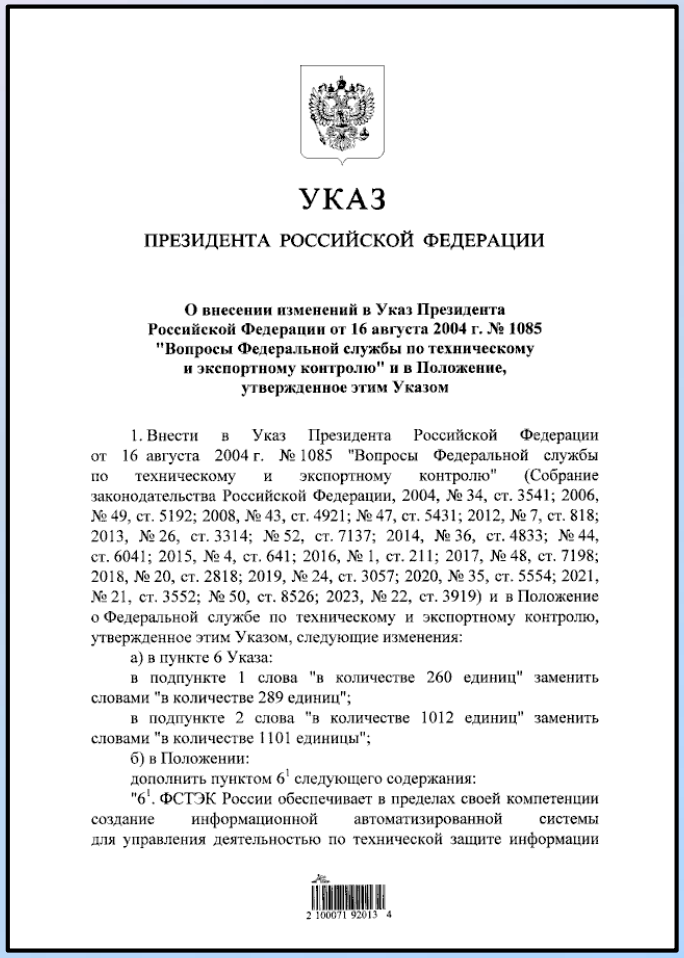
О методическом подходе к оценке текущего состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры в органах государственной власти и организациях

Начальник 9 управления ФСТЭК России

БОНДАРЕНКО Сергей Васильевич

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

2 100071 92013 4

- Централизованный учет информационных систем и иных объектов критической информационной инфраструктуры по отраслям экономики
- ***Мониторинг текущего состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры***
- 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

ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ

Стратегия национальной безопасности Российской Федерации

(утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400)

Доктрина информационной безопасности Российской Федерации

(утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646)

Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности»

