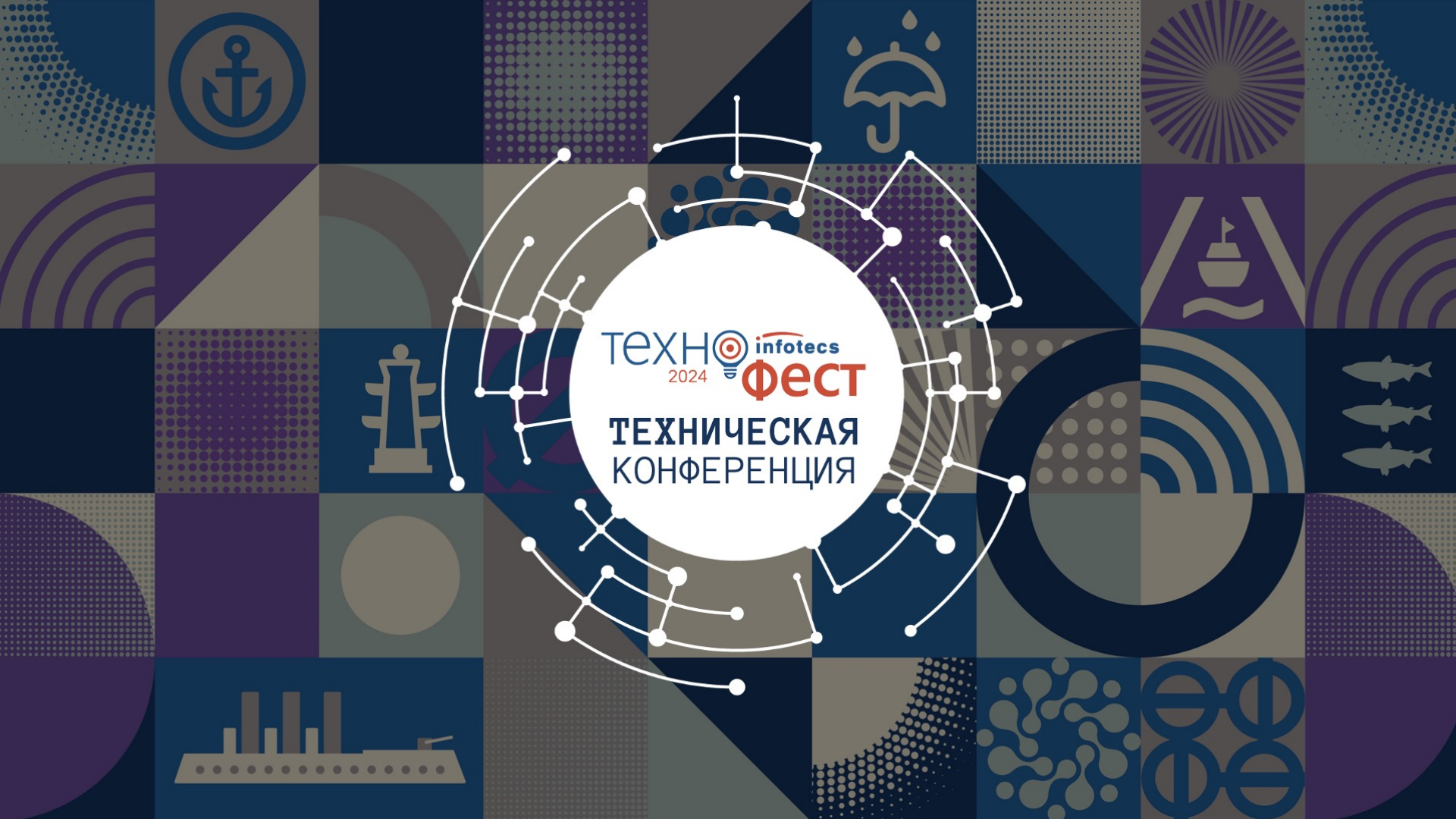

ТЕХНО
2024
infotecs
ФЕСТ
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Защита информации на объекте КИИ. Рациональный подход и реалии субъектов.

Петров Андрей
руководитель центра мониторинга и реагирования
на инциденты информационной безопасности – начальник
отдела аттестаций и разработки документов ООО «Инфолайн»

Категорирование объектов КИИ. Этапы работ.

