Некоторые аспекты расчета показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Звягинцева Полина Александровна

начальник отдела Управления ФСТЭК России

Об утверждении Требований
о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

31. Оценка состояния защиты информации должна проводиться на основе определения оператором:

а) показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации (далее — показатель защищенности $К_{зи}$);

б) показателя, который определяет достаточность и эффективность проведения мероприятий по защите информации (далее — показатель уровня зрелости $П_{зи}$).

Показатель защищенности $К_{зи}$ и показатель уровня зрелости $П_{зи}$ являются показателями деятельности по защите информации оператора.

Для определения значений и расчета показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ должны применяться методические документы, утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о ФСТЭК России (далее — методические документы ФСТЭК России)[9].

РАСЧЕТ ПОКАЗАТЕЛЯ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ

- Обеспечивается минимальный уровень защиты от типовых актуальных угроз безопасности информации **(Кзи = 1);**
- Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеются предпосылки реализации актуальных угроз безопасности информации **(0,75 < Кзи < 1);**
- Минимальный уровень безопасности от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности информации **(Кзи ≤ 0,75)**

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ 0,1

	Показатель
$К_{11}$	На заместителя руководителя органа возложены полномочия ответственного лица за обеспечение информационной безопасности органа и определены его обязанности

1. Проверить наличие приказа или иного организационно-распорядительного документа органа государственной власти (далее – орган) о возложении на заместителя руководителя полномочий по обеспечению информационной безопасности органа и определению его обязанностей.

2. Оценить наличие в приказе или ином организационно-распорядительном документе органа обязанностей ответственного заместителя руководителя органа (организации) по организации защиты информации в органе.

***3.**В случае непредставления необходимого документа, а также отсутствия положения об обязанности ответственного заместителя руководителя за организацию защиты информации в органе показателю присваивается нулевое значение*

1. Возложение полномочий и (или) определение структурного подразделения (работников) в органе (организации) подтверждается изданием соответствующего локального правового акта.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ 0,1

	Показатель
K_{12}	Определены функции (обязанности) структурного подразделения (или отдельных работников), ответственного за обеспечение информационной безопасности органа

1.Проверить наличие приказа или иного организационно-распорядительного документа в органе о создании структурного подразделения (или возложению полномочий на отдельных работников), ответственного за обеспечение информационной безопасности органа.

2.Оценить наличие в приказе или ином организационно-распорядительном документе органа (организации) полномочий (функций) структурного подразделения по ИБ по обеспечению защиты информации в органе (организации).

3.В случае непредставления необходимого документа, а также отсутствия положения об обязанности ответственного заместителя руководителя за организацию защиты информации в органе показателю присваивается нулевое значение

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ 0,1

	Показатель
K_{13}	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

Проверить наличие договора (контракта), заключенного с подрядными организациями, обеспечивающими ***администрирование и (или) техническую поддержку информационной инфраструктуры*** *органа и оценить наличие в них требований по защите информации в подключаемых к информационной инфраструктуре органа системах подрядной организации*

1. В случае если подрядные организации не привлекаются, частному показателю безопасности k_{13} присваивается значение из таблицы.

Контракт № [redacted]

на оказание услуг по техническому сопровождению компонента Единой государственной информационной системы в сфере здравоохранения Новосибирской области [redacted]

г. Новосибирск «__»_____2025 г.

3. Порядок оказания Услуг

3.1. Исполнитель оказывает Услуги в соответствии с Описанием объекта закупки (Приложение №1 к Контракту).

3.2. Место оказания Услуг: По месту нахождения Исполнителя, при необходимости по [redacted]

Для оказания услуг в удалённом режиме Исполнитель запрашивает доступ к необходимым ресурсам Компонентов ЕГИСЗ НСО у Заказчика.

