КСБ-СОФТ

Ответы на насущные вопросы по информационной безопасности объектов КИИ

Спикер:

- **Шляпкин Максим –** начальник отдела защиты объектов КИИ и АСУ ТП, КСБ-СОФТ

Модератор:

- **Ильин Александр –** руководитель регионального направления, КСБ-СОФТ

«КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

80+
регионов внедрения

4000+
реализованных проектов

Портфолио КСБ-СОФТ

Обменивайтесь сообщениями во вкладке «Чат»

Запись вебинара направим Всем участникам на указанный при регистрации e-mail

Задавайте вопросы во вкладке «Вопросы»

План вебинара

- Новая Методика ФСТЭК России по оценке показателя состояния технической защиты информации и обеспечения безопасности ЗОКИИ РФ
- Повышение осведомленности персонала в части ИБ КИИ
- Первоочередные меры по ИБ для защиты ЗОКИИ
- Зачем защищать незначимые объекты КИИ
- Категорирование объектов КИИ (понижение ошибочно присвоенной категории значимости, формирование обоснований показателей критериев значимости и т.д.)
- Ответы на дополнительные вопросы

Наградим авторов 3 лучших вопросов фирменным мерчем!

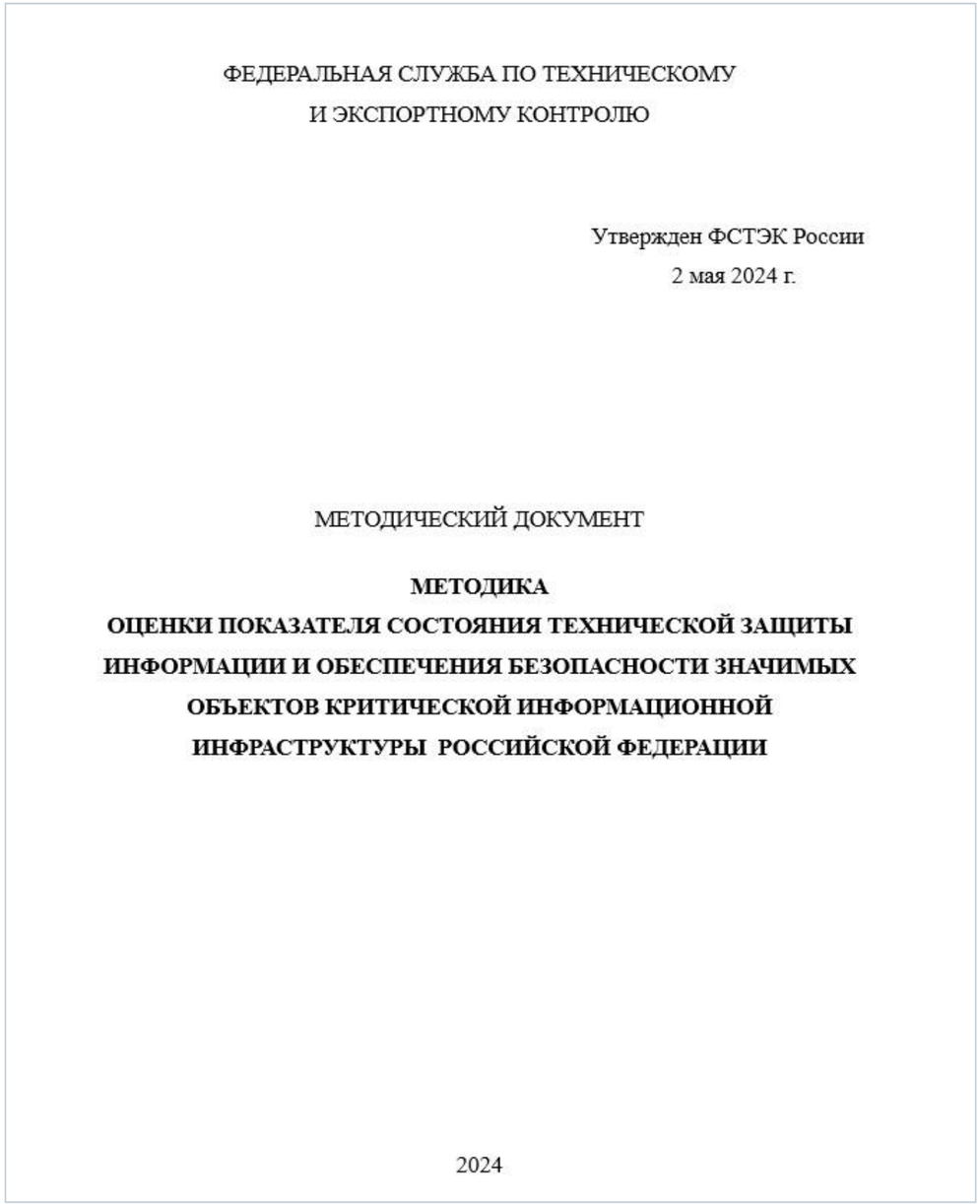
Цикл вебинаров, посвященных вопросам ИБ в КИИ

