

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 2.0:

Что изменится с новым приказом
ФСТЭК России?


infotecs



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Вебинар





**ВАЛЕНТИН
СЕЛИФАНОВ**

заместитель руководителя
обособленного подразделения



**ИВАН
СИТЬКОВ**

коммерческий
директор ГК ЦИБ



Ключевой задачей является экспертная оценка новых требований регулятора и формирования исчерпывающего перечня необходимых действий и сроков их реализации.

НА ВЕБИНАРЕ ВЫ ПОЛУЧИТЕ:

- Пошаговый план мероприятий для выполнения требований, утверждённых приказом ФСТЭК России № 117 от 11.04.2025;
- Чек-лист решений;
- Ответы экспертов на ваши вопросы.

ЭКСПЕРТЫ ВЕБИНАРА

Сегодня с нами эксперты с многолетним опытом в области информационной безопасности. Они ответят на все ваши вопросы.



**НИКИТА
СЕЛЮТИН**

специалист по защите
информации ООО «ЦИБ»



**АЛЕКСАНДР
АНДРОСЕНКО**

инженер 1 категории
ООО «ЦИБ»



Компания «ИнфоТеКС» – ведущий разработчик и производитель высокотехнологичных программных и программно-аппаратных средств защиты информации. Входит в ТОП-10 крупнейших российских компаний в сфере защиты информации.

В портфеле ИнфоТеКС более 50 продуктов для защиты информации, выпускаемых под брендом ViPNet. Среди них решения для защиты каналов связи, решения по обнаружению и пресечению угроз и вторжений, защите серверов и рабочих станций от несанкционированного доступа, решения по защите мобильных устройств и коммуникаций, ИБ АСУ ТП, IIoT, криптографические сервисы, криптографические библиотеки, модули для встраивания и другие решения.

ИнфоТеКС – первая российская компания, которая сертифицировала квантово-криптографическую систему выработки и распределения ключей.



ТОП-5 ИТ-компаний в области разработки ПО

ТОП-10 в сфере защиты информации

>50 продуктов для защиты информации

>30 ЛЕТ на рынке ИБ

13 офисов по стране

>1700 сотрудников

**<МЫ ЗАЩИЩАЕМ ИНФОРМАЦИЮ,
КОТОРУЮ ВЫ ЦЕНИТЕ/>**



ТОП-30

системных интеграторов России



Количество аттестованных
объектов информатизации



Количество спроектированных
систем защиты



«Лучшее малое предприятие
в сфере услуг» 2019 г.
(Алтайский край)



Количество введенных
в эксплуатацию систем
защиты информации



SOC-мониторинг инфраструктуры
и выявления инцидентов
информационной безопасности



**ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

**СИСТЕМНЫЙ
ИНТЕГРАТОР РОССИИ**

«ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» - СИСТЕМНЫЙ ИНТЕГРАТОР С КОМПЕТЕНЦИЯМИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

НАША КОМПАНИЯ —

технологичный партнёр как для бизнеса, так и для государственных организаций: создаём системы защиты любого уровня сложности, которые работают на результат.

МИССИЯ КОМПАНИИ —

внедрять информационные технологии с целью оптимизации и управляемости технологических процессов организаций, делая их ИТ-инфраструктуру более мобильной, безопасной, способной экономить ресурсы и время заказчика.

**«ЦИБ» - ВАШ ЩИТ В МИРЕ ТЕХНОЛОГИЙ: ЗАЩИЩАЕМ И ОБЕРЕГАЕМ!
С НАМИ ВЫ ВСЕГДА НА ШАГ ВПЕРЕДИ КИБЕРУГРОЗ!**

НОВЫЕ ТРЕБОВАНИЯ ПО ИБ

Ответ на новые киберугрозы

 **infotecs**



НОВЫЕ ТРЕБОВАНИЯ ПО ИБ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ **часть 5 статьи 16**