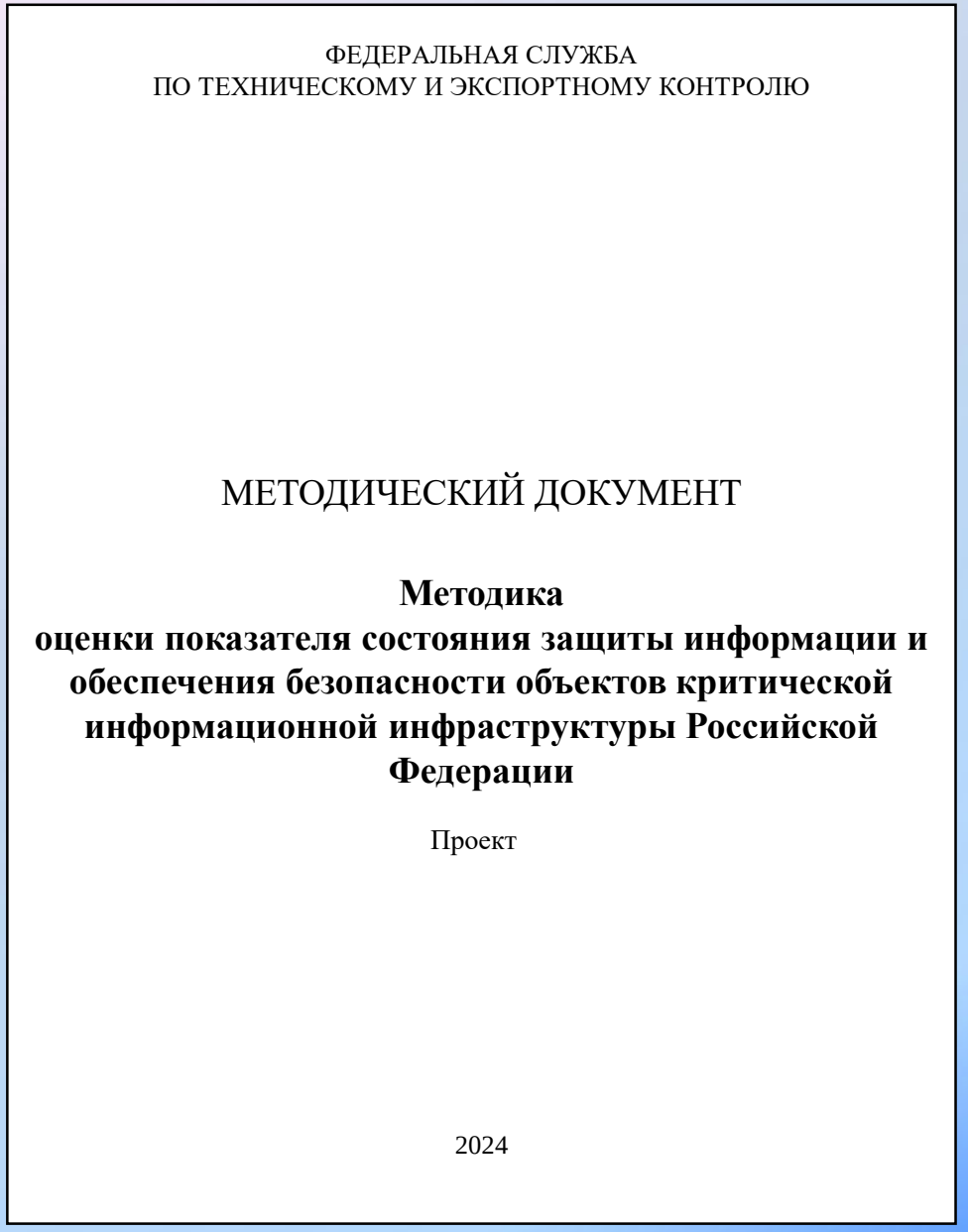
Нормативные правовые акты ФСТЭК России

Приказ ФСТЭ от 20 октября № 025 «Об утверждении по техническо информации, со сведения, соста государственну	Приказ ФСТЭК от 11 февраля 2 № 17 «Об утверждении Тр о защите информа составляющ государственную содержащейс государствен информационных с	Приказ ФСТЭК от 18 февраля 2 № 21 «Об утверждении С содержания организ и технических м обеспечению безоп персональных данн обработке в информ системах персона данных»	Приказ ФСТЭК Р от 6 декабря 20 № 227 «Об утверждении п ведения реестра зна объектов критиче информационн инфраструктур Российской Федер	Приказ ФСТЭК Ро от 11 декабря 201 № 229 «Об утверждении ф акта проверки»	Приказ ФСТЭК Рос от 21 декабря 2017 № 235 «Об утверждени требований к создан систем безопасно значимых объект критической информационно инфраструктуры Российской Федера	Приказ ФСТЭК Росси от 25 декабря 2017 г. № 239 «Об утверждении требова по обеспечению безопасно значимых объектов критической информацион инфраструктуры Российс Федерации»	Приказ ФСБ России и ФСТЭК России №416/№484 от 31 августа 2010 г. Об утверждении требований о защите информации, содержащихся в информационных системах общего пользования

Нормативные правовые акты ФСБ России

риказ ФСБ 24 июля 2 366 «Об утверж Положен Национал координаци центре компьютер инцидент	Приказ ФСБ 24 июля 2018 «Об утверж порядка об информа компьюте инцидентах субъектами	Приказ ФСБ от 6 мая 2019 «Об утверж требован средст обнаруж предупреж ликвида компьютерн	Приказ ФСБ России от 24 июля 2018 г. N 367 «Об утверждении перечня информации, представляемой в ГосСОПКА и порядка ее представления»