Подготовительные работы по категорированию

- ✓ Определение принадлежности к субъектам КИИ
- ✓ Создание комиссии по категорированию, назначение ответственных
- ✓ Инвентаризация процессов и выявление критичных процессов
- ✓ Формирование перечня ОКИИ, подлежащий категорированию

Мероприятия проводимые при категорировании

- ✓ Анализ возможных источников угроз и действий нарушителя
- ✓ Анализ возможных угроз безопасности
- ✓ Оценка возможных последствий (масштабов) от реализации компьютерных атак и сопоставление с показателями значимости (ПП-127)
- ✓ Присвоение категории

Включение в перечень объектов КИИ (ФСТЭК)

ФСТЭК России проводит работы по проверке, учету и ведению реестра (перечня) объектов КИИ

Категорирование объектов КИИ. Этапы работ.

Что такое процесс и какова степень его детализации

Подразделение нижнего уровня

=

Процесс

функции подразделений = процесс

Если сомневаетесь то включайте все процессы. На поздних стадиях анализа большинство процессов будет отсеяна

Результат:

Перечень всех процессов субъекта КИИ

Категорирование объектов КИИ. Этапы работ.

Что такое процесс и какова степень его детализации

Все функции организации:

- Документооборот;
- Административно-хозяйственные;
- Планово-финансовая деятельность;
- Проведение претензионной работы с должниками;
- Заключение, изменение, расторжение договоров

Если сомневаетесь то включайте все процессы. На поздних стадиях анализа большинство процессов будет отсеяна

Результат:

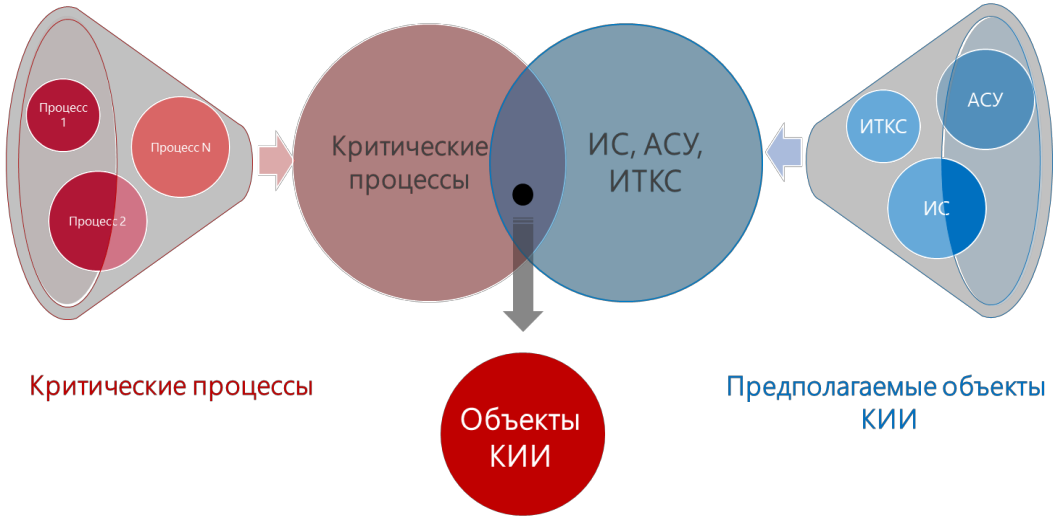
Перечень всех процессов субъекта КИИ

Категорирование объектов КИИ. Этапы работ.

Что значит детализация

Категорирование объектов КИИ. Этапы работ.

Формирование перечня объектов КИИ

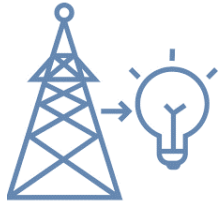


Результат:

Перечень объектов КИИ подлежащих категорированию

Категорирование объектов КИИ. Этапы работ.

Формирование перечня объектов КИИ

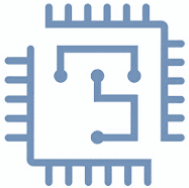


Энергетика

- SCADA промышленные контроллеры;
- интеллектуальные счетчики.
- системы автоматизированного учета электроэнергии

Здравоохранение

- лабораторные анализаторы;
- рентгеновское оборудование;
- оборудование УЗИ;
- мониторы пациентов.



Промышленность

- SCADA промышленные контроллеры;
- технологическое оборудование;
- автоматизированные линии.