Если Вы хотите, чтобы мы подробно разобрали Ваш вопрос на следующем вебинаре, задавайте вопрос по ссылке:

Ответы на вопросы

Вопрос № 1

Нужно ли организациям, не являющимся субъектами КИИ, обязательно выполнять требования новой методики ФСТЭК России по оценке показателя технической защищенности?



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 ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

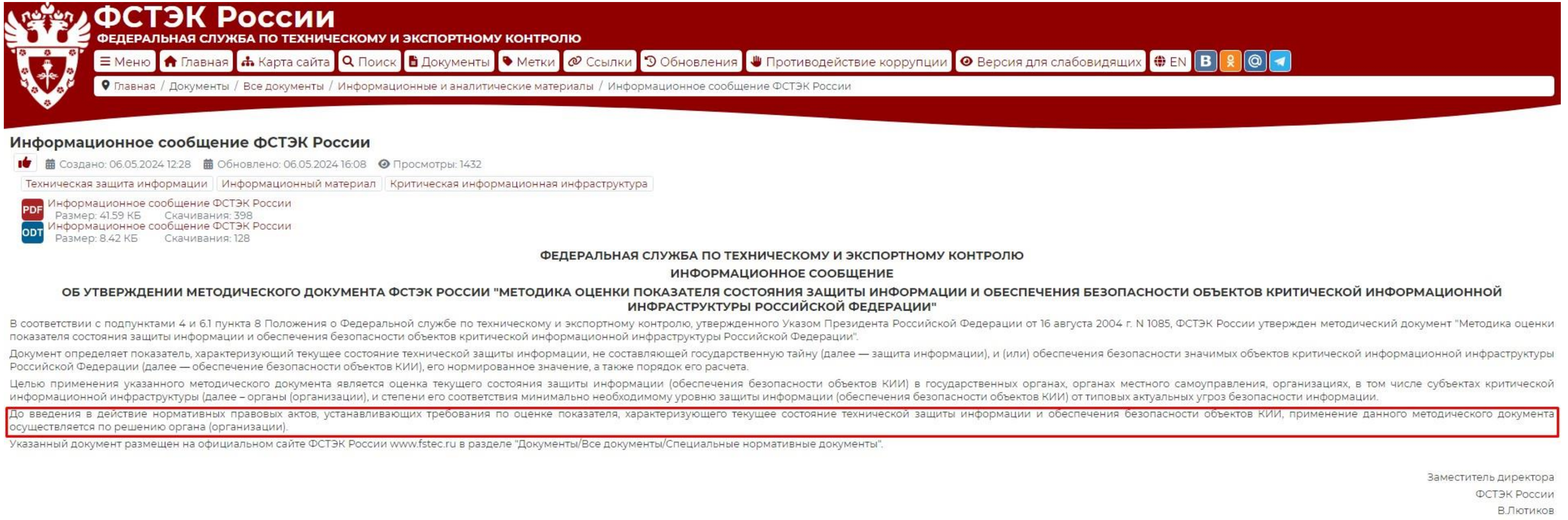
2024

Предназначена для всех организаций (например, ОГВ, ОМСУ), которые в своих системах обрабатывают информацию, не составляющей государственную тайну (например, в ГИС, ИСПДн) и владельцев значимых объектов КИИ

Вышеупомянутые организации,
применяя данную методику, могут:

- оценить текущее состояние защиты информации и (или) обеспечения безопасности объектов КИИ;
- разработать на основе такой оценки меры по повышению уровня защищенности;
- провести оценку эффективности деятельности заместителя руководителя организации, на которого возложены полномочия по обеспечению ИБ, и (или) структурного подразделения, осуществляющего функции по обеспечению ИБ организации.

