Актуальные вопросы защиты информации и обеспечения безопасности значимых объектов КИИ

ЗВЯГИНЦЕВА Полина Александровна
начальник отдела Управления ФСТЭК России
по Сибирскому федеральному округу,
февраль 2026

ФСТЭК России

Обеспечение безопасности критической информационной инфраструктуры

Значимые объекты критической информационной инфраструктуры

Техническая защита информации

Государственные информационные системы, муниципальные информационные системы
…

Изменения в Кодекс Российской Федерации об административных правонарушениях

в части усиления ответственности за нарушение правил защиты информации

Статья 13.12. КоАП	Прошлая редакция	Новая действующая редакция
Часть 2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну)	Граждане – от 1,5 тыс. руб. до 2,5 тыс.руб. Должностные лица – от 2,5 тыс. руб. до 3 тыс.руб. Юр. лица – от 20 тыс. руб. до 25 тыс.руб.	Граждане – от 5 тыс. руб. до 10 тыс.руб. Должностные лица – от 10 тыс. руб. до 50 тыс.руб. Юр. лица – от 50 тыс. руб. до 100 тыс.руб.
Часть 4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну	Должностные лица – от 3 тыс. руб. до 4 тыс.руб. Юр. лица – от 20 тыс. руб. до 30 тыс.руб.	Должностные лица – от 20 тыс. руб. до 50 тыс.руб. Юр. лица – от 50 тыс. руб. до 100 тыс.руб.
Часть 6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации	Граждане – от 500 руб. до 1 тыс.руб. Должностные лица – от 1 тыс. руб. до 2 тыс.руб. Юр. лица – от 10 тыс. руб. до 15 тыс.руб.	Граждане – от 5 тыс. руб. до 10 тыс.руб. Должностные лица – от 10 тыс. руб. до 50 тыс.руб. Юр. лица – от 50 тыс. руб. до 100 тыс.руб.
Часть 7. Нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации	Граждане – от 1 тыс.руб. до 2 тыс.руб. Должностные лица – от 3 тыс. руб. до 4 тыс.руб. Юр.лица – от 15 тыс. руб. до 20 тыс.руб.	Граждане – от 10 тыс. руб. до 20 тыс.руб. Должностные лица – от 20 тыс. руб. до 50 тыс.руб. Юр.лица – от 50 тыс. руб. до 100 тыс.руб.

Статья 13.12_1 КоАП	Административный штраф
Часть 1. Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния,	Должностные лица – от 10 тыс.руб. до 50 тыс.руб. Юр. лица – от 50 тыс.руб. до 100 тыс.руб.

Статья 19.7_15 КоАП	Административный штраф
Часть 1. Непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, либо об отсутствии необходимости присвоения ему одной из таких категорий либо представление недостоверных сведений	Должностные лица – от 10 тыс.руб. до 50 тыс.руб. Юр. лица – от 50 тыс.руб. до 100 тыс.руб.

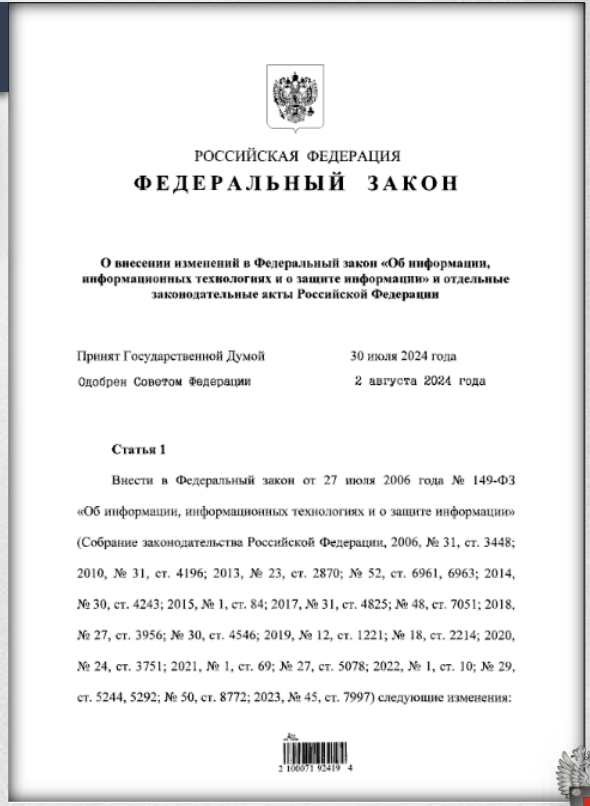
Совершенствование требований о защите информации

Совершенствование требований о защите информации

О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»

8.1.Не допускается передача информации из государственных информационных систем в иные информационные системы, не соответствующие требованиям о защите информации, установленным **статьей 16 настоящего Федерального закона**.

