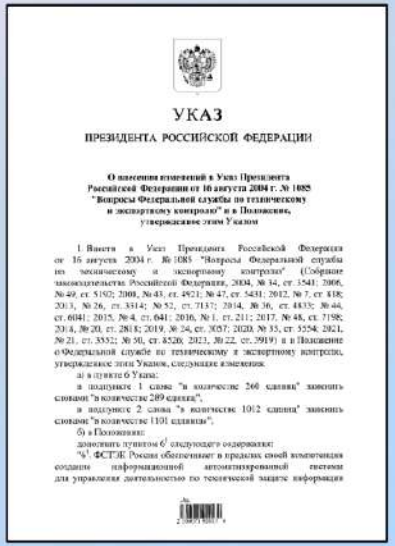
МЕТОДИКА ОЦЕНКИ ПОКАЗАТЕЛЯ СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗВЯГИНЦЕВА Полина Александровна
начальник отдела Управления ФСТЭК России
по Сибирскому федеральному округу,
сентябрь 2024

Оценка состояния защиты информации и обеспечения безопасности объектов КИИ и эффективности деятельности органов государственной власти и организаций

Указ Президента Российской Федерации от 8 ноября 2023 г. № 846 «О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

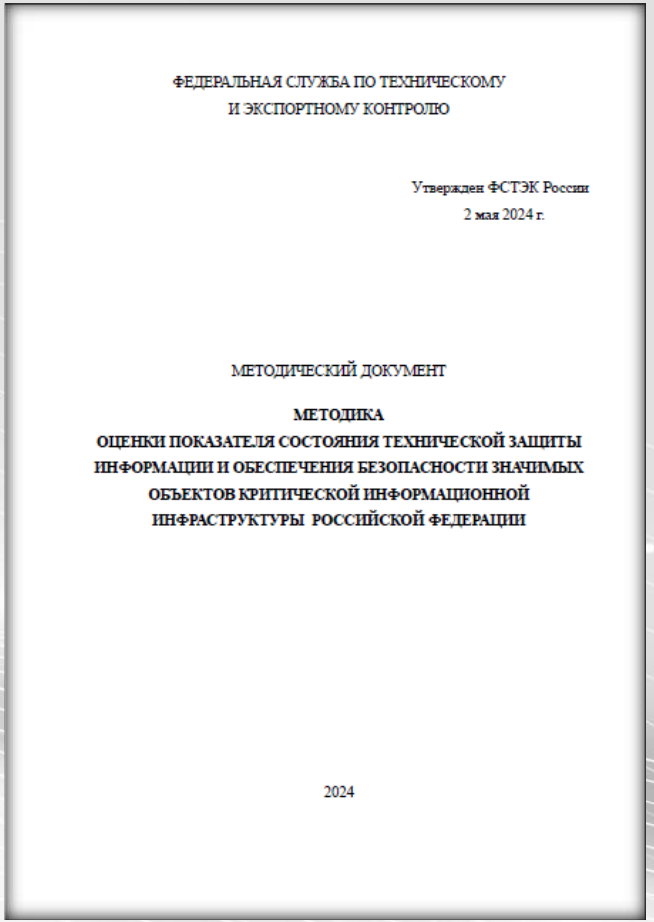
Новые полномочия ФСТЭК России

Мониторинг текущего состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры

Организация и проведение оценки эффективности деятельности ОГВ и организаций по технической защите информации и обеспечению безопасности значимых объектов КИИ

Показатель состояния защиты информации и обеспечения безопасности объектов КИИ в органе государственной власти и (или) организации

Показатель зрелости деятельности органов государственной власти и организаций по защите информации и обеспечению безопасности объектов КИИ



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

- Документ размещен на официальном сайте ФСТЭК России

www.fstec.ru в разделе «Документы/Все документы/Специальные нормативные документы».

25. Оценка состояния защиты информации проводится на основе определения оператором:

а) показателя, характеризующего текущее состояние защиты информации от актуальных угроз безопасности информации;

б) показателя, характеризующего эффективность проведения мероприятий и реализации мер по защите информации.

Показатели состояния защиты информации и уровня зрелости являются ключевыми показателями эффективности деятельности по защите информации ответственного лица, структурного подразделения, специалистов по защите информации оператора.

Для расчета значений показателей состояния защиты информации и уровня зрелости применяются методические документы, утвержденные ФСТЭК России)

$$К_{ЗИ}=(k_{11}+k_{12}+k_{13})R_1+(k_{21}+k_{22}+...+k_{2i})R_2+(k_{31}+k_{32}+...+k_{3i})R_3+(k_{41}+k_{42}+k_{43})R_4$$

Организация и управление

Номер (i) и наименование показателя безопасности	k_{ji}	R_j
1. На заместителя руководителя органа (организации) возложены полномочия ответственного лица за обеспечение информационной безопасности органа (организации) и определены его обязанности. Возложение полномочий и (или) определение структурного подразделения (работников) в органе (организации) подтверждается изданием соответствующего локального правового акта.	**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	**0,30**	

Защита пользователей

Номер (i) и наименование показателя безопасности	k_{ji}	R_j
1. Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике.	**0,30**	**0,25**
2. Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)	**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**	

Защита информационных систем

Номер (i) и наименование показателя безопасности	k_{ji}	R_j
1. На сетевом периметре информационных систем установлены МЭ L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет, контролируется межсетевыми экранами уровня L3/L4)	**0,20**	**0,35**
2. На устройствах и интерфейсах, доступных из сети Интернет, отсутствуют уязвимости критического уровня опасности	**0,20**	
3. На пользовательских устройствах и серверах отсутствуют уязвимости критического уровня	**0,10**	
4. Обеспечен документальный или автоматизированный учет пользовательских устройств, серверов и сетевых устройств	**0,10**	
5. Обеспечена проверка вложений в электронных письмах электронной почты на наличие ВПО	**0,15**	
6. Обеспечено централизованное управление средствами антивирусной защиты (не менее чем 80% пользовательских устройств контролируются средствами антивирусной защиты с централизованным управлением).	**0,15**	
7. Реализована очистка входящего из сети Интернет сетевого трафика от аномалий на уровне L3/L4 (заключен договор с провайдером)	**0,10**	

Мониторинг информационной безопасности

Номер (i) и наименование показателя безопасности	k_{ji}	R_j
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**	

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

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

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»)

Обеспечивается минимально необходимый уровень безопасности от актуальных угроз безопасности информации ($К_{ИБ}$ =1)

Минимально необходимый уровень безопасности от актуальных угроз безопасности информации не обеспечивается, имеются предпосылки к реализации угроз безопасности информации (0,75<$К_{ИБ}$<1)

Минимально необходимый уровень безопасности от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации угроз безопасности информации ($К_{ИБ}$ <=0,75)

11

ЗВЯГИНЦЕВА Полина Александровна

Спасибо за внимание!

т.(383)203-54-09