Информационное сообщение ФСТЭК России



ФСТЭК России
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Меню | Главная | Карта сайта | Поиск | Документы | Метки | Ссылки | Обновления | Противодействие коррупции | Версия для слабовидящих | EN

Главная / Документы / Все документы / Информационные и аналитические материалы / Информационное сообщение ФСТЭК России

Информационное сообщение ФСТЭК России

Создано: 06.05.2024 12:28 Обновлено: 06.05.2024 16:08 Просмотры: 1432

Техническая защита информации | Информационный материал | Критическая информационная инфраструктура

PDF Информационное сообщение ФСТЭК России
Размер: 41.59 КБ Скачивания: 398

ODT Информационное сообщение ФСТЭК России
Размер: 8.42 КБ Скачивания: 128

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

ОБ УТВЕРЖДЕНИИ МЕТОДИЧЕСКОГО ДОКУМЕНТА ФСТЭК РОССИИ "МЕТОДИКА ОЦЕНКИ ПОКАЗАТЕЛЯ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ"

В соответствии с подпунктами 4 и 6.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, ФСТЭК России утвержден методический документ "Методика оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации".

Документ определяет показатель, характеризующий текущее состояние технической защиты информации, не составляющей государственную тайну (далее — защита информации), и (или) обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее — обеспечение безопасности объектов КИИ), его нормированное значение, а также порядок его расчета.

Целью применения указанного методического документа является оценка текущего состояния защиты информации (обеспечения безопасности объектов КИИ) в государственных органах, органах местного самоуправления, организациях, в том числе субъектах критической информационной инфраструктуры (далее – органы (организации), и степени его соответствия минимально необходимому уровню защиты информации (обеспечения безопасности объектов КИИ) от типовых актуальных угроз безопасности информации.

До введения в действие нормативных правовых актов, устанавливающих требования по оценке показателя, характеризующего текущее состояние технической защиты информации и обеспечения безопасности объектов КИИ, применение данного методического документа осуществляется по решению органа (организации).

Указанный документ размещен на официальном сайте ФСТЭК России www.fstec.ru в разделе "Документы/Все документы/Специальные нормативные документы".

Заместитель директора
ФСТЭК России
В.Лютиков

https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii

Показатель защищенности (Кзи)

В качестве показателя, характеризующего текущее состояние защиты информации (обеспечения безопасности объектов КИИ) в организации, в методике используется **показатель текущего состояния защищенности Кзи**, который характеризует степень достижения организацией **минимально необходимого уровня защиты информации** от типовых актуальных угроз безопасности информации ИС, АСУ, ИТКС и иных объектов информатизации.

Для оценки КЗИ определяются значения частных показателей безопасности kji.

Частные показатели безопасности характеризуют реализацию в организации отдельных мер по защите информации. Каждому частному показателю в методике присвоен определенный «вес» и все они поделены на следующие группы:

- организация и управление;
- защита пользователей;
- защита информационных систем;
- мониторинг информационной безопасности и реагирование.

Частные показатели

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование показателя безопасности	Значение частного показателя (k_{ji})	Значение весового коэффициент группы показателей (R_j)
1.	Организация и управление	1. На заместителя руководителя органа (организации) возложены[3] полномочия ответственного лица за обеспечение информационной безопасности органа (организации) и определены его обязанности	0,30	0,10
		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[4]	0,30	

Частные показатели

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование показателя безопасности	Значение частного показателя (k_{ji})	Значение весового коэффициент группы показателей (R_j)
2.	Защита пользователей	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	0,25
		2. Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)[3]	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	

