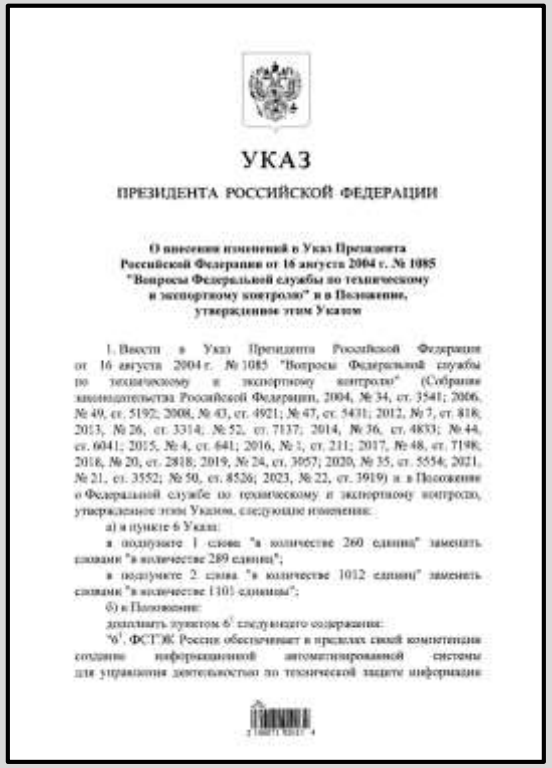
МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ПОКАЗАТЕЛЯ СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Заместитель начальника отдела
9 управления ФСТЭК России
Булгаков Андрей Сергеевич

НОВЫЕ ПОЛНОМОЧИЯ ФСТЭК РОССИИ

Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" и в Положение, утвержденное этим Указом

1. Внести в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137; 2014, № 36, ст. 4833; № 44, ст. 6041; 2015, № 4, ст. 641; 2016, № 1, ст. 211; 2017, № 48, ст. 7198; 2018, № 20, ст. 2818; 2019, № 24, ст. 3057; 2020, № 35, ст. 5554; 2021, № 21, ст. 3552; № 50, ст. 8526; 2023, № 22, ст. 3919) и в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное этим Указом, следующие изменения:

а) в пункте 6 Указа:

в подпункте 1 слова "в количестве 260 единиц" заменить словами "в количестве 289 единиц";

в подпункте 2 слова "в количестве 1012 единиц" заменить словами "в количестве 1101 единицы";

б) в Положении:

дополнить пунктом 6[1] следующего содержания:

"6[1]. ФСТЭК России обеспечивает в пределах своей компетенции создание информационной автоматизированной системы для управления деятельностью по технической защите информации

- Мониторинг текущего состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры.
- Централизованный учет информационных систем и иных объектов критической информационной инфраструктуры по отраслям экономики.
- Оперативное информирование об угрозах безопасности информации и уязвимостях информационных систем и иных объектов критической информационной инфраструктуры.
- Оперативное доведение мер по технической защите от выявленных угроз и уязвимостей.
- Организация и проведение оценки эффективности деятельности ОГВ и организаций по технической защите информации и обеспечению безопасности значимых объектов критической информационной инфраструктуры.

ТИПОВЫЕ НЕДОСТАТКИ, СОЗДАЮЩИЕ ПРЕДПОСЫЛКИ ДЛЯ РЕАЛИЗАЦИИ КОМПЬЮТЕРНЫХ АТАК

Слабые пароли пользователей и администраторов, однофакторная идентификация, использование паролей, установленных по умолчанию

Уязвимости программного обеспечения, используемого в информационных системах

Активные учетные записи уволенных работников

Использование для доступа к информационной инфраструктуры личных устройств работников

Использование на рабочих местах работников личных мессенджеров, социальных сетей

ПРОДОЛЖИТЕЛЬНОСТЬ ПОДБОРА ПАРОЛЕЙ

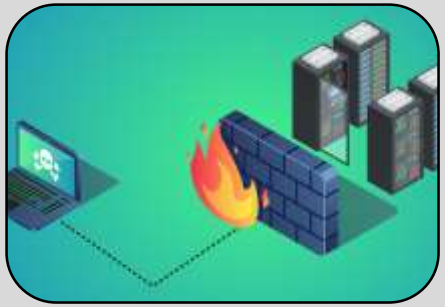
ДЛИНА ПАРОЛЯ	КОЛ-ВО ВАРИАНТОВ	СТОЙКОСТЬ	ВРЕМЯ ПЕРЕБОРОВ
1	36	5 бит	менее секунды
2	1 296	10 бит	менее секунды
3	46 656	15 бит	менее секунды
4	1 679 616	21 бит	17 секунд
5	60 466 176	26 бит	10 минут
6	2 176 782 336	31 бит	6 часов
7	78 364 164 096	36 бит	9 дней
8	$2{,}821\ 109\ 9 \times 10^{12}$	41 бит	11 месяцев
9	$1{,}015\ 599\ 5 \times 10^{14}$	46 бит	32 года
10	$3{,}656\ 158\ 4 \times 10^{15}$	52 бита	1 162 года
11	$1{,}316\ 217\ 0 \times 10^{17}$	58 бит	41 823 года
12	$4{,}738\ 381\ 3 \times 10^{18}$	62 бита	1 505 615 лет

ПЕРВООЧЕРЕДНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Антивирусная защита рабочих мест

Мониторинг событий информационной безопасности

Контроль почтовых вложений на предмет наличия вредоносного программного обеспечения