ИТКС

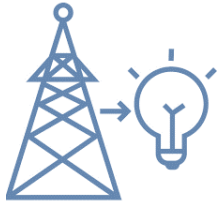
Информационная система ИС

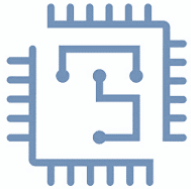
Автоматизированная система управления АСУ

Информационно-телекоммуникационная сеть ИТКС

Категорирование объектов КИИ. Этапы работ.

Формирование перечня объектов КИИ





Энергетика

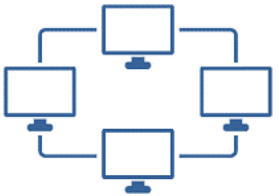
- SCADA промышленные контроллеры;
- интеллектуальные счетчики.
- систем автоматизированного учета электроэнергии

Здравоохранение

- лабораторные анализаторы;
- рентгеновское оборудование;
- оборудование УЗИ;
- мониторы пациентов.

Промышленность

- SCADA промышленные контроллеры;
- технологическое оборудование;
- автоматизированные линии.



ИТКС

Информационная система ИС

Автоматизированная система управления АСУ

Информационно-телекоммуникационная сеть ИТКС

Категорирование объектов КИИ. Этапы работ.

Дополнительные материалы (документы) по категорированию

- ✓ Методические рекомендации по категорирование объектов критической информационной инфраструктуры от компании STEP Logic, 2019;
- ✓ «Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта», согласовано с ФСТЭК 05.05.2023;
- ✓ Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи. Согласовано с ФСТЭК и ФСБ, 2019;
- ✓ «Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения», Министерство здравоохранения РФ, 05.04.2021;
- ✓ «Методические рекомендации по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической информационной инфраструктуры на объектах информатизации медицинских организаций для учреждений государственной системы здравоохранения Московской области», Министерство здравоохранения Московской области, 2020.

Построение системы защиты информации на объекте КИИ.

Организационные меры:

силы (кадры);

документы.

Технические меры:

средства защиты информации.

[НСД] [МЭ] [СОВ] [АВЗ] [АНЗ] [СКЗИ]

Кадровое обеспечение субъектов КИИ.

Требования к специалистам обеспечивающим ИБ на объектах КИИ

- ✓ Приказ ФСТЭК от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»;
- ✓ Приказ ФСТЭК от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»;
- ✓ Постановление Правительства РФ от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя организации, ответственном за обеспечение информационной безопасности в организации, и типового положения о структурном подразделении в организации, обеспечивающем информационную безопасность организации».

Наличие высшего профильного образования по ИБ:
Специалитет или магистратура (не бакалавриат).
Специальности «Компьютерная безопасность», «Информационная безопасность», «ИБ в телекоммуникационных сетях», «ИБ АС», «Информационно-аналитические системы безопасности».
или профессиональная переподготовка:
Приказ Министерства образования и науки РФ №1316 от 19.10.2020 «Требования к программам переподготовки по ЗИ…».
Минимальный срок программы профессиональной подготовки не менее 360 академических часов;
Программа обучения должна быть согласована с ФСТЭК.

Кадровое обеспечение субъектов КИИ.

Требования к специалистам обеспечивающим ИБ на объектах КИИ

Как выполнить? Стратегия.

Вариант 1: Повысить руководителя ИБ подразделения до уровня заместителя по ИБ:
Требуется повышение компетенций и управленческих навыков.

Вариант 2: Переподготовить (переобучить) имеющегося или назначаемого заместителя по ИБ
Перечень образовательных организаций: Сайт ФСТЭК → раздел «Техническая ЗИ» → «Обучение специалистов» → Перечень организаций осуществляющих образовательную деятельность;

Организационные меры по ИБ на объектах КИИ.

Разработка организационно-распорядительных документов

Требования нормативных документов:.

- ✓ Федеральный закон от 26.07.2017 № 187-ФЗ;
- ✓ Постановление Правительства РФ от 08.02.2018 г. № 127 ;
- ✓ Постановление Правительства РФ от 15.07.2022 № 1272;
- ✓ Указ Президента РФ от 01.05.2022 № 250;
- ✓ Приказ ФСТЭК от 21.12.2017 № 235;
- ✓ Приказ ФСТЭК от 25.12.2017 № 239;
- ✓ Приказ ФСБ от 19.06.2019 №281;
- ✓ Приказ ФСБ от 19.06.2019 №282;
- ✓ …

Организационные меры по ИБ на объектах КИИ.