Ответственность Исполнителя за оказание тех или иных услуг, требующих удаленного доступа, наступает с момента получения такого доступа к необходимым ресурсам. Исполнитель несёт ответственность за сбой в работе Компонентов ЕГИСЗ НСО и Сервисов интеграции, возникших в результате оказания услуг Исполнителем.

Оказание услуг в очном режиме осуществляется индивидуально, на рабочих местах пользователей и Уполномоченной организации в заранее согласованное время (с понедельника по пятницу с 9-00 до 18-00, кроме праздничных дней1) в соответствии со временем часовой зоны, в которой расположен Функциональный заказчик (г. Новосибирск).

3.3. Срок оказания Услуг Исполнителем по Контракту в полном объеме: с 01.02.2025 г. по 30.11.2025 г.

3.4. Срок исполнения Контракта: с 01.02.2025 г. по 25.12.2025 г.

---

[1] В соответствии с установленным в Российской Федерации производственным календарем на 2025 год при пятидневной рабочей неделе.

6. ТРЕБОВАНИЯ К ПРЕДОСТАВЛЕНИЮ ДОСТУПА

Для оказания услуг в удалённом режиме Исполнитель запрашивает доступ к необходимым ресурсам [redacted] у Заказчика. После согласования перечня ресурсов Системы, к которым необходимо обеспечить удаленный доступ со стороны Исполнителя, и уровня запрашиваемых полномочий, Заказчик в течение трех рабочих дней с момента подписания правил доступа обеспечивает доступ (при наличии технической возможности) к запрашиваемым серверам, на которых установлена Система и ее компоненты, в том числе к имеющимся в рас
серверам защищённ
использованием тех
требованиям безопас
требуемых для удал
осуществляется Испо

8. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

При оказании услуг по настоящему описанию объекта закупки, Исполнитель должен обеспечить соблюдение сотрудниками Исполнителя требований к обеспечению конфиденциальности, целостности и доступности обрабатываемой в Системе информации.

Исполнитель должен определить перечень работников, для которых предполагается удаленный доступ к информационной инфраструктуре Системы, а также перечень информации и информационных ресурсов, расположенных на серверах Системы, к которым будет предоставляться удаленный доступ.

Информация о правах доступа (предоставление, изменение, прекращение прав доступа) сотрудников Исполнителя к компонентам Системы и ее информационным ресурсам должна фиксироваться Исполнителем в ходе оказания услуг по настоящему описанию объекта закупки и предоставляться Заказчику и (или) функциональному заказчику по требованию.

В целях регистрации и учета действий пользователей и администраторов, в [redacted] ЕГИСЗ НСО внутренними (встроенными) средствами Системы должно быть обеспечено журналирование (фиксирование) действий пользователей и администраторов – вход (выход) в (из) системы, действий с персональными данными, совершаемых пользователями в рамках сессии пользователя.

Средства диагностирования Системы должны обеспечивать сбор и накопление информации о процессах загрузки и передачи данных, критических ошибках и предупреждениях в работе программных средств системы, загрузке аппаратной части (процессоры, память). Выполнение требования должно достигаться за счет внутренних

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ПОЛЬЗОВАТЕЛЕЙ	0,25

№	Показатель
K_{21}	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

1.Проверить наличие в органе утвержденного документа, содержащего требования к паролям учетных записей пользователей информационной инфраструктуры органа.

2.Проверить как обеспечена реализация требований к минимальной длине пароля/используемым символам.

3. Проверить соответствие паролей учетных записей пользователей установленным требованиям .

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ПОЛЬЗОВАТЕЛЕЙ — 0,25

№	Показатель
K_{22}	Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)

1. Провести анализ привилегированных учетных записей в информационной инфраструктуре органа.

2. Определить каким образом реализована для привилегированных учетных записей двухфакторная аутентификация (например, токен, сертификаты).

3. Проверить реализацию двухфакторной аутентификации для привилегированных учетных записей

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ПОЛЬЗОВАТЕЛЕЙ — 0,25

№	Показатель
K_{23}	Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию.