5.Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений применяемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации

Принят Государственной Думой 30 июля 2024 года

Одобрен Советом Федерации 2 августа 2024 года

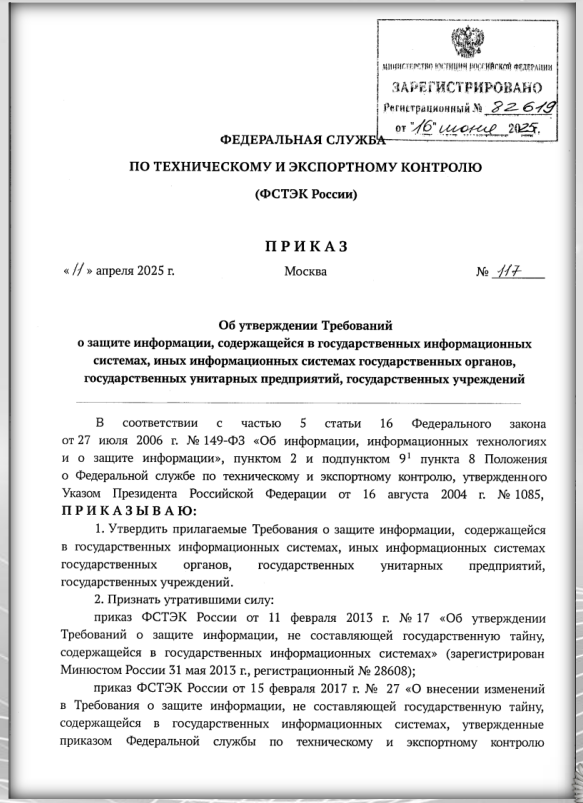
Статья 1

Внести в Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2013, № 23, ст. 2870; № 52, ст. 6961, 6963; 2014, № 30, ст. 4243; 2015, № 1, ст. 84; 2017, № 31, ст. 4825; № 48, ст. 7051; 2018, № 27, ст. 3956; № 30, ст. 4546; 2019, № 12, ст. 1221; № 18, ст. 2214; 2020, № 24, ст. 3751; 2021, № 1, ст. 69; № 27, ст. 5078; 2022, № 1, ст. 10; № 29, ст. 5244, 5292; № 50, ст. 8772; 2023, № 45, ст. 7997) следующие изменения:

Приказ ФСТЭК России от 11 апреля 2025 г. № 117

Требования
о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

вступают в силу с 1 марта 2026 г.



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 82619
от "16" июня 2025

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« // » апреля 2025 г. Москва № 117

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

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», пунктом 2 и подпунктом 9^1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085,
П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений.

2. Признать утратившими силу:

приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608);

приказ ФСТЭК России от 15 февраля 2017 г. № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю

II. Организация деятельности по защите информации и управление данной деятельностью

Организация деятельности по защите информации должна включать:

а) разработку и утверждение **политики защиты информации**;

б) определение **лиц, ответственных** за защиту информации;

в) применение **программных, программно-аппаратных средств,** предназначенных для защиты информации;

г) разработку и утверждение **внутренних стандартов** по защите информации;

д) разработку и утверждение **внутренних регламентов** по защите информации;

е) выделение организационных, технических и иных **ресурсов**, необходимых для защиты информации.