Частные показатели

Номер группы показателей (j)	**Наименование групп показателей**	Номер (i) и наименование показателя безопасности	Значение частного показателя (k_{ji})	Значение весового коэффициент группы показателей **(R_j)**
3.	Защита информационных систем	1. На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет[1], контролируется межсетевыми экранами уровня L3/L4)	0,20	0,35
		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. 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))	0,10	
		5. Обеспечена проверка вложений в электронных письмах электронной почты[2] на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств)	0,15	
		6. Обеспечено централизованное управление средствами антивирусной защиты[3] (не менее чем 80% пользовательских устройств[4] 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	
		7. Реализована очистка входящего из сети Интернет сетевого трафика от аномалий на уровне[5] L3/L4 (заключен договор с провайдером)	0,10	

Частные показатели

Номер группы показателей (j)	**Наименование групп показателей**	Номер (i) и наименование показателя безопасности	Значение частного показателя (k_{ji})	Значение весового коэффициент группы показателей **(R_j)**
4.	Мониторинг информационной безопасности и реагирование	1. Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей	0,40	0,30
		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 защищенности

$$К_{ЗИ}=(k_{11}+k_{12}+k_{13})R_1+(k_{21}+k_{22}+...+k_{2i})R_2+(k_{31}+k_{32}+...+k_{3i})R_3+(k_{41}+k_{42}+...+k_{4i})R_4,$$

Где:

R_j — весовой коэффициент
j — й группы частных показателей безопасности

Значение $К_{ЗИ}$	Текущее состояние защиты информации (обеспечения безопасности объектов КИИ)
$К_{ЗИ}=1$	Обеспечивается минимальный уровень защиты от типовых актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как минимальный базовый («зеленый»)
$0,75<К_{ЗИ}<1$	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеются предпосылки реализации актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как низкий («оранжевый»)
$К_{ЗИ}\leq0,75$	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как критический («красный»)

Вопрос № 2

Назовите топ СЗИ, которые точно необходимо внедрять любому владельцу ЗОКИИ

Первоочередные меры защиты информации

Инвентаризация информационных ресурсов

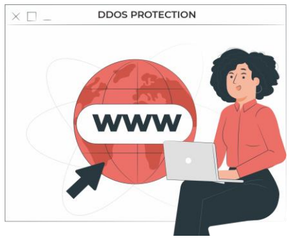
Антивирусная защита рабочих мест

Защита периметра информационной инфраструктуры

Управление доступом пользователей

Мониторинг событий информационной безопасности

Контроль почтовых вложений на предмет наличия вредоносного программного обеспечения



Очистка входящего из сети «Интернет» трафика

Организационные меры в отношении персонала субъекта КИИ

ЗАПРЕТИТЬ:

- использовать посторонние USB-накопители на АРМ ЗОКИИ;
- заходить в личную почту через АРМ ЗОКИИ;
- загружать и устанавливать стороннее ПО на АРМ ЗОКИИ;
- передавать конфиденциальную информацию (файлы) через внешние облачные сервисы;
- скачивать файлы из внешних источников на АРМ ЗОКИИ;
- пользоваться социальными сетями на рабочем месте;
- развертывать дополнительные Wi-Fi сети на территории промышленного объекта;
- заряжать лишние устройства через АРМ и серверы ЗОКИИ

Вопрос № 3

Если у нас НОКИИ, будут ли к нам всё равно обращаться регуляторы (ФСТЭК)?

Взаимодействие с ФСТЭК России

Первичное:

- отправка регулятору перечня ОКИИ и сведений по форме приказа ФСТЭК России № 236;
- отправка регулятору модели угроз и технического задания (**в случае если ОКИИ является ГИС**)

Дальнейшее:

- отправка результатов категорирования новых ОКИИ;
- отправка регулятору актуализированных сведений по форме приказа ФСТЭК России № 236 **в случае изменений сведений об объекте КИИ, указанных в форме**;
- отправка регулятору актуализированных сведений по форме приказа ФСТЭК России № 236 **в случае изменения показателей критериев значимости или их значений**;
- отправка регулятору актуализированных сведений по форме приказа ФСТЭК России № 236 **не реже 1 раза в 5 лет;**
- подготовка ответов на запросы регулятора, осуществляемые в рамках мониторинга текущего состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры;
- сопровождение регулятора при проведении выездной проверке соблюдения выполнения требований по ИБ

Вопрос № 4

**Подскажите, что делать, если субъект понял,
что все его объекты не имеют категорию значимости?
Значит ли это что объекты можно не защищать?
В каких НПА написано, что нужно защищать НОКИИ?**

В каких случаях НОКИИ подлежат защите?

