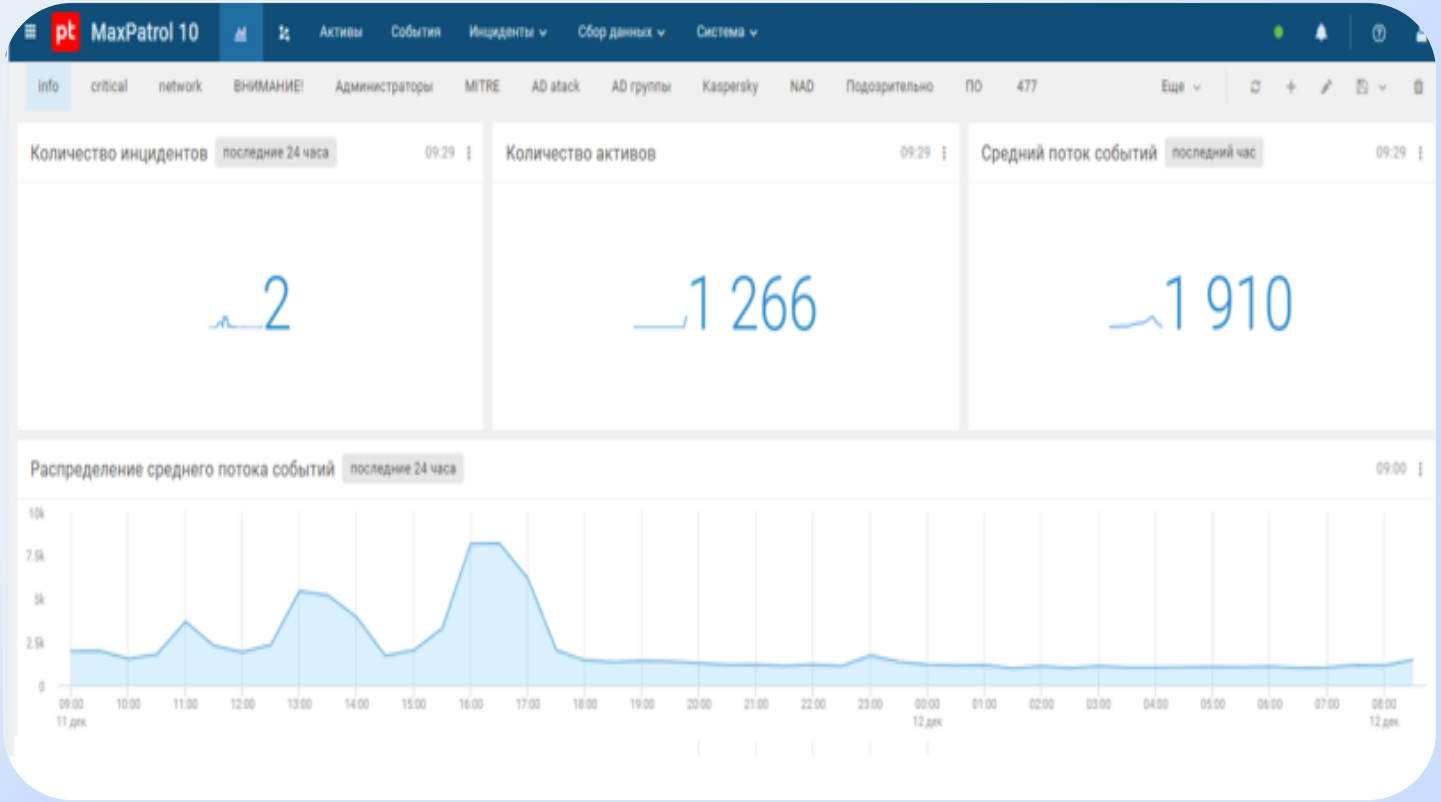
- ✓ снимок экрана с вкладки настроек системы (средства) мониторинга информационной безопасности, отображающий установленные настройки оповещения о неудачных попытках входа для всех привилегированных учетных записей.



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

С результатами оценки предоставляются следующие подтверждающие документы и материалы:

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



# О методическом подходе к оценке текущего состояния защиты информации в информационных системах и обеспечения безопасности объектов критической информационной инфраструктуры в органах государственной власти и организациях

**Жиров Павел Валентинович**

Начальник управления ФСТЭК России