1. Проанализировать перечень сервисных учетных записей, а также учетных записей разработчиков, применяемых в информационной инфраструктуре органа

2. Удостовериться, что в СЗИ от НСД настроен сброс пароля после первой аутентификации пользователя, а также установлены требования к длине пароля и используемым символам.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ПОЛЬЗОВАТЕЛЕЙ — 0,25

№	Показатель
$К_{24}$	Отсутствуют активные учетные записи работников органа (организации) и работников, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения.

1.Оценить наличие в Регламенте о парольной политики положений о порядке создания, удаления учетных записей уволенных работников органа, либо подрядных организаций, с которыми прекращены трудовые отношения.

2.Проанализировать перечень учетных записей работников органа, а также разработчиков и сервисные ученые записи, с которыми в течение года прекращены трудовые или иные отношения (при наличии).

3.Удостовериться, что СЗИ от НСД отсутствуют активные учетные записи работников, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ — 0,35

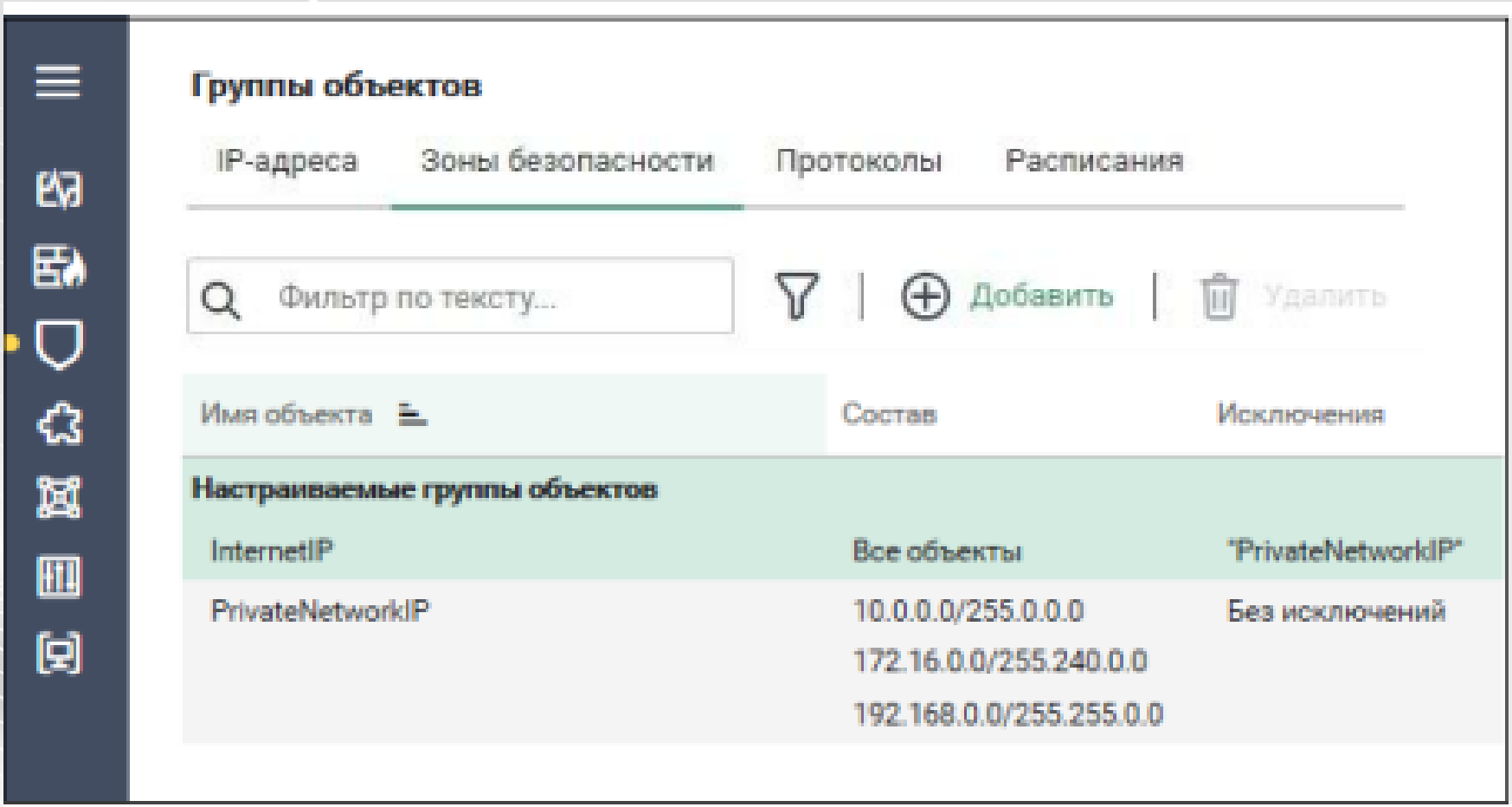
№	Документы, мероприятия
$К_{31}$	На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет, контролируется межсетевыми экранами уровня L3/L4).