Защита периметра информационной инфраструктуры

Инвентаризация информационных ресурсов

Управление доступом пользователей

Очистка входящего из сети «Интернет» трафика

МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ 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

Цель применения

Оценка степени достижения ОГВ и субъектами КИИ минимально необходимого (базового) уровня защиты информации, не составляющей гос. тайну и значимых объектов КИИ от наиболее распространенных УБИ

Оцениваемый параметр

Показатель состояния технической защиты информации, и обеспечения безопасности значимых объектов КИИ РФ

Этапы оценки

- ✓ Сбор и анализ исходных данных, необходимых для оценки уровня безопасности от актуальных УБИ
- ✓ Определение значений частных показателей безопасности
- ✓ Расчет значения показателя состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ и сравнение его с нормированными значениями

Результаты оценки

- ✓ Минимальный базовый уровень безопасности от актуальных УБИ («зеленый»)
- ✓ Низкий уровень обеспечения безопасности от актуальных УБИ («оранжевый»)
- ✓ Критический уровень обеспечения безопасности от актуальных УБИ («красный»)

Для кого актуальна?

- ✓ ФСТЭК России
- ✓ Органы государственной власти
- ✓ Субъекты КИИ

МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

Организация и управление

Защита пользователей

Защита информационных систем

Мониторинг информационной безопасности и реагирование

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ГРУППА ПОКАЗАТЕЛЕЙ	ВЕСОВОЙ КОЭФФИЦИЕНТ	НАИМЕНОВАНИЕ ПОКАЗАТЕЛЯ	ЗНАЧЕНИЕ
1. Организация и управление	0,10	1. На заместителя руководителя органа (организации) возложены полномочия ответственного лица за обеспечение информационной безопасности органа (организации) и определены его обязанности	0,20
		2. Определено структурное подразделение (или отдельные работники), осуществляющее функции по обеспечению информационной безопасности органа (организации), и определены функции (обязанности)	0,35
		3. С подрядными организациями, имеющими доступ к информационным системам, заключены соглашения об обеспечении безопасности (соглашения заключены с 90% подрядчиков), предусматривающие ответственность за реализацию угроз через информационную инфраструктуру подрядчика	0,30

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ГРУППА ПОКАЗАТЕЛЕЙ	ВЕСОВОЙ КОЭФФИЦИЕНТ	НАИМЕНОВАНИЕ ПОКАЗАТЕЛЯ	ЗНАЧЕНИЕ
2. Защита пользователей	0,25	1. Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике	0,30
		2. **Для привилегированных пользователей при аутентификации используется второй фактор (не менее 50% привилегированных пользователей)**	0,30
		3. Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию	0,20
		4. Отсутствуют активные учетные записи для работников, с которыми прекращены трудовые или иные отношения	0,20

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ГРУППА ПОКАЗАТЕЛЕЙ	ВЕСОВОЙ КОЭФФИЦИЕНТ	НАИМЕНОВАНИЕ ПОКАЗАТЕЛЯ	ЗНАЧЕНИЕ
3. Защита информационных систем	0,35	1. На сетевом периметре информационных систем установлены межсетевые экраны уровней L3/L4 (доступ к 100% интерфейсов, доступных из сети «Интернет», контролируется межсетевыми экранами уровней L3/L4)	0,20
		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 и (или) на официальных сайтах разработчиков более 30 дней	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)	0,10
		4. Обеспечен учет пользовательских устройств (не менее 80% устройств и серверов учтено)	0,10
		5. Обеспечена проверка вложений в электронных письмах на наличие вредоносного программного обеспечения (проверяются вложения для не менее чем 80% пользовательских устройств)	0,15
		6. Средства антивирусной защиты с централизованным управлением установлены (не менее чем 85% пользовательских устройств контролируются средствами антивирусной защиты с централизованным управлением). Политиками установлена периодичность обновления баз данных признаков вредоносного программного обеспечения не раже 1 раза в месяц	0,15
		7. Реализована очистка входящего из сети «Интернет» сетевого трафика от аномалий на уровне L3/L4 (заключен договор с провайдером)	0,10

ЧАСТНЫЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ

ГРУППА ПОКАЗАТЕЛЕЙ	ВЕСОВОЙ КОЭФФИЦИЕНТ	НАИМЕНОВАНИЕ ПОКАЗАТЕЛЯ	ЗНАЧЕНИЕ
4. Мониторинг информационной безопасности и реагирование	0,30	**1. Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей**	0,40
		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 СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ

$$К_{ИБ}=(k_{11}+ k_{21}+ \ldots k_{i1})*R_1+(k_{12}+ k_{22}+ \ldots k_{i2})*R_2+\ldots(k_{14}+ k_{24}+ \ldots k_{i4})*R_4$$

Где:

$К_{ИБ}$ – показатель

R_j – весовой коэффициент группы частных показателей безопасности

k_{ij} – показатель безопасности

$К_{ИБ}=1$	обеспечивается минимально необходимый уровень безопасности от актуальных угроз безопасности информации. Уровень обеспечения безопасности – минимальный базовый («зеленый»)
$0,75<К_{ИБ}<1$	минимально необходимый уровень безопасности от актуальных угроз безопасности информации не обеспечивается, имеются предпосылки реализации актуальных угроз безопасности информации. Уровень обеспечения безопасности – низкий («оранжевый»)
$К_{ИБ}\leq0,75$	минимально необходимый уровень безопасности от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности информации. Уровень обеспечения безопасности – критический («красный»)

СПАСИБО ЗА ВНИМАНИЕ!

Булгаков
Андрей Сергеевич

+7 (495) 693-68-72

otd93@fstec.ru