1	Если НОКИИ является ГИС, то необходимо выполнять требования по защите ГИС
2	Если НОКИИ является ИС с собрабткой ПДн, то необходимо выполнять требования по защите ПДн
3	Если существуют отраслевые требования по ИБ, в которых предъявляются требования по защите НОКИИ
4	Если существует вероятность воздействия на ЗОКИИ в результате атаки на НОКИИ

Не забываем про часть 2 ст. 9 187-ФЗ, которая распространяется в том числе на владельцев НОКИИ

Субъекты критической информационной инфраструктуры обязаны:

1) незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также Центральный банк Российской Федерации (в случае, если субъект критической информационной инфраструктуры осуществляет деятельность в банковской сфере и в иных сферах финансового рынка) в установленном указанным федеральным органом исполнительной власти порядке (в банковской сфере и в иных сферах финансового рынка указанный порядок устанавливается по согласованию с Центральным банком Российской Федерации);

2) оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

3) в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

Вопрос № 5

**Также встает вопрос о 250 Указе. Необходимо создать подразделение и назначить ответственного за ИБ.
Но в нашей организации это будет лишним, нанимать специалиста по ИБ, так как ИТ-специалисты вполне сами справляются. Да и зачем нам специалист по ИБ, если защищать по законам ничего не нужно?**

Распространение требований Указа Президента РФ № 250

субъекты КИИ;

федеральные органы исполнительной власти;

высшие исполнительные органы государственной власти субъектов Российской Федерации;

государственные фонды;

государственные корпорации;

стратегические предприятия, стратегические акционерные общества;

системообразующие организации российской экономики;

иные организации, созданные на основании федеральных законов.

Вопрос № 6

В 2018, начиная свой путь в КИИ, по ошибке присвоили объекту 2 категорию значимости. Сейчас же понимаем, что это неправильное решение. Как теперь объяснить ФСТЭК что объект понижает категорию? (до незначимой) Думаем, ФСТЭК не разрешит нам понизить и из реестра объектов КИИ ничего не уберет.

Вариант 1

1	В рамках заседания ПДК по категорированию осуществляется пересмотр показателей критериев значимости. Подробно аргументируются новые значения показателей критериев значимости
2	Оформление протоколов заседания ПДК, актов категорирования, сведений по форме приказа ФСТЭК России № 236
3	Отправка во ФСТЭК России новых сведений по форме приказа ФСТЭК России № 236. В официальном письме признаем ранее допущенную ошибку.
4	Подготовка ответов на дополнительные вопросы регулятора

Вариант 2

1	Анализ характеристик ЗОКИИ, которые привели к завышению категории значимости.
2	Определение способа изменения данной характеристики
3	Издание приказа о модернизации ЗОКИИ
4	Проведение модернизации, в результате которой происходит изменение нужных харакетристик ЗОКИИ

Вариант 2

5	Издание приказа о вводе модернизированной ИС/АСУ/ИТКС в эксплуатацию
6	Проведение заседание ПДК с оформлением актов категорирования и сведений по форме приказа ФСТЭК России № 236
7	Отправка во ФСТЭК России сведений по форме приказа ФСТЭК России № 236, копии приказов о модернизации и приемки в эксплуатацию
8	Подготовка ответов на дополнительные вопросы регулятора

Вопрос № 7

Всё еще актуально определять объект как ОКИИ = ОКВЭД + негативные последствия из ПП 127?