Разработка организационно-распорядительных документов

№ п/п	Наименование документа	Основание для разработки документа	Процесс управления или обеспечения ИБ
	Категорирование объектов КИИ		
1.	Приказ о создании Комиссии по категорированию объектов критической информационной инфраструктуры	п.11 ПП № 127	категорирование
2.	Положение о Комиссии по категорированию объектов критической информационной инфраструктуры	п.11-14, ПП № 127	категорирование
3.	Заключение о наличии критических процессов и объектов критической информационной инфраструктуры	п.14 ПП № 127	категорирование
4.	Перечень объектов критической информационной инфраструктуры	п.15 ПП № 127	категорирование
5.	Модель угроз и нарушителя безопасности информации значимого объекта критической информационной инфраструктуры	п.п. Г.Д п.14, ПП № 127; п.11.1 приказа ФСТЭК № 239	категорирование
6.	Акт категорированию объекта критической информационной инфраструктуры	п.16 ПП № 127	категорирование
7.	Сведения о категорировании объекта критической информационной инфраструктуры	п. 17 ПП № 127; приказ ФСТЭК № 236	категорирование

Организационные меры по ИБ на объектах КИИ.

Разработка организационно-распорядительных документов

№ п/п	Наименование документа	Основание для разработки документа	Процесс управления или обеспечения ИБ
Предпроектная и проектная документация			
8.	Частное техническое задание на создание подсистемы обеспечения безопасности информации значимого объекта критической информационной инфраструктуры. С приложениями:	п.10 приказа ФСТЭК № 239	проектирование
9.	Перечень мер по обеспечению безопасности информации на значимом объекте критической информационной инфраструктуры	п.23 приказа ФСТЭК № 239	проектирование
10.	Протокол анализа уязвимостей значимого объекта критической информационной инфраструктуры	п.12.6 приказа ФСТЭК № 239	испытание и приемка
11.	Акт приемки значимого объекта критической информационной инфраструктуры в эксплуатацию.	п.12.7 приказа ФСТЭК № 239	испытание и приемка

Организационные меры по ИБ на объектах КИИ.

Разработка организационно-распорядительных документов

Организационные меры по обеспечению безопасности информации значимого объекта критической информационной инфраструктуры			
10.	**Положение об обеспечении безопасности значимого объекта критической информационной инфраструктуры. В составе следующих разделов:**	п.п. а),б),в) п.25 приказа ФСТЭК №235, п.33 приказа ФСТЭК №235, п.п.. в) Приказа ФСТЭК № 239	Политики информационной безопасности
	Порядок реализации мер по обеспечению безопасности информации на значимом объекте критической информационной инфраструктуры	п.12.2 приказа ФСТЭК № 239; п. п. б) п.25 приказа ФСТЭК № 235	Защита системы
	Планирование мероприятий по обеспечению безопасности информации на значимом объекте критической информационной инфраструктуры	Меры ПЛН.0 приказа ФСТЭК № 239	Планирование
	Информирование и обучение персонала значимого объекта критической информационной инфраструктуры по вопросам обеспечения безопасности информации	Мера ИПО.0 приказа ФСТЭК № 239. п.13.7 ФСТЭК №239; п.п.б) п.25 ФСТЭК № 235	Ознакомление и обучение
	Обеспечение целостности информационных ресурсов значимого объекта критической информационной инфраструктуры	Мера ОЦЛ.0 приказа ФСТ ЭК № 239	Защита системы
	Обеспечение доступности информационных ресурсов значимого объекта критической информационной инфраструктуры	Мера ОДТ.0 приказа ФСТЭК № 239	Защита системы
	Политика обеспечения конфиденциальности информационных ресурсов значимого объекта критической информационной инфраструктуры		Защита системы
	Защита компонентов значимого объекта критической информационной инфраструктуры	Мера ЗИС.0 приказа ФСТЭК № 239	Защита системы
	Идентификация и аутентификация субъектов и объектов доступа значимого объекта критической информационной инфраструктуры	Мера ИАФ.0 приказа ФСТЭК № 239	Управление доступом
	Управление доступом к информационным ресурсам значимого объекта критической информационной инфраструктуры	Мера УПД.0 приказа ФСТЭК № 239	Управление доступом
	Ограничение программной среды на средствах вычислительной техники значимого объекта критической информационной инфраструктуры	Мера ОПС.0 приказа ФСТЭК № 239	Управление доступом
	Защита машинных носителей информации на значимом объекте критической информационной инфраструктуры. Учет, хранение, обращение и уничтожение машинных носителей	Мера ЗНИ.0 приказа ФСТЭК № 239	Управление активами

Организационные меры по ИБ на объектах КИИ.