Политика защиты информации

Руководитель или уполномоченное им лицом

утверждает

1) Область действия политики…;
2) Цели и задачи защиты информации;
3) Принципы и защиты информации;
4) Перечни объектов защиты,…;
5) Категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия;
6) Состав организационной системы управления деятельностью по защите информации и схему взаимодействия ее элементов;
7) Ответственность работников за нарушение требований о защите информации и установленных оператором (обладателем информации) правил обработки информации

должна учитывать

ознакомлены выполнять

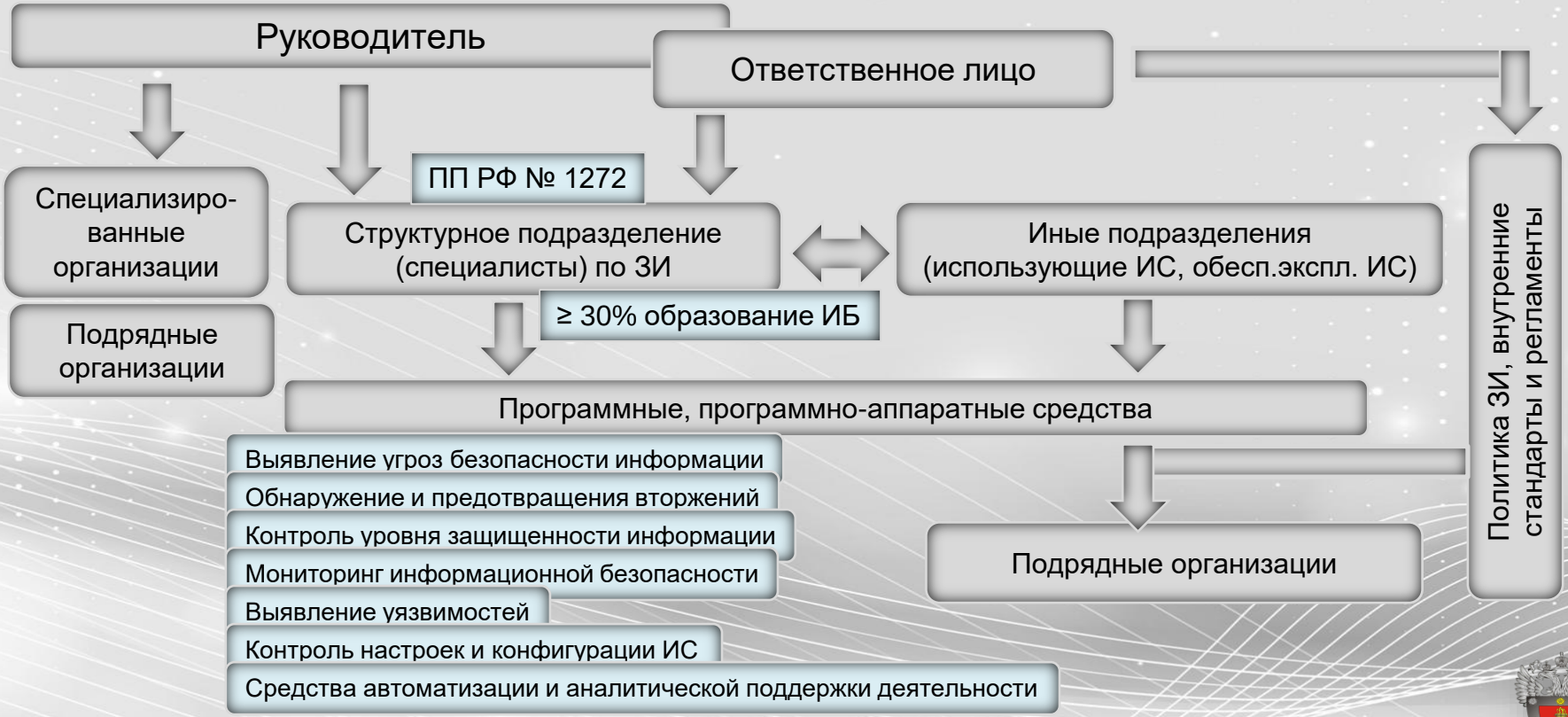
Информационные системы

Информационно-телекоммуникационную инфраструктуру

Подрядные организации

Подразделения (работники) оператора

Организация деятельности по защите информации и управление данной деятельностью



Организация деятельности по защите информации и управление данной деятельностью

Структурное подразделение (специалисты) по защите информации

Руководитель оператора, ответственное лицо

На основе представленных предложений и в пределах имеющихся средств

Предложения по организационным, материально-техническим и иным обеспечивающим ресурсам, необходимым для проведения мероприятий и принятия мер по защите информации,

с указанием сведений о целях защиты информации, на достижение которых требуются ресурсы, и перечня негативных последствий (событий), наступление которых прогнозируется

Предусматривает выделение организационных, материально-технических и иных обеспечивающих ресурсов для проведения мероприятий и принятия мер по защите информации

привлечения при необходимости дополнительных сил и средств для защиты информации в соответствии с Требованиями на всех этапах жизненного цикла информационных систем.