Объекты КИИ

Объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры

Пример типового перечня ОКИИ

ПЕРЕЧЕНЬ
типовых объектов критической информационной инфраструктуры Российской Федерации, функционирующих в области металлургической промышленности

№ п/п	Наименование типового объекта критической информационной инфраструктуры (ИС, ИТКС, АСУ)	Осуществляемые критические процессы типовым отраслевым объектом КИИ	ОКВЭД
1	2	3	4
1.	Системы управления технологическим процессом подготовки сырья	Выполнение работ по рудоподготовке и обогащению; Выполнение работ по производству металлов.	52.10 Деятельность по складированию и хранению 20.11 Производство промышленных газов 24.10 Производство чугуна, стали и ферросплавов 24.10.1 Производство основных продуктов из железа и стали 24.10.11 Производство чугуна 24.10.12 Производство ферросплавов 24.10.13 Производство продуктов прямого восстановления железной руды и губчатого железа
2.	Система управления технологическим процессом хранения сырья или продукции	Обеспечение хранения веществ, сырья или продукции, требующих особых условий хранения; Приём и подготовка металлосодержащего сырья, производство чернового металла, производство чистового металла (готовой продукции), концентрирование и выделение металлов, складирование отвальных шлаков; Складирование и учёт металлосодержащего сырья, складирование и учёт чернового металла,	

Вопрос № 8

Что является самым важным в Протоколе ПДК?
Что необходимо указать в нем?

Пример формы протокола постоянно действующей комиссии по категорированию ОКИИ

Приложение №2
к Методическим рекомендациям по категорированию объектов критической информационной инфраструктуры в сфере транспорта

Протокол заседания комиссии по категорированию объектов критической информационной инфраструктуры

Форма

ПРОТОКОЛ
заседания комиссии по категорированию объектов критической информационной инфраструктуры

_____
наименование субъекта КИИ

от «___»_____20__г.

по_____
тема заседания комиссии

Постоянно действующая комиссия по категорированию объектов критической информационной инфраструктуры _____
наименование субъекта КИИ

в составе:
Председатель комиссии:

_____ _____
должность *Фамилия Имя Отчество*

Члены комиссии:

_____ _____
должность *Фамилия Имя Отчество*

_____ _____
должность *Фамилия Имя Отчество*

_____ _____
должность *Фамилия Имя Отчество*

рассмотрев исходные данные с целью _____
тема заседания комиссии,

ОПРЕДЕЛИЛА:
1. <указываются решения комиссии по теме заседания>
2. …….
3. …….

Приложения*: <Указываются приложения, содержащие согласованные комиссией исходные данные, результаты анализа, отчетные документы по теме заседания>.*

Председатель комиссии:

_____
должность *Фамилия Имя Отчество* *подпись*

«___»_____ 20__г.

Члены комиссии:

_____
должность *Фамилия Имя Отчество* *подпись*

«___»_____ 20__г.

_____
должность *Фамилия Имя Отчество* *подпись*

«___»_____ 20__г.

_____
должность *Фамилия Имя Отчество* *подпись*

«___»_____ 20__г.

Секретарь комиссии

_____
должность *Фамилия Имя Отчество* *подпись*

«___»_____ 20__г.

Вопрос № 9

Что вы считаете самым сложным в категорировании объектов?

Процесс категорирования ОКИИ

Критерии залога успеха:

- **Полноценный состав** постоянно действующей комиссии по категорированию и ее **вовлеченность в процесс**
- **Подробное обоснование** полученных значений по каждому из рассчитываемых критериев значимости с приведением достоверных статистических данных, информации из регламентов проведения профилактических работ, отраслевых документов по функциональной безопасности и т.п.