Разработка организационно-распорядительных документов

Организационные меры по обеспечению безопасности информации значимого объекта критической информационной инфраструктуры			
	Антивирусная защита информационных ресурсов значимого объекта критической информационной инфраструктуры	Мера АВЗ.0 приказа ФСТЭК № 239	Антивирусная защита
	Предотвращение вторжений (компьютерных атак) на значимый объект критической информационной инфраструктуры	Мера СОВ.0 приказа ФСТЭК № 239	Обнаружение вторжений
	Защита технических средств и систем значимого объекта критической информационной инфраструктуры	Мера ЗТС.0 приказа ФСТЭК № 239	Защита технических средств
	Управление конфигурацией технических средств и систем значимого объекта критической информационной инфраструктуры	Мера УКФ.0 приказа ФСТЭК № 239	Конфигурации
	Управление обновлениями программного обеспечения применяемого на значимом объекте критической информационной инфраструктуры	Мера ОПО.0 приказа ФСТЭК № 239	Обновления ПО
	Реагирование на инциденты информационной безопасности и принятия мер по ликвидации их последствий	Мера ИНЦ.0 приказа ФСТЭК № 239; п.п. б) п.25 приказа ФСТЭК № 235	Инциденты
	Действия в нештатных ситуациях (в том числе вызванных инцидентами информационной безопасности)	Мера ДНС.0 приказа ФСТЭК № 239; п.12.2 ФСТЭК №239; п.п. а) п.13.6 приказа ФСТЭК №239	Инциденты
	Взаимодействие подразделений при решении задач обеспечения безопасности информации на значимом объекте критической информационной инфраструктуры	п.п. б) п.25 приказа ФСТЭК № 235	Взаимодействие
	Порядок проведения аудита безопасности информации на значимом объекте критической информационной инфраструктуры	Мера АУД.0 приказа ФСТЭК № 239, п. 36 Приказа ФСТЭК №235	Контроль
	Контроль выполнения мероприятий по обеспечению безопасности информации на значимом объекте критической информационной инфраструктуры	п.п. в) п.13.1 приказа ФСТЭК № 239; п.п. в) п.13.8 приказа ФСТЭК № 239	Планирование

Организационные меры по ИБ на объектах КИИ.

Разработка организационно-распорядительных документов

11.	Инструкция по учету, хранению, обращению и уничтожению машинных носителей защищаемой информации	Мера ЗНИ.1 приказа ФСТЭК № 239 (пп.5 п.2 ст.19 ФЗ-152)	Управление активами
12.	Приказ о распределении ответственности за обеспечение безопасности информации на значимом объекте критической информационной инфраструктуры (назначение ответственного за организацию работ по обеспечению безопасности информации, назначение подразделения и/или лица ответственного за обеспечение безопасности информации, а также администраторов информационной безопасности)	п.10 приказа ФСТЭК № 235; п.п. г), п. 12.3 приказа ФСТЭК № 239	Ответственность
13.	Должностная инструкция лица ответственного за организацию работ по обеспечению безопасности информации на значимом объекте критической информационной инфраструктуры;	п.13 приказа ФСТЭК № 235	Ответственность
14.	Должностная инструкция лица ответственного за обеспечение безопасности информации на значимом объекте критической информационной инфраструктуры	п.13 приказа ФСТЭК № 235	
15.	Положение о подразделении ответственного за обеспечение безопасности информации на значимом объекте критической информационной инфраструктуры	п.10, п.12, п.13, п.14 приказа ФСТЭК № 235	Ответственность
16.	План мероприятий по обеспечению безопасности информации на значимом объекте критической информационной инфраструктуры (ежегодный)	п.13.1 приказа ФСТЭК № 239; п.п. б) п.25 приказа ФСТЭК № 235; п.29 приказа ФСТЭК № 235	Планирование
17.	Отчет о выполнении плана мероприятий по обеспечению безопасности информации на значимом объекте критической информационной инфраструктуры	п.32 приказа ФСТЭК № 235	Планирование
18.	Приказ о создании Комиссии по контролю состояния обеспечения безопасности информации на значимом объекте критической информационной инфраструктуры	п.36 приказа ФСТЭК № 235	Контроль
19.	Заключение (акт оценки) по результатам контроля выполнения принятых организационных и технических мер по обеспечению безопасности информации на значимом объекте критической информационной инфраструктуры	п.п. в) п.13.8 приказа ФСТЭК № 239; п.36 приказа ФСТЭК № 235	Контроль
20.	Приказ «Об установлении границ контролируемой зоны»	Мера ЗТС.2 приказа ФСТЭК № 239	Защита ТС
21.	Приказ «О создании системы безопасности на значимом объекте критической информационной инфраструктуры» (утверждение организационных и технических мер)	п.9 приказа ФСТЭК № 239	