ПРИКАЗ ФСТЭК РОССИИ ОТ 11.04.2025 №117



ПРИКАЗ ФСБ РОССИИ ОТ 18.03.2025 №117



Государственная Информационная Система



иные Информационные Системы гос. органов, ГУП, ГУ



Муниципальная Информационная Система



ИС, в которые передается информация ограниченного доступа из ГИС





ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

НОВЫЕ ТРЕБОВАНИЯ ПО ИБ

Приказ ФСТЭК России от 11.04.2025 №117



ЭВОЛЮЦИЯ ТРЕБОВАНИЙ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

2002

АС

2007-2008

**АС,
КСИИ,
ИСПДн**

2013-2014

**АС,
ИСПДн,
ГИС,
АСУ ТП**

2017

**АС
ИСПДн,
ГИС,
АСУ ТП
ЗО КИИ**

2026

**ИС
ЗО КИИ**

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ЗИ И УПРАВЛЕНИЕ ДАННОЙ ДЕЯТЕЛЬНОСТЬЮ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs



ОПЕРАТОР

обладатель
информации

должен
организовывать
деятельность по ЗИ
и управлять ею в
соответствии с
Требованиями



А

РАЗРАБОТКА И УТВЕРЖДЕНИЕ ПОЛИТИКИ ЗИ



Б

ОПРЕДЕЛЕНИЕ ЛИЦ, ОТВЕТСТВЕННЫХ ЗА ЗИ



В

ПРИМЕНЕНИЕ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ
СРЕДСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ЗИ



Г

РАЗРАБОТКУ И УТВЕРЖДЕНИЕ ВНУТРЕННИХ СТАНДАРТОВ ПО ЗИ



Д

РАЗРАБОТКУ И УТВЕРЖДЕНИЕ ВНУТРЕННИХ РЕГЛАМЕНТОВ ПО ЗИ



Е

ВЫДЕЛЕНИЕ ОРГАНИЗАЦИОННЫХ, ТЕХНИЧЕСКИХ И ИНЫХ
РЕСУРСОВ, НЕОБХОДИМЫХ ДЛЯ ЗИ

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ЗИ И УПРАВЛЕНИЕ ДАННОЙ ДЕЯТЕЛЬНОСТЬЮ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs



ПОЛИТИКА



ВНУТРЕННИЕ СТАНДАРТЫ

Требования к реализации мер по
ЗИ применительно к особенностям
деятельности оператора
(обладателя информации) и
функционирования ИС 13



ВНУТРЕННИЕ РЕГЛАМЕНТЫ

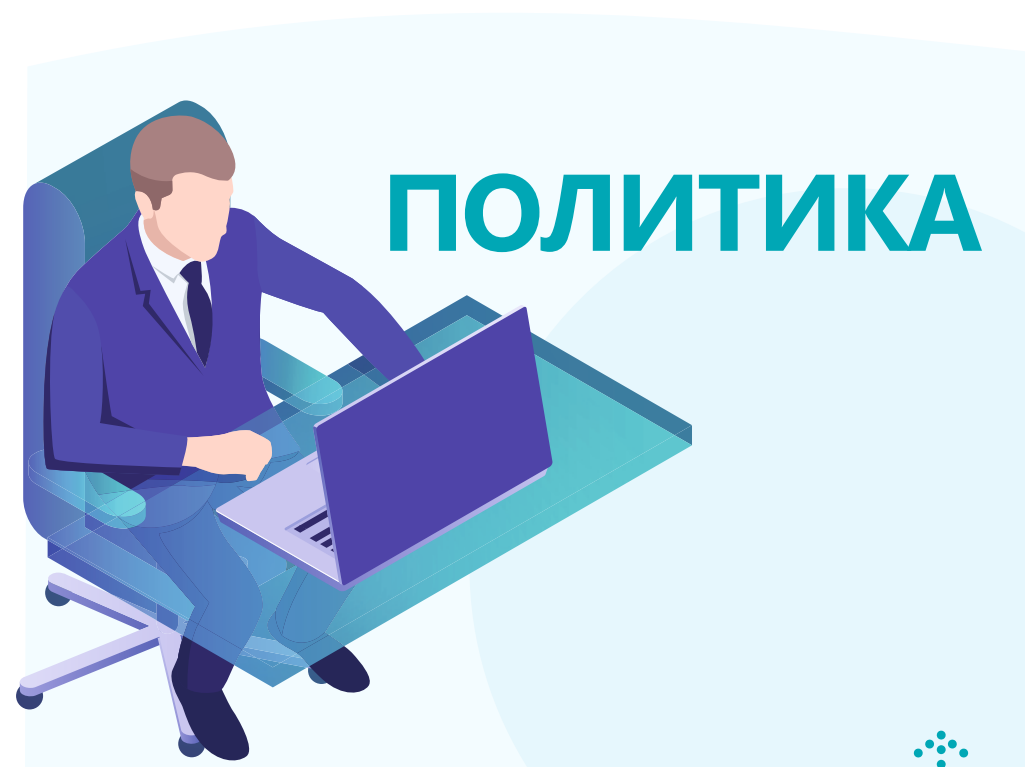
Порядок проведения мероприятий
или описание реализуемых
процессов по ЗИ применительно к
особенностям деятельности
оператора (обладателя
информации) и функционирования
ИС 17