1.Оценить применение на периметре информационных систем межсетевых экранах уровня сети (L3/L4).

2.Проанализировать имеющиеся в органе результаты сканирования инфраструктуры на предмет определения сервисов и служб, доступных из сети Интернет.

3.Проанализировать настройки межсетевого экрана, сравнить с Правилами фильтрации …, утвержденными в органе.

4.Сравнить перечень интерфейсов органа, доступных из сети Интернет с параметрами фильтрации межсетевого экрана. Доступ к сервисам и службам, доступным из сети Интернет, должен осуществляться через межсетевой экран.


Группы объектов
IP-адреса
Зоны безопасности
Протоколы
Расписания
Фильтр по тексту...
Добавить
Удалить
Имя объекта
Состав
Исключения
Настраиваемые группы объектов
InternetIP
Все объекты
"PrivateNetworkIP"
PrivateNetworkIP
10.0.0.0/255.0.0.0
172.16.0.0/255.240.0.0
192.168.0.0/255.255.0.0
Без исключений

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ — 0,35

№	Документы, мероприятия
$К_{32}$	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.

1.Проанализировать результаты последнего сканирования информационной инфраструктуры органа на предмет наличия критических уязвимостей. Выделить уязвимости, относящиеся к устройствам и интерфейсам, доступным из сети Интернет, сопоставив уязвимости с перечнем таких устройств и интерфейсов.

2.Провести анализ отчета с результатами сканирования информационной инфраструктуры на наличие уязвимостей и определить наличие критических уязвимостей на устройствах и интерфейсах, доступных из сети Интернет.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ — 0,35

№	Документы, мероприятия
$К_{33}$	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.

1.Проанализировать результаты последнего сканирования информационной инфраструктуры органа на предмет наличия критических уязвимостей. Выделить уязвимости, относящиеся к пользовательским устройствам и серверам, сопоставив уязвимости с перечнем таких устройств и серверов.

2.Провести анализ отчета с результатами сканирования информационной инфраструктуры на предмет наличия критических уязвимостей на пользовательских устройствах и серверах.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ — 0,35

№	Документы, мероприятия
$К_{34}$	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)).

1. Проверить фактическое состояние состава информационной (автоматизированной) системы составу в техническом паспорте.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ — 0,35

№	Документы, мероприятия
$К_{35}$	Обеспечена проверка вложений в электронных письмах электронной почты на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств).