Организационные меры по ИБ на объектах КИИ.

Разработка организационно-распорядительных документов

22.	Регламент взаимодействия субъекта критической информационой инфраструктуры с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА)	п.п. б) п.25 приказа ФСТЭК № 235, п.2 приложения 1 к приказу ФСБ №368, п.4 приложения 2 к приказу ФСБ №368, п. 5 и 9 приложения 2 к приказу ФСБ № 367	Инциденты
23.	План действий в нештатных ситуациях при работе значимого объекта критической информационной инфраструктуры	Мера ДНС.1 приказа ФСТЭК № 239. п.12.2 ФСТЭК № 239; п. п. а) п.13.6 приказа ФСТЭК № 239	Инциденты
24.	Журнал ознакомления сотрудников субъекта критической информационной инфраструктуры с организационно-распорядительными документами по обеспечению безопасности информации значимого объекта критической информационной инфраструктуры	п.15 приказа ФСТЭК № 235; п.27 приказа ФСТЭК № 235	Ознакомление и обучение
25.	Журнал ознакомления подрядчиков субъекта критической информационной инфраструктуры с организационно-распорядительными документами по обеспечению безопасности информации значимого объекта критической информационной инфраструктуры	п.16 приказа ФСТЭК № 235	Ознакомление и обучение
26.	Журнал проведения инструктажа по вопросам обеспечения безопасности информации на значимом объекте критической информационной инфраструктуры	п.15 приказа ФСТЭК № 235	Ознакомление и обучение
27.	Правила безопасной работы при эксплуатации значимого объекта критической информационной инфраструктуры	п.12.2 приказа ФСТЭК № 239; п.15 приказа ФСТЭК № 235; п.п.в) п.25 приказа ФСТЭК № 235	Эксплуатация объекта КИИ

Организационные меры по ИБ на объектах КИИ.

Разработка организационно-распорядительных документов

Как разработать? Возникающие трудности.

1. Знание большого количества нормативной документации;
2. Требуется много (очень много) рабочего времени.

Способ преодолеть возникающие трудности.

1. Выделенные специалист по организационным мерам в составе подразделения по обеспечению безопасности информации объекта КИИ;
2. Разработка документов с привлечением компании – лицензиата ФСТЭК (аутсорсинг).

Организационные меры по ИБ на объектах КИИ.

Разработка организационно-распорядительных документов

Как разработать? Возникающие трудности.

1. Знание большого количества нормативной документации;
2. Требуется много (очень много) рабочего времени.

Не забудьте ознакомить с документами сотрудников !!!

Способ преодолеть возникающие трудности.

1. Выделенные специалист по организационным мерам в составе подразделения по обеспечению безопасности информации объекта КИИ;
2. Разработка документов с привлечением компании – лицензиата ФСТЭК (аутсорсинг).

Технические меры по ИБ на объектах КИИ.

Подбор средств защиты информации (СЗИ)

Вопросы подбора и внедрения СЗИ.

1. Стоимость;
2. Совместимость с используемым ПО и СВТ;
3. Наличие действующих сертификатов ФСТЭК и/или ФСБ.

[НСД] [МЭ] [СОВ] [АВЗ] [АНЗ] [СКЗИ]

Требования по подбору и внедрению СЗИ.

1. Разработка частного технического задания на подсистему защиты (протокол подбора СЗИ);
2. Проект на подсистему защиты информации.

разработка по ГОСТам 34 серии

ГОСТ 34

Технические меры по ИБ на объектах КИИ.