Внутренние стандарты по защите информации

требования к **первичной идентификации лиц**, обладающих правами доступа к информационным системам и (или) содержащейся в них информации и их использованию;

требования к применяемым **моделям доступа пользователей**;

перечень **разрешенного и (или) запрещенного для использования программного обеспечения**;

требования **к типовым конфигурациям и настройкам программных, программно-аппаратных средств**;

требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения доступа пользователей из сети «Интернет»;

требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения **удаленного доступа пользователей к ИС и содержащейся в них информации**, включая требования к обеспечению безопасной дистанционной работы;

ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации ими ИС;

требования к защите **физических и виртуальных устройств** ИС, имеющих постоянный доступ к сети «Интернет»;

требования к защите **мобильных устройств**, планшетных, переносных компьютеров, применяемых пользователями для доступа к ИС (за исключением мобильных устройств, предназначенных для доступа к сайтам сети "Интернет" и иным публичным веб-ресурсам);

требования **к непрерывности функционирования** информационных систем;

требования **к резервному копированию информации**, программного обеспечения и его конфигураций;

требования к **сбору, регистрации и анализу событий**, связанных с возможным нарушением безопасности информации, нарушением функционирования информационных систем, реализацией угроз безопасности информации

требования к защите информации **при подключении к информационным системам иных информационных систем**, включая требования к каналам передачи данных при взаимодействии с такими информационными системами.

Внутренние регламенты по защите информации

порядок создания, учета, изменения и блокирования, контроля, удаления **учетных записей**;

порядок создания, учета, изменения и блокирования, контроля, удаления **привилегированных учетных записей**;

порядок создания, изменения, блокирования, контроля, удаления **аутентификационной информации и средств…**;

порядок предоставления пользователям **удаленного доступа** к ИС и содержащейся в них информации;

порядок и условия предоставления работникам **подрядных организаций** доступа к ИС, содержащейся в них информации, и (или) передачи им информации, контроля за таким доступом, передачей в случае привлечения подрядных организаций;

порядок предоставления работникам **иных государственных органов, организаций** доступа к ИС, …;

порядок предоставления пользователям доступа из ИС в сеть **"Интернет"** и контроля ее использования;

порядок повышения уровня **знаний и информированности пользователей** по вопросам защиты информации;

порядок выявления, оценки и устранения **уязвимостей** ИС;

порядок получения, оценки, тестирования и применения **обновлений** программных, программно-аппаратных;

порядок обработки, хранения и обращения с информацией ограниченного доступа;

порядок разработки **безопасного программного обеспечения** в случае его самостоятельной разработки оператором (обладателем информации);

порядок обеспечения **физической защиты** ИС;

порядок вывода в контур промышленной эксплуатации сервисов, доступ к которым осуществляется **с использованием сети "Интернет"**, в случае наличия таких сервисов;

порядок **мониторинга** информационной безопасности информационных систем;

порядок **восстановления** штатного функционирования ИС и тестирования процессов восстановления;

порядок **контроля уровня защищенности информации**, содержащейся в ИС.

Управление деятельностью по защите информации

Разработка и планирование мероприятий и мер по ЗИ	Проведение мероприятий и принятие мер по ЗИ	Проведение оценки состояния ЗИ	Совершенствование мероприятий и мер по ЗИ.
События в ИС…	Реализация организационных и технических мер по ЗИ	Показатель защищенности Кзи	Планирование мероприятий по ЗИ
ИС, ПО, ПАС…		Показатель уровня зрелости Пзи	Реализация мер по ЗИ
УБИ			
Состав и сроки проведения мероприятий и принятия мер			