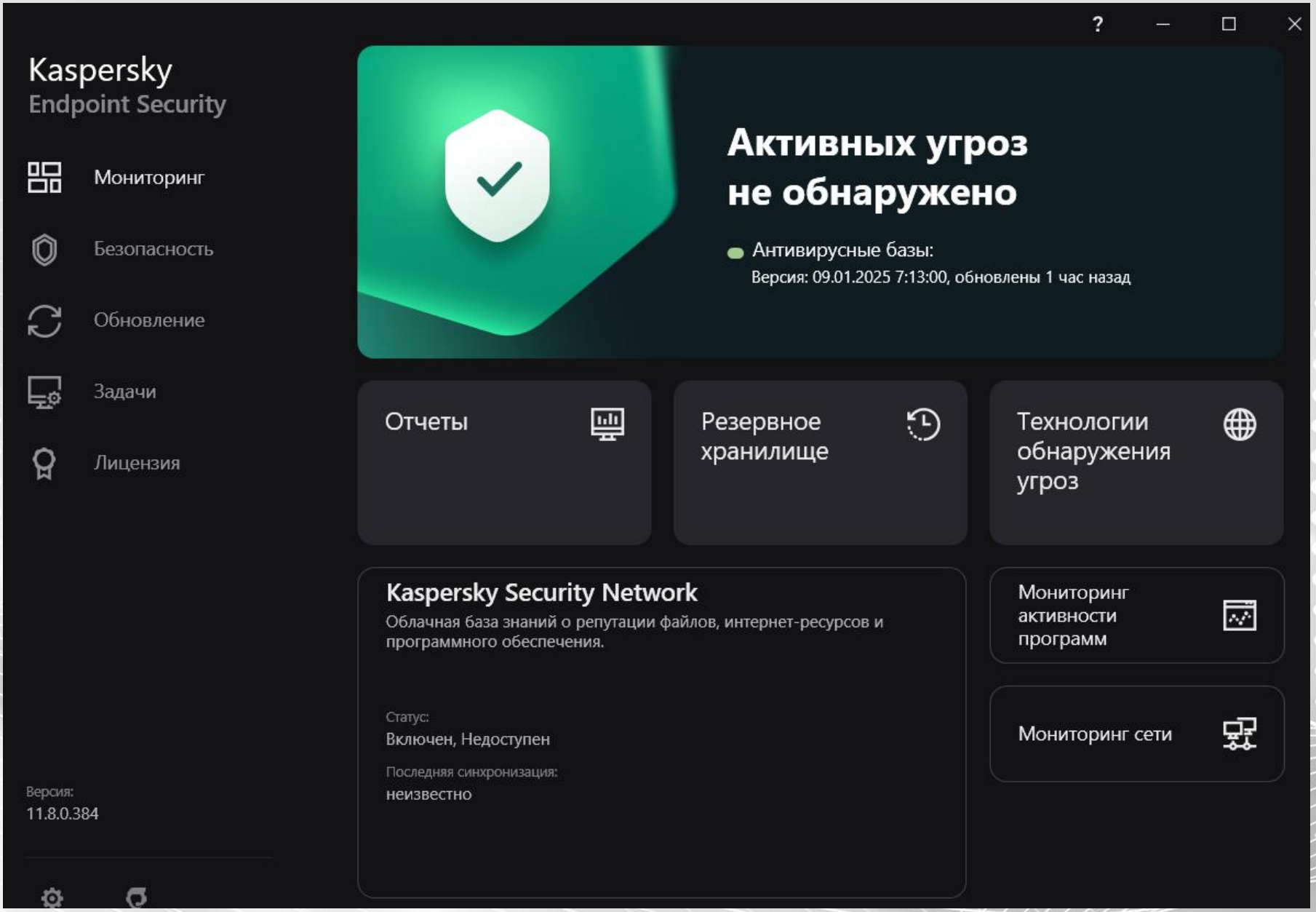
1.Оценить используется ли в информационной инфраструктуре электронная почта.