Подбор средств защиты информации (СЗИ)

Вопросы оптимизации подбора и внедрения СЗИ.

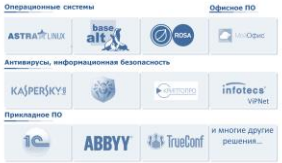
1. п. 28 Приказа ФСТЭК № 239. Использование не сертифицированных СЗИ (необходимо самостоятельно провести их испытание и приемку);
2. использование встроенных СЗИ и использование функции безопасности встроенных в применяемое программное обеспечение;
3. включать в ТЗ на разработку/доработку программного обеспечения требования к совместимости с новыми версиями отечественного системного и прикладного программного обеспечения.

Технические меры по ИБ на объектах КИИ.

Дополнительные требования к СВТ и СЗКИ. Импортозамещение.

Отечественные: средства вычислительной техники, программное обеспечение, средства защиты информации

СВТ



ПО

СЗИ

СДЕЛАНО В РОССИИ

Технические меры по ИБ на объектах КИИ.

Дополнительные требования к СВТ и СЗКИ. Импортозамещение.

Отечественные: средства вычислительной техники, программное обеспечение, средства защиты информации?

ОТЕЧЕСТВЕННЫЕ РЕШЕНИЯ

- Проблемы совместимости с эксплуатируемым ПО;
- Иногда, более низкая производительность;
- Отсутствие наработанных кейсов по технической поддержке.

ЗАРУБЕЖНЫЕ РЕШЕНИЯ

- Проблемы с обновлениями;
- Проблемы с закрытием уязвимостей;
- Отсутствие технической поддержки;
- «Заградительные» меры со стороны государства.

Так брать или не брать?

Технические меры по ИБ на объектах КИИ.

Дополнительные требования к СВТ и СЗКИ. Импортозамещение.

	Приказ ФСТЭК 235	Приказ ФСТЭК 239	Указ Президента РФ № 250	Указ Президента РФ № 166	Постановление Правительства РФ № 1912
СВТ	Нет требований по происхождению	Нет требований по происхождению	Нет требований по происхождению	Преимущественное применение российских СВТ	**ЗАПРЕТ с 01.09.2024**
ПО	Нет требований по происхождению	Нет требований по происхождению	Нет требований по происхождению	**ЗАПРЕТ закупать для владельцев ЗО КИИ закупающих по 223-ФЗ. ЗАПРЕТ с 01.01.2025 для ОГВ**	**ЗАПРЕТ с 01.09.2024**
СЗИ	Нет требований по происхождению Возможно ограничение! Требование наличия технической поддержки	Нет требований по происхождению Возможно ограничение! Требование сертификации (в случаях предусмотренных законом)	**ЗАПРЕТ эксплуатации с 01.01.2025**	Нет требований по происхождению	**ЗАПРЕТ с 01.09.2024**

Технические меры по ИБ на объектах КИИ.

Дополнительные требования по ИБ. Мониторинг ИБ.

Приказ ФСТЭК от 25.12.2017 № 239 : меры АУД, ИНЦ и др.

Приказ ФСБ от 19.06.2019 №281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»;

Приказ ФСБ от 19.06.2019 №282 «Об утверждении Порядка информирования ФСБ России о КИ, реагирования на них, принятия мер по ликвидации последствий КА, проведенных в отношении ЗО КИИ РФ.

Технические меры по ИБ на объектах КИИ.

Дополнительные требования по ИБ. Мониторинг ИБ.

Приказ ФСБ от 19.06.2019 №282 «Об утверждении Порядка информирования ФСБ России о КИ, реагирования на них, принятия мер по ликвидации последствий КА, проведенных в отношении ЗО КИИ РФ.

Информация о компьютерном инциденте, связанном с функционированием значимого объекта критической информационной инфраструктуры, **направляется** субъектом критической информационной инфраструктуры **в НКЦКИ** в **срок не позднее 3 часов** с момента обнаружения компьютерного инцидента, а в отношении иных объектов критической информационной инфраструктуры - в срок не позднее 24 часов с момента его обнаружения

Направить план после утверждения в НКЦКИ в течении 7 календарных дней

ГОССОПКА
Обнаружение. Предупреждение. Ликвидация.