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПОЗИ И УПРАВЛЕНИЕ ДАННОЙ ДЕЯТЕЛЬНОСТЬЮ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs



ИС / ИТ ИНФРАСТРУКТУРА

ДОГОВОР, ДОКУМЕНТЫ ОПЕРАТОРА

- Подрядные организации
- Подразделения (работники)

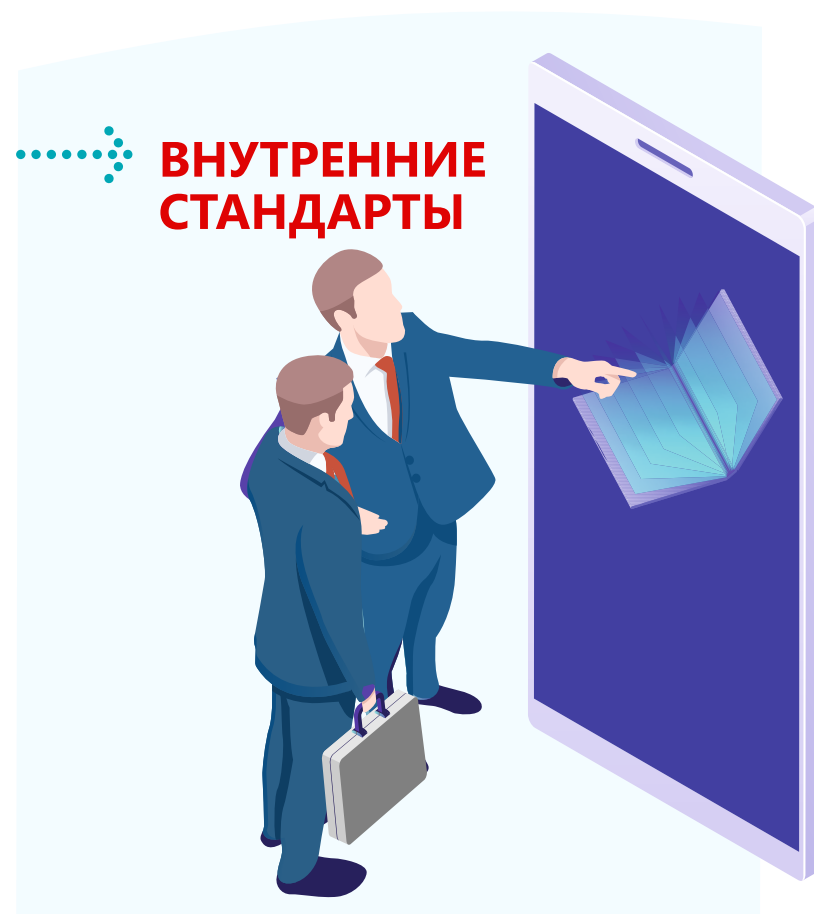
➔	ОБЛАСТЬ ДЕЙСТВИЯ
➔	ЦЕЛИ И ЗАДАЧИ
➔	ПРИНЦИПЫ
➔	ПЕРЕЧНИ ОБЪЕКТОВ ЗАЩИТЫ
➔	КАТЕГОРИИ ЛИЦ, ИХ ОБЯЗАННОСТИ И ПОЛНОМОЧИЯ
➔	СОСТАВ ОРГАНИЗАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ
➔	ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ЗИ И УПРАВЛЕНИЕ ДАННОЙ ДЕЯТЕЛЬНОСТЬЮ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs