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


ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

Методика
оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации

Проект

2024

ЦЕЛЬ ПРИМЕНЕНИЯ:

Оценка степени достижения ОГВ и организациями минимально необходимого (базового) уровня защиты информации и значимых объектов КИИ от наиболее распространенных угроз безопасности информации

ОЦЕНИВАЕМЫЙ ПАРАМЕТР:

Показатель состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ ($К_{ЗИ}$)

ЭТАПЫ ОЦЕНКИ:

- ✓ Сбор и анализ исходных данных, необходимых для оценки
- ✓ Определение значений частных показателей безопасности
- ✓ Расчет показателя состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ и его сравнение с нормированным значением

ТИПОВЫЕ НЕДОСТАТКИ, СОЗДАЮЩИЕ ПРЕДПОСЫЛКИ ДЛЯ УСПЕШНОЙ РЕАЛИЗАЦИИ КОМПЬЮТЕРНЫХ АТАК

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

Наличие в программном обеспечении, используемом в информационных системах, уязвимостей критического уровня

Активные учетные записи уволенных работников

Использование для доступа к информационной инфраструктуре личных устройств работников

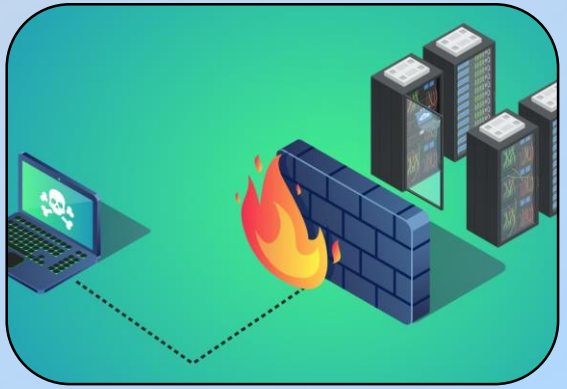
Использование на рабочих местах работников личных мессенджеров, социальных сетей

ДЛИНА ПАРОЛЯ (СИМВОЛОВ)	КОЛИЧЕСТВО ВАРИАНТОВ	ВРЕМЯ ПОДБОРА
1	36	менее секунды
2	1 296	менее секунды
3	46 656	менее секунды
4	1 679 616	17 секунд
5	60 466 176	10 минут
6	2 176 782 336	6 часов
7	78 364 164 096	9 дней
8	$2{,}821\ 109\ 9 \times 10^{12}$	11 месяцев
9	$1{,}015\ 599\ 5 \times 10^{14}$	32 года
10	$3{,}656\ 158\ 4 \times 10^{15}$	1 162 года
11	$1{,}316\ 217\ 0 \times 10^{17}$	41 823 года
12	$4{,}738\ 381\ 3 \times 10^{18}$	1 505 615 лет

ПЕРВООЧЕРЕДНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

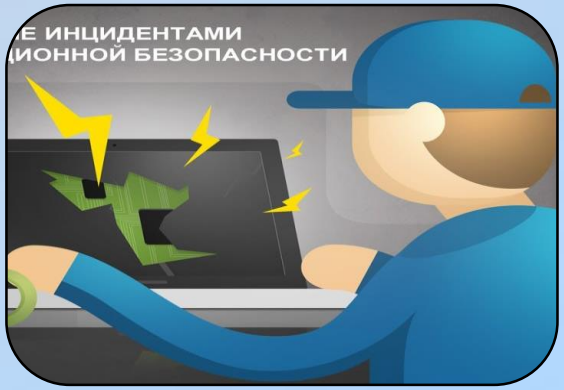
Инвентаризация информационных ресурсов

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

ЧАСТНЫЕ ПОКАЗАТЕЛИ

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
		4. Предоставлены своевременные ответы на запросы ФСТЭК России о выполнении мер по защите информации, рекомендованных к реализации (ответы представлены на более чем 95% запросов)	0,15

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 85% 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