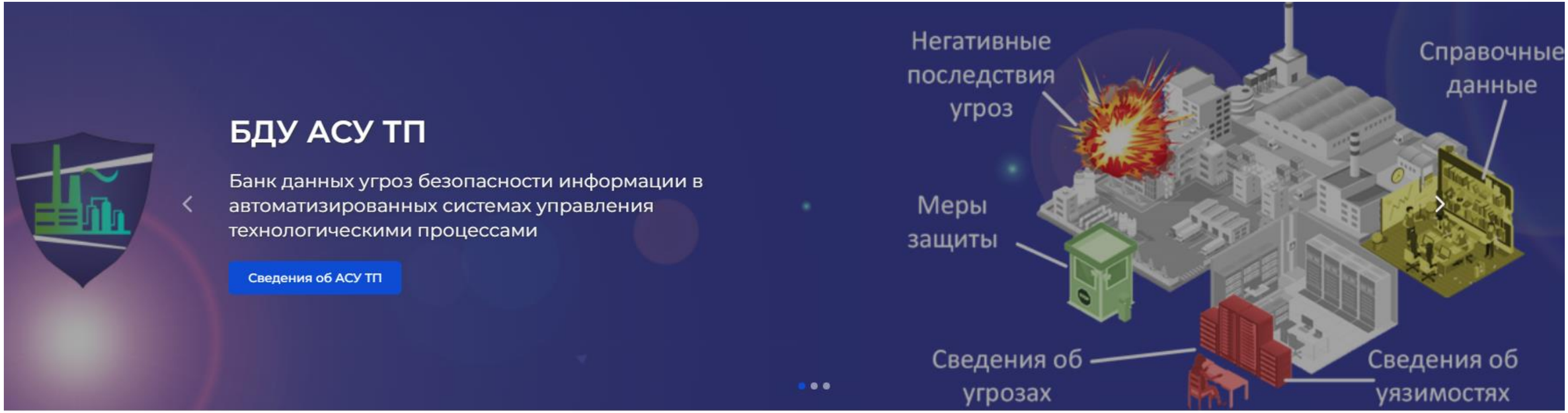
Рекомендации:

- Рассматривайте **наихудшие сценарии** в результате проведения **целенаправленных компьютерных атак**
- Опирайтесь на декларации промышленной безопасности опасного производственного объекта, декларации безопасности гидротехнического сооружения, паспорты безопасности объекта топливно-энергетического комплекса (при наличии) и т.п., **но учитывайте последствия только в случае возникновения компьютерных инцидентов на ОКИИ**

Вопрос № 10

Интересует практика правоприменения новой БДУ ФСТЭК для АСУ ТП по действующей методике

БДУ АСУ ТП



https://bduasutp.fstec.ru/

Вопрос № 11

Как объяснять работникам что-то про КИИ, если они даже не могут полностью выговорить словосочетание "Критическая информационная инфраструктура"?
(обычные работяги, которые делают свою работу, и что такое КИИ и знать не хотят)

Ответственность за несоблюдение требований в сфере защиты КИИ (УК РФ)

Уголовная ответственность			
УК РФ	274.1 (ч.1)	Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.	• принудительные работы до 5 лет с ограничением свободы до 2 лет или без такового; • лишение свободы от 2 до 5 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет.
	274.1 (ч.2)	Неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ РФ, или иных вредоносных компьютерных программ, если он повлек причинение вреда КИИ РФ	• принудительные работы на срок до 5 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет и с ограничением свободы на срок до 2 лет или без такового; • лишение свободы на срок от 2 до 6 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет
	274.1 (ч.3)	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ, или ИС, ИТС, АСУ, сетей электросвязи, относящихся к КИИ РФ, либо правил доступа к указанным информации, ИС, ИТС, АСУ, сетям электросвязи, если оно повлекло причинение вреда КИИ РФ	• принудительные работы до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового; • лишение свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.
	274.1 (ч.4)	Деяния, предусмотренные частями 1-3 статьи 274.1, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения	лишение свободы на срок от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.
	274.1 (ч.5)	Деяния, предусмотренные частями 1-4 статьи 274.1, если они повлекли тяжкие последствия	лишение свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового.

Ответственность за несоблюдение требований в сфере защиты КИИ (КоАП РФ)