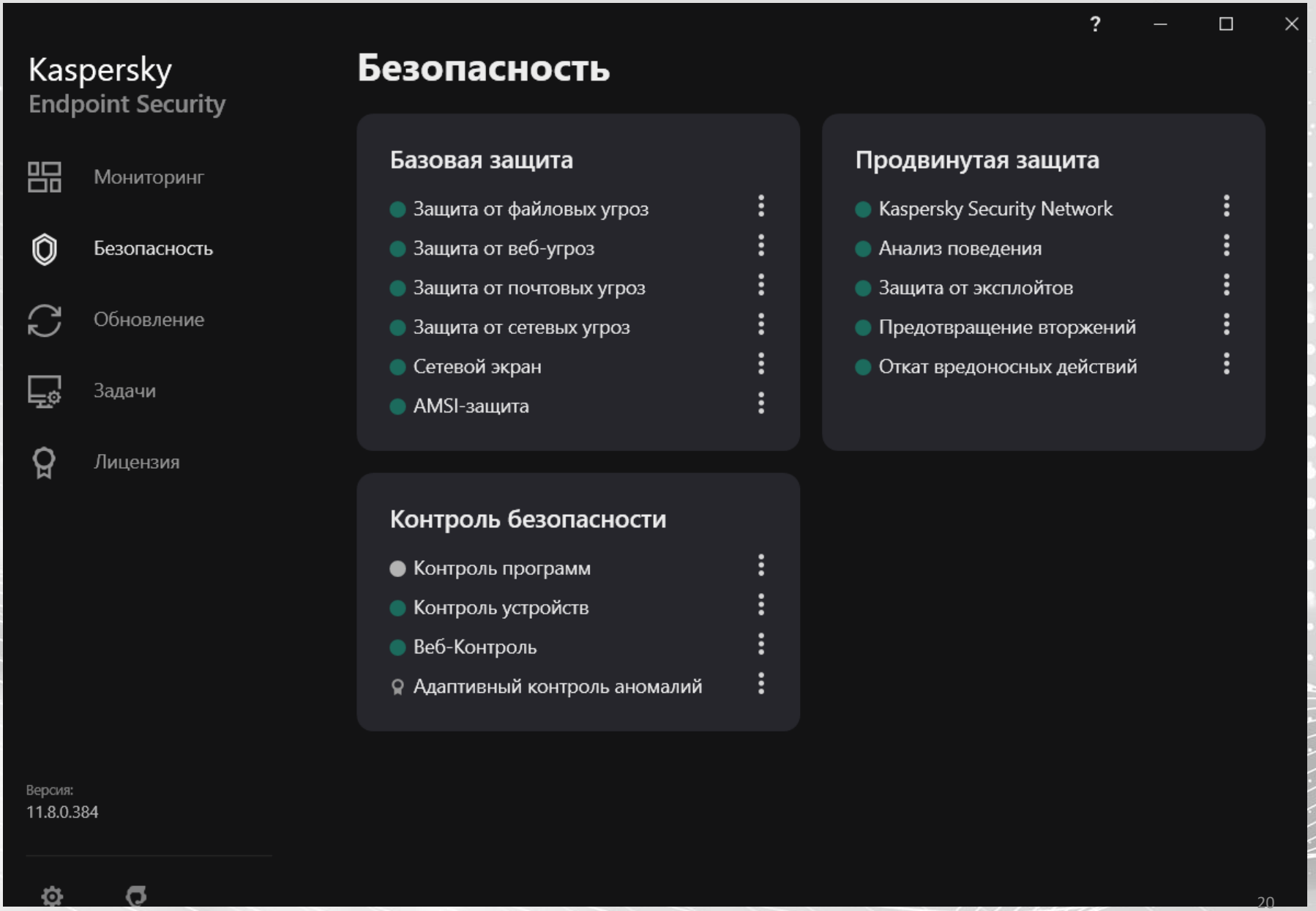
2.Проанализировать количество почтовых клиентов, в том числе количество АРМ, на которых они установлены, а также количество учетных записей, применяемых в органе для обмена электронными письмами.

3.Оценить применяются ли средства антивирусной защиты на указанных АРМ.

4.Проверить каким образом и какими средствами обеспечена проверка вложений в электронных письмах.