Направить в НКЦКИ в течении **3** часов с момента обнаружения инцидента

Для подготовки к реагированию на КИ и принятию мер по ликвидации последствий КА субъектом КИИ, которому на праве собственности, аренды или ином законном основании принадлежит ЗО КИИ, в срок до 90 календарных дней со дня включения данного объекта в реестр ЗО КИИ РФ разрабатывается **план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак**.

Технические меры по ИБ на объектах КИИ.

Дополнительные требования по ИБ. Мониторинг ИБ.

Выявление и реагирование на инциденты информационной безопасности.

Силы мониторинга (выявления инцидентов ИБ)
SOC (Security Operations Center)

- Собственный (ведомственный) SOC;
- Внешний(корпоративный) SOC.

Силы реагирования (устранения последствий)
CSIRT (Computer Security Incident Response Team)

- Собственные силы реагирования.

Технические меры по ИБ на объектах КИИ.

Эксплуатация объекта КИИ. Планирование контроль ответственность.
Информационная безопасность — это процесс!

Суть требований НПА:
После создания (внедрения) системы ИБ на объекте КИИ, ее необходимо поддерживать в актуальном состоянии и совершенствовать.

Поддержка в актуальном состоянии документов:
- Своевременное внесение изменений в технический паспорт;
- Периодический пересмотр уровня защищенности / класса защищенности;
- Рассмотрение новых угроз безопасности информации. Внесение изменений в Модели угроз и нарушителя;
- Внесение изменений в Техническое задание на создание ПОИБ ИС;
- Актуализация организационно-распорядительной документации на объект КИИ.

…

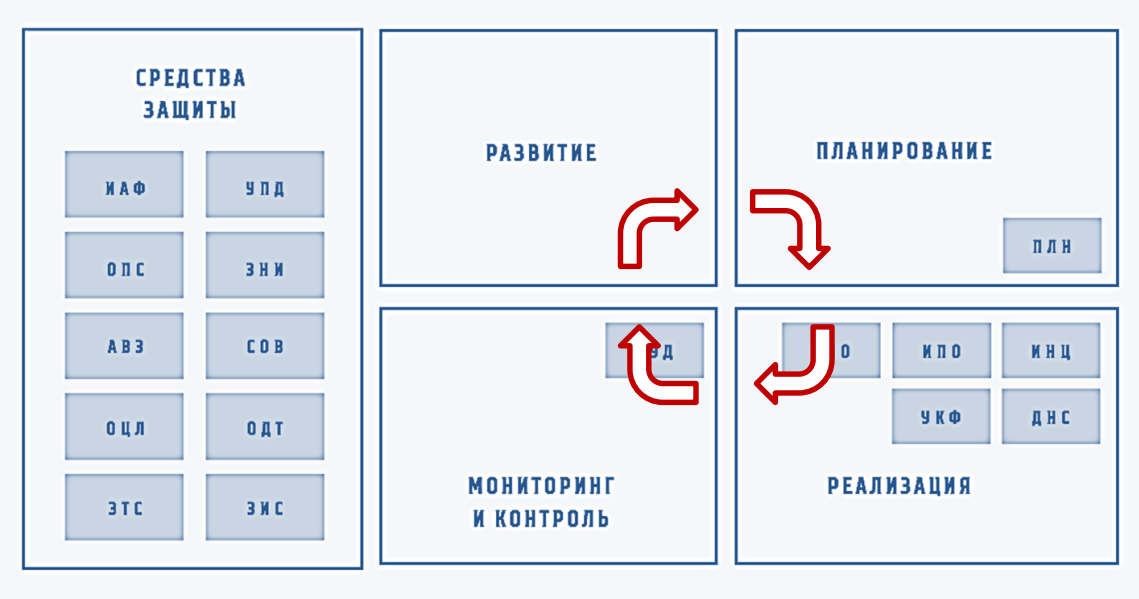
Техническая защита информации. Поддержка СЗИ:
- Периодический анализ защищенности (поиск уязвимостей);
- Техническая поддержка;
- Настройка СЗИ;
- Контроль работоспособности СВТ и СЗИ;
- Мониторинг событий ИБ в ИС.

Технические меры по ИБ на объектах КИИ.

Эксплуатация объекта КИИ. Планирование контроль ответственность.
Информационная безопасность — это процесс!

4 блока:

1. Планирование;
2. Реализация;
3. Контроль и мониторинг;
4. Развитие.



Спасибо за внимание!

E-mail: office@infoline-rk.ru

Тел: (8 8142) 77-20-20