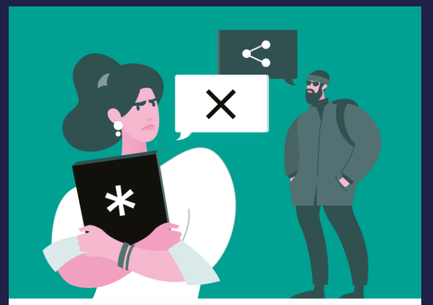
НПА	Статья	Тип нарушения	Наказание
		Административная ответственность	
КоАП РФ	13.12.1 (ч.1)	Нарушение требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ РФ, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, если такие действия (бездействие) не содержат уголовно наказуемого деяния	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 50 000 до 100 000 рублей.
	13.12.1 (ч.2)	Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.
	13.12.1 (ч.3)	Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными организациями, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты	• для должностных лиц – штраф от 20 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.
	19.7.15 (ч.1)	Непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, сведений о результатах присвоения объекту КИИ РФ одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности КИИ РФ, либо об отсутствии необходимости присвоения ему одной из таких категорий либо представление недостоверных сведений	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • за повторное нарушение – штраф от 10 000 до 50 000 рублей (ч.3 ст. 19.7.15); • для юридических лиц – штраф от 50 000 до 100 000 рублей; • за повторное нарушение – штраф от 100 000 до 200 000 рублей (ч.3 ст. 19.7.15).
	19.7.15 (ч.2)	Непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ информации, предусмотренной законодательством в области обеспечения безопасности КИИ РФ, за исключением случаев, предусмотренных частью 2 статьи 13.12.1 КоАП	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.

Бесплатные курсы по кибербезопаности
от наших партнеров **Positive Technologies**

1) Базовая кибербезопасность: первое погружение
https://info.edu.ptsecurity.com/cybersecuritycourse

2) Личная кибербезопасность:
https://info.edu.ptsecurity.com/antihackingcourse

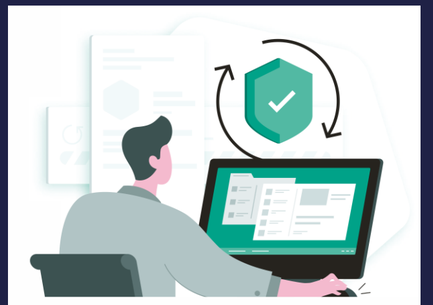
Всегда используйте только сложные пароли



Любая рабочая информация может быть конфиденциальной

Не открывайте исполняемые файлы, приложенные к электронным письмам

Перед вводом своих данных на любом сайте обязательно проверьте его на подлинность



Антивирус должен быть включен всегда, когда включен ваш компьютер

Не храните в браузере пароли от важных ресурсов

Ссылка на плакаты от Лабаратории Касперского:

Мы поможем Вам защитить данные и выполнить требования НПА

Компания КСБ-СОФТ оказывает полный комплекс услуг по защите объектов КИИ

Безопасность объектов КИИ

Выявление и категорирование объектов КИИ, разработка и внедрение комплексного решения по обеспечению безопасности значимых объектов КИИ, организация взаимодействия с центром ГосСОПКА, анализ уязвимостей и пентест

Импортозамещение

Решение задач импортозамещения в соответствии со стратегией развития информационного общества в Российской Федерации

SOCRAT - центр мониторинга и реагирования на инциденты информационной безопасности

Мониторинг и предотвращение атак на начальных стадиях, либо выявление следов проникновения

Оценка показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры

Выполнение работ по новой методике ФСТЭК России от 02.05.2024 г.

Оценка показателя состояния технической защиты информации и обеспечения безопасности ЗОКИИ

Работы	Отчётные документы
Экспертный аудит для сбора исходных данных, необходимых для оценки показателя защищенности	Отчет о проведении аудита с результатами проведения опроса (интервьюирования) работников
Анализ уязвимостей устройств и интерфейсов, доступных из сети Интернет, а также пользовательских устройств и серверов	Отчет об анализе уязвимостей
Регламентация оценки показателя технической защищенности	Регламент оценки показателя технической защищенности
Проведение оценки показателя защищенности	Акт оценки показателя защищенности
Планирование работ по защите информации	План реализации мероприятий по повышению уровня защищенности

Ценность для Заказчика

Прозрачная картина
по состоянию ИБ в организации
для руководства и службы ИБ

Живой план работ
по повышению уровня защищенности,
обновляемый не реже раз в полгода

Своевременная
отчетность перед регулятором

Устойчивое функционирование
ЗОКИИ и противодействие типовым угрозам

Работайте с нами!

https://ksb-soft.ru/

428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9

8 800 3333-872

info@ksb-soft.ru

Телеграм-канал
«Мнение интегратора»

Задайте свой
вопрос для разбора
на следующем вебинаре