ПРИКАЗ ФСТЭК РОССИИ 117

ЧТО НОВОГО? МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

ПРИКАЗ
ФСТЭК РОССИИ 17
14 ГРУПП

ПРИКАЗ
ФСТЭК РОССИИ 117
17 ГРУПП



- 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) обнаружение и предотвращение вторжений на сетевом уровне;
- о) сегментация и межсетевое экранирование;
- п) защита каналов передачи данных и сетевого взаимодействия

ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

КЛАСС	1	2	3
ВИД ТРЕБОВАНИЯ			
СВТ	5	5	5
СЗИ	4	5	6
УД	4	5	6
УРОВЕНЬ ВОЗМОЖНОСТЕЙ НАРУШИТЕЛЯ	ВЫСОКИЙ	ПОВЫШЕННЫЙ	БАЗОВЫЙ

П. 64 И П. 72 ПРИКАЗА ФСТЭК РОССИИ № 117

ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

||| ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ДОЛЖНЫ ПРИМЕНЯТЬСЯ СЕРТИФИЦИРОВАННЫЕ СЗИ В СООТВЕТСТВИИ С ИНСТРУКЦИЯМИ (ПРАВИЛАМИ) ПО ИХ ЭКСПЛУАТАЦИИ, УСТАНОВЛЕННЫМИ РАЗРАБОТЧИКАМИ В ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИИ.

||| ПРИМЕНЯЕМЫЕ СЗИ ДОЛЖНЫ БЫТЬ ОБЕСПЕЧЕНЫ СО СТОРОНЫ ИХ РАЗРАБОТЧИКОВ ПОДДЕРЖКОЙ БЕЗОПАСНОСТИ НА ТЕРРИТОРИИ РФ, ВКЛЮЧАЯ ВЫПУСК И ПРИМЕНЕНИЕ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ОБЕСПЕЧИВАЮЩИХ УСТРАНЕНИЕ ВЫЯВЛЕННЫХ УЯЗВИМОСТЕЙ, ДЕФЕКТОВ И НЕДОСТАТКОВ.

ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

ТРЕБОВАНИЯ К ПОДДЕРЖКЕ БЕЗОПАСНОСТИ СРЕДСТВА

УД

6

5

4

разработка компенсирующих мер по ЗИ или ограничений по применению средства, а также доведение информации о недостатках и указанных мерах и ограничениях до потребителей в часах с момента обнаружения

+

72 ч

48 ч

Об окончании производства и (или) поддержки безопасности средства, потребители и ФСТЭК России должны быть проинформированы не позднее чем