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 85% устройств и серверов учтено)	0,10
		5. Обеспечена проверка вложений в электронных письмах на наличие вредоносного программного обеспечения (проверяются вложения для не менее чем 85% пользовательских устройств)	0,15
		6. Обеспечено централизованное управление средствами антивирусной защиты (не менее чем 85% пользовательских устройствах контролируются средствами антивирусной защиты под централизованным управлением). При этом обеспечены контроль и установка обновления 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 L3/L4 (заключен договор с провайдером)	0,10

ЧАСТНЫЕ ПОКАЗАТЕЛИ

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

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

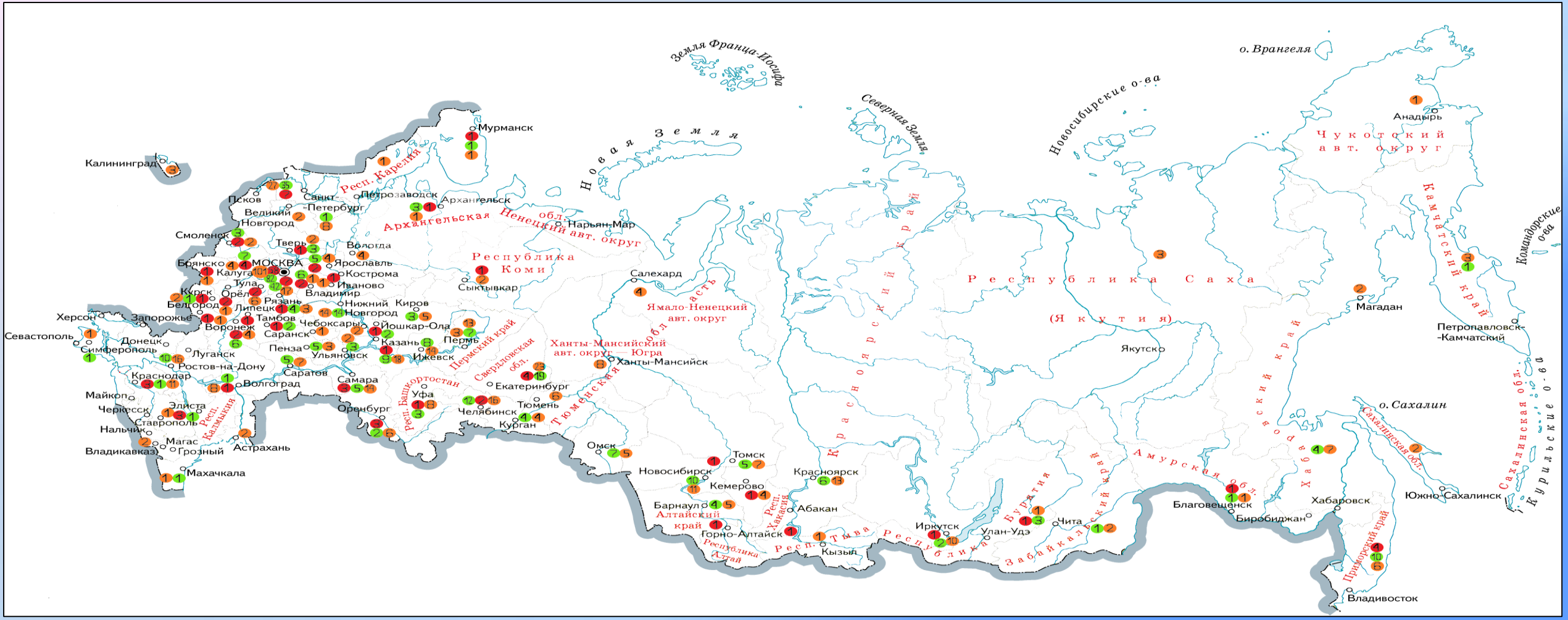
Где:

R_j – весовой коэффициент группы частных показателей безопасности

k_{ij} – значение частного показателя безопасности

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

РЕЗУЛЬТАТЫ ОЦЕНКИ ПОКАЗАТЕЛЯ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ



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 ($К_{ИБ} <=0,75$)

О методическом подходе к оценке текущего состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры в органах государственной власти и организациях

Начальник 9 управления ФСТЭК России

БОНДАРЕНКО Сергей Васильевич