Проведение мероприятий и принятие мер по защите информации

Требования к проведению мероприятий и принятию мер по защите информации

- Выявление и оценка УБИ
- Контроль конфигураций ИС
- Управления уязвимостями
- Управление обновлениями
- Обеспечение ЗИ при применении конечных устройств
- Обеспечение ЗИ при применении мобильных устройств
- Обеспечение ЗИ при удаленном доступе
- Обеспечение ЗИ привилегированного удаленного доступа
- Обеспечение мониторинга ИБ
- Обеспечение РБПО
- Обеспечение физической защиты ИС
- Обеспечение непрерывности функционирования ИС при НС
- Повышение уровня знаний и информированности
- Обеспечение ЗИ при взаим-вии с подрядными орг-циями
- Обеспечение ЗИ при от компьютерных атак (DDoS-атак)
- Обеспечение ЗИ при использовании ИИ
- Реализация в ИС мер по их защите и защите информации
- Проведение контроля уровня защищенности
- Обеспечение непрерывного взаимодействия с ГосСОПКА

Базовые меры защиты

а) идентификация и аутентификация

б) управление доступом

в) регистрация событий безопасности

г) защита виртуализации и облачных вычислений

д) защита технологий контейнерных сред и их оркестрации

е) защита сервисов электронной почты

ж) защита веб-технологий

з) защита программных интерфейсов взаимодействия приложений

и) защита конечных устройств

к) защита мобильных устройств

л) защита технологий интернета вещей

м) защита точек беспроводного доступа

н) антивирусная защита

о) обнаружение и предотвращение вторжений на сетевом уровне

п) сегментация и межсетевое экранирование

р) защита от компьютерных атак, направленных на отказ в обслуживании

с) защита каналов передачи данных и сетевого взаимодействия

Управление деятельностью по защите информации

Проводимые мероприятия и принимаемые **меры по защите информации** должны быть направлены

на блокирование (нейтрализацию) актуальных для информационной системы **угроз безопасности информации**

в соответствии **с целями защиты информации**, определенными в политике защиты информации.

Аттестация информационных систем и контроль уровня защищенности информации

Информационная система

До ввода в эксплуатацию

Аттестация на соответствие Требованиям в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. № 77

В ходе эксплуатации

Контроль уровня защищенности информации

а) выявление уязвимостей ИС с последующей экспертной оценкой;

б) выявление несанкционированных подключений устройств к ИС;

в) тестирование ИС путем моделирования реализации актуальных угроз;

г) проведение в соответствии с планом тренировок.

При отсутствии возможности реализации отдельных мероприятий и (или) принятия мер по защите информации в соответствии с Требованиями

оператором (обладателем информации) должны быть разработаны и внедрены компенсирующие меры, позволяющие обеспечить блокирование (нейтрализацию) актуальных угроз.

При этом оператором (обладателем информации) должно быть обосновано применение компенсирующих мер на этапе создания информационных систем,

а при аттестации информационных систем - подтверждена их эффективность для блокирования (нейтрализации) актуальных угроз.

не применяется

– для оценки текущего состояния защиты информации (обеспечения безопасности значимых объектов КИИ) в органе (организации) и степени его соответствия минимально необходимому уровню защиты информации (обеспечения безопасности значимых объектов КИИ) от типовых актуальных угроз безопасности информации

Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденная ФСТЭК России 2 мая 2024 г.