1 год



СИСТЕМЫ ТРЕБОВАНИЙ К СЗИ

ФСТЭК РОССИИ

ВИД СЗИ от **НСД**



Класс **Тип** **УД**

СВТ



СОВ



САВЗ

СДЗ



СКН



МЭ



ОС

УДАЛЕННЫЕ РМ

ВИРТУАЛИЗАЦИЯ

КОНТЕЙНЕРЫ

СУБД

NGFW

EDR

ФСБ РОССИИ

СКЗИ

КС1, КС2, КС3



КВ



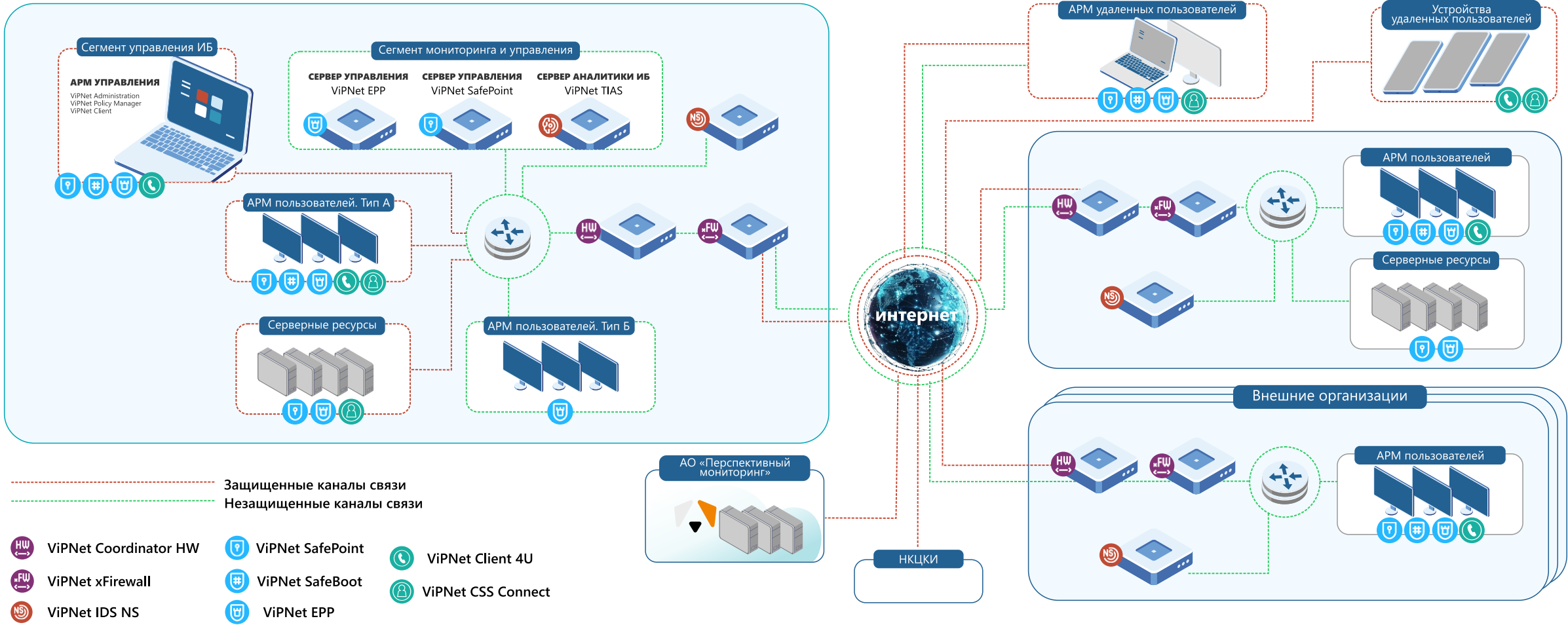
КА



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

СИСТЕМА ЗАЩИТЫ РАСПРЕДЕЛЕННЫХ ОБЪЕКТОВ



ПРИКАЗ ФСТЭК РОССИИ 117

ЧТО НОВОГО? МЕРОПРИЯТИЯ ПО ЗАЩИТЫ ИНФОРМАЦИИ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

ПРИКАЗ ФСТЭК РОССИИ 17 – 7

- а) выявление и оценка УБИ;
- б) контроль конфигураций ИС;
- в) управление уязвимостями;
- г) управление обновлениями;
- д) обеспечение ЗИ при обработке, хранении и обращении с информацией ограниченного доступа;
- е) обеспечение ЗИ при применении конечных устройств;
- ж) обеспечение ЗИ при применении мобильных устройств;
- з) обеспечение ЗИ при удаленном доступе пользователей к ИС;
- и) обеспечение ЗИ при беспроводном доступе пользователей к ИС;
- к) обеспечение ЗИ при предоставлении пользователям привилегированного доступа;
- л) обеспечение мониторинга ИБ;