5.Выборочно осуществить на рабочих местах пользователей проверки почтовых вложений (проверить осведомленность пользователей по этому вопросу).


Kaspersky
Endpoint Security
Мониторинг
Безопасность
Обновление
Задачи
Лицензия
Версия:
11.8.0.384
Активных угроз не обнаружено
Антивирусные базы:
Версия: 09.01.2025 7:13:00, обновлены 1 час назад
Отчеты
Резервное хранилище
Технологии обнаружения угроз
Kaspersky Security Network
Облачная база знаний о репутации файлов, интернет-ресурсов и программного обеспечения.
Статус:
Включен, Недоступен
Последняя синхронизация:
неизвестно
Мониторинг активности программ
Мониторинг сети


Kaspersky
Endpoint Security
Мониторинг
Безопасность
Обновление
Задачи
Лицензия
Версия:
11.8.0.384
Безопасность
Базовая защита
Защита от файловых угроз
Защита от веб-угроз
Защита от почтовых угроз
Защита от сетевых угроз
Сетевой экран
AMSI-защита
Продвинутая защита
Kaspersky Security Network
Анализ поведения
Защита от эксплойтов
Предотвращение вторжений
Откат вредоносных действий
Контроль безопасности
Контроль программ
Контроль устройств
Веб-Контроль
Адаптивный контроль аномалий

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ — 0,35

№	Документы, мероприятия
$К_{36}$	Обеспечено централизованное управление средствами антивирусной защиты (не менее чем 80% пользовательских устройств 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.

1.Проверить, осуществляется ли централизованное обновление средств антивирусной защиты, а также оценить с использованием каких средств (например, СЗИ Kaspersky Security Center, № 3155).

2.Проанализировать перечень пользовательских устройств, используемых в органе (количество АРМ). Сколько устройств контролируется в KSC.

3.В случае применения средств антивирусной защиты с централизованным управлением сверить перечень пользовательских устройств с перечнем устройств, указанным в средстве антивирусной защиты с централизованным управлением.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ 0,35

№	Документы, мероприятия
$К_{37}$	Реализована очистка входящего из сети Интернет сетевого трафика от аномалий на уровне L3/L4 (заключен договор с провайдером)

1.Проанализировать перечень веб-сайтов, служб и иных сервисов, доступных из сети Интернет, функционирующих в органе (организации).

2.Оценить какими средствами в органе организована очистка входящего из сети «Интернет» трафика.

3.В случае, если фильтрация трафика осуществляется подрядной организацией, проанализировать соответствующий договор, заключенный с данной организацией.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ — 0,30

№	Документы, мероприятия
$К_{41}$	Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей.

1.Оценить какими средствами в органе (организации) реализован централизованный сбор событий безопасности.

2.Проанализировать в отношении каких событий безопасности осуществляется сбор, а также каким образом организовано оповещение о неудачных попытках входа для привилегированных учетных записей.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ — 0,30

№	Документы, мероприятия
$К_{42}$	Реализован централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с сетью Интернет.

1. Проанализировать перечень всех устройств, взаимодействующих с сетью Интернет.

2. В дополнение к порядку оценки показателя, содержащегося в предыдущем пункте, проверить как в органе реализован сбор событий безопасности на всех устройствах, взаимодействующих с сетью Интернет.

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ — 0,30

№	Документы, мероприятия
$К_{43}$	Утвержден документ, определяющий порядок реагирования на компьютерные инциденты.

Проверить наличие организационно-распорядительного документа, утвержденного в органе, определяющего порядок реагирования на компьютерные инциденты.

п. 18 Приказа ФСТЭК России № 17
п. 13 Приказа ФСТЭК России № 239

Рекомендации Управления от 31 июля 2024 г. № 1677
Рекомендации Управления от 31 июля 2024 г. № 1678

ЗВЯГИНЦЕВА Полина Александровна

Спасибо за внимание!

т.(383)203-54-09