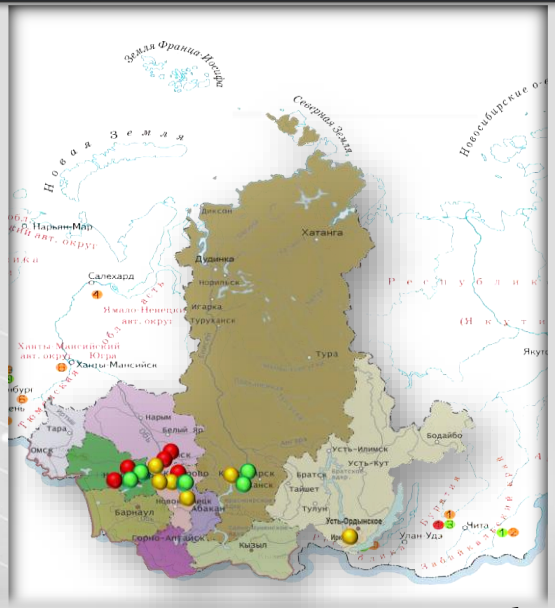
№	Мероприятия	Значение
1.	Централизованный сбор событий безопасности и оповещение о неудачных попытках..	**0,12**
2.	Централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с Интернет	**0,105**
3.	На устройствах и интерфейсах, доступных из сети Интернет, отсутствуют уязвимости критического уровня…	**0,0875**
4.	Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям	**0,075**
5.	Реализована многофакторная аутентификация привилегированных пользователей	**0,075**
6.	Документ, определяющий порядок реагирования на компьютерные инциденты	**0,075**
7.	На сетевом периметре информационных систем установлены МЭ L3/L4	**0,07**
8.	На пользовательских устройствах и серверах отсутствуют уязвимости критического уровня …	**0,0525**
9.	Обеспечена проверка вложений в электронных письмах электронной почты на наличие ВПО	**0,0525**
10.	Обеспечено централизованное управление средствами антивирусной защиты	**0,0525**
11.	Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными…	**0,05**
12.	Отсутствуют активные учетные записи работников органа и работников, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения	**0,05**
13.	Определены функции структурного подразделения (или отдельных работников), ответственного за обеспечение информационной безопасности органа	**0,04**
14.	Реализована очистка входящего из сети Интернет сетевого трафика от компьютерных атак, направленных на отказ в обслуживании на уровне L3/L4	**0,035**
15.	Назначение заместителя и возложение на него обязанностей	**0,03**
16.	Требования к подрядным организациям	**0,03**

План мероприятий по совершенствованию защиты информации

№	Наименование мероприятия	Срок выполнения	Ответственные подразделения (работники)
1	Внести изменения в парольную политику в части установления требований к учетным записям привилегированных пользователей	до 21 сентября 2025	Начальник отдела ИБ
2	…		

Результатом реализации мероприятий плана должно быть достижение значений **показателя защищенности Кзи** и **показателя уровня зрелости Пзи** не ниже нормированных значений.

ОЦЕНКА ПОКАЗАТЕЛЯ СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ 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)**

Направление информации во ФСТЭК России

Пункт Приказа	Что направляем	Периодичность (не реже)	Срок
32	Оценка показателя защищенности $К_{зи}$	1 раз/6 месяцев	5 раб. дней
32, 73	Оценка показателя уровня зрелости $П_{зи}$	1 раз/2 года	5 раб. дней
36	Согласование Модели угроз и ТЗ	При создании	-
38	Информация о найденных уязвимостях отсутствующих в БДУ	При обнаружении	5 раб. дней
49	Последний в текущем году отчет по результатам мониторинга или итоговый отчет за текущий год (в случае его разработки)	Ежегодно	-
65, 73	Аттестационные материалы (Приказ ФСТЭК России № 77)	При аттестации	5 раб. дней
65, 73	Протоколы контроля защиты информации (Приказ ФСТЭК России № 77)	1 раз/2 года (для аттестованных ИС)	-
67	Отчет по результатам проведения контроля уровня защищенности	1 раз/3 года или после инцидента	5 раб. дней

Количество доведенных дополнительных мер по повышению защищенности за 2025 год

51 рекомендации,

по устранению уязвимостей

72 рекомендации,

содержащие организационно-технические меры

Доведение дополнительных мер по повышению защищенности информационной инфраструктуры Российской Федерации

- Меры, связанные с устранением уязвимостей в программном обеспечении:
  - Установление обновления программного обеспечения в соответствии с Методикой тестирования обновлений безопасности…, утвержденной ФСТЭК России 28 октября 2022 г., Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России 30 июня 2025 г.;
  - Принятие компенсирующих мер защиты информации;
  - Данная уязвимость не актуальна, ввиду отсутствия соответствующего программного обеспечения.
- Организационно-технические меры для повышения защищенности информационной инфраструктуры.

Спасибо за внимание!

По вопросам расчета показателя защищенности Кзи и реализации мер защиты информации

ЗВЯГИНЦЕВА Полина Александровна

т.(383)203-54-09

По вопросам реализации Требований по защите информации

ЩЕКЛАЧЕВ Иван Владимирович

т.(383)203-54-13