ПРИКАЗ ФСТЭК РОССИИ 117–21

- м) обеспечение разработки безопасного ПО;
- н) обеспечение физической защиты ИС;
- о) обеспечение непрерывности функционирования ИС при возникновении нештатных ситуаций;
- п) повышение уровня знаний и информированности пользователей по вопросам ЗИ;
- р) обеспечение ЗИ при взаимодействии с подрядными организациями;
- с) обеспечение защиты от КА, направленных на отказ в обслуживании;
- т) обеспечение ЗИ при использовании ИИ;
- у) реализация в ИС мер по их защите и защите содержащейся в них информации;
- ф) проведение контроля уровня защищенности информации, содержащейся в ИС;
- х) обеспечение непрерывного взаимодействия с ГосСопкой на информационные ресурсы РФ

НОВОЕ

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

68. Мероприятия и меры по ЗИ, предусмотренные Требованиями, должны реализовываться оператором (обладателем информации) с использованием методических документов ФСТЭК России

п. 36 МУ	МЕТОДИКА ОЦЕНКИ УГРОЗ БИ, 05.02.2021
п. 39 Обновление ПО	МЕТОДИКА ТЕСТИРОВАНИЯ ОБНОВЛЕНИЙ ..., 28.10.2022
п. 38 Управление уязвимостями	РУКОВОДСТВО ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ..., 17.05.2023
	МЕТОДИКА ОЦЕНКИ УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ..., 30.06.2025
п. 31, 32 показатели Кзи Пзи	МЕТОДИКА ОЦЕНКИ ПОКАЗАТЕЛЯ СОСТОЯНИЯ ТЗИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗО КИИ РФ, 02.05.2024
	?
п. 68 Меры ЗИ	?
п. 65 Аттестация	МЕТОДИКА ИСПЫТАНИЙ СИСТЕМ ЗИ МЕТОДАМИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ, 25.06.2025

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

СООТВЕТСТВИЕ СТАНДАРТАМ

П. 23 МОНИТОРИНГ



разделы 4 и 5 ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения.»

П. 50 РАЗРАБОТКА БЕЗОПАСНОГО ПО



разделы 4 и 5 ГОСТ Р 59939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования.»

П. 42, 46, 48, СТРОГАЯ АУТЕНТИФИКАЦИЯ



П. 3.54 ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие требования.»

Аутентификация с применением только метода многофакторной взаимной аутентификации и использованием криптографических протоколов аутентификации.

НАПРАВЛЕНИЕ ИНФОРМАЦИИ ВО ФСТЭК РОССИИ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

ПУНКТ ПРИКАЗА	ЧТО ОТПРАВЛЯЕМ	ПЕРИОДИЧНОСТЬ (НЕ РЕЖЕ)	СРОК
32	Оценка показателя защищенности Кзи	1 раз/6 месяцев	5 раб. дней
32, 73	Оценка показателя уровня зрелости Пзи	1 раз/2 года	5 раб. дней
36	МУ (ТЗ) ссылка на ПП РФ 676 (только для ГИС)	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

НАПРАВЛЕНИЕ ИНФОРМАЦИИ ВО ФСТЭК РОССИИ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

ПУНКТ ПРИКАЗА	ВНУТРЕННИЙ ПРОЦЕСС	ПЕРИОД
38	Устранение уязвимостей	от 24 ч до 7 к/дней
53	Восстановление функционирования	от 24 ч до 4 недель
55	Проверка возможности восстановления выполнения значимых функций с использованием резервных копий	1/ 2 года
57	Оценка уровня знаний	1/ 3 года или после КИ

СОЗДАНИЕ ЭФФЕКТИВНЫХ СИСТЕМ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs



СОЗДАНИЕ ЭФФЕКТИВНЫХ СИСТЕМ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs



Мотивация



Условия



Квалификация



ПОВЫШЕНИЕ КВАЛИФИКАЦИИ
И ПЕРЕПОДГОТОВКА

<https://infotecs-edu.ru/>



КИБЕРУЧЕНИЯ

<https://amonitoring.ru/product/ampire/>



КИБЕРПОЛИГОН AMPIRE

— это виртуальная инфраструктура предприятия, на которую проводятся компьютерные атаки по разным векторам



**ПРАКТИЧЕСКАЯ
НАПРАВЛЕННОСТЬ**



**АВТОМАТИЧЕСКИЙ
АТАКУЮЩИЙ**



**РАЗНООБРАЗНЫЕ
СЦЕНАРИИ АТАК**



**ПОДКЛЮЧЕНИЕ
К ГОССОПКА**

РЕГУЛЯТОРИКА: РОСТ ЦЕНЫ ОШИБКИ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

КоАП 13.11



За ПДн специальных
категорий до **15 МЛН.РУБ.**

КоАП 13.12



За нарушение правил защиты
информации до **100 ТЫС. РУБ.**

ЧЕК-ЛИСТ ДЕЙСТВИЙ ПОСЛЕ ВЕБИНАРА

Информационная безопасность 2.0



**ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

Чек-лист

1. АНАЛИЗ ТЕКУЩЕЙ ИНФРАСТРУКТУРЫ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

 **infotecs**



Провести аудит существующих систем защиты



Проверить соответствие текущих мер требованиям приказа



Оценить уровень защищенности информационных систем

2. ОРГАНИЗАЦИОННЫЕ МЕРЫ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

 **infotecs**



Создать рабочую группу по внедрению новых требований



Разработать план перехода на новые стандарты



Определить ответственных за реализацию каждого пункта



Составить график выполнения работ

3. ТЕХНИЧЕСКИЕ РЕШЕНИЯ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

 **infotecs**



Обновить документацию по защите информации



Проверить актуальность используемых средств защиты



Составить список необходимого дополнительного ПО



Планировать интеграцию новых решений

4. РАБОТА С ПЕРСОНАЛОМ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

 **infotecs**



Организовать обучение сотрудников новым требованиям



Разработать инструкции по работе в новых условиях



Провести тренинги по реагированию на инциденты



Обновить регламенты информационной безопасности

5. КОНТРОЛЬ И МОНИТОРИНГ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

 **infotecs**



Настроить систему мониторинга соответствия требованиям



Определить метрики для оценки эффективности



Создать план регулярных проверок



Организовать систему отчетности

6. ВЗАИМОДЕЙСТВИЕ С ПОДРЯДЧИКАМИ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs



Проверить договоры на соответствие новым требованиям



Обновить соглашения с поставщиками услуг



Провести аудит подрядных организаций



Определить требования к партнерам по ИБ

7. БЮДЖЕТИРОВАНИЕ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

 **infotecs**



Составить смету необходимых затрат



Планировать этапы внедрения с учетом бюджета



Определить приоритетные направления расходов



Заложить средства на сопровождение

8. ДОКУМЕНТАЦИЯ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

 **infotecs**



Обновить политику информационной безопасности



Составить новые регламенты



Подготовить приказы и распоряжения



Вести учет всех изменений

9. ТЕСТИРОВАНИЕ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

 **infotecs**



Провести пилотное внедрение



Проверить работоспособность новых решений



Оценить влияние на бизнес-процессы



Собрать обратную связь от пользователей

10. ОТЧЕТНОСТЬ



ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs



Подготовить документы для регуляторов



Составить внутренние отчеты о выполнении требований



Организовать систему учета инцидентов



Вести журнал изменений в системе защиты

 **infotecs**



**ПОДПИСЫВАЙТЕСЬ
НА НАШИ
СОЦ.СЕТИ**





**ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**



**ПОДПИСЫВАЙТЕСЬ
НА НАШИ
СОЦ.СЕТИ**



БЛАГОДАРИМ ЗА УЧАСТИЕ!

Надеемся, материал был полезен и вы сможете применить его в работе.

До новых встреч!

