МИНИСТЕРСТВО АРХИТЕКТУРЫ И СТРОИТЕЛЬСТВА СМОЛЕНСКОЙ ОБЛАСТИ

П Р И К А З

«09» 10 2025 №184-ОД

Об утверждении Регламента оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации Министерства архитектуры и строительства Смоленской области

В соответствии с учетом положений методического документа ФСТЭК России от 2 мая 2024 г. № 17 «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»,

п р и к а з ы в а ю:

1. Утвердить прилагаемый Регламент оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации Министерства архитектуры и строительства Смоленской области.
2. Контроль за исполнением настоящего приказа оставляю за собой.

Министр К.Н. Ростовцев

Приложение
к приказу Министерства архитектуры и строительства Смоленской области
от «09» 10 2025 г. № 184-ОД

Регламент оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации Министерства архитектуры и строительства Смоленской области

1. Общие сведения

1.1. Настоящий Регламент разработан с учетом положений методического документа ФСТЭК России от 2 мая 2024 г. «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

1.2. Целью разработки данного Регламента является определение Министерством архитектуры и строительства Смоленской области (далее – Министерство) порядка оценки показателя, характеризующего состояние технической защиты информации, не составляющей государственную тайну, и обеспечения безопасности объектов информатизации (далее – показатель КЗИ) Министерства.

1.3. Нормированное значение показателя КЗИ равно 1 (КЗИ = 1). Несоответствие показателя КЗИ нормативному значению указывает на наличие в Министерстве возможности реализации актуальных угроз безопасности информации или предпосылок для их реализации.

1.4. Показатель КЗИ характеризует степень достижения Министерством минимального необходимого уровня защищенности информации от актуальных угроз безопасности информации во временном интервале оценивания и заданных условиях эксплуатации объектов информатизации.

1.5. Оценка показателя КЗИ проводится 1 раз в 6 месяцев.

1.6. Внеочередная оценка показателя защищенности КЗИ проводится в следующих случаях:

– возникновения инцидента информационной безопасности, повлекшего наступление негативных последствий (возникновение значимого инцидента);

– развития (изменения) архитектуры объекта информатизации;

– запроса министра архитектуры и строительства Смоленской области о текущем значении показателя защищенности КЗИ;

– запроса ФСТЭК России.

1.7. Настоящий Регламент предназначен для сотрудников Министерства, привлекаемых для оценки показателя КЗИ.

2. Сокращения

2.1. Ответственное лицо за ИБ – заместитель министра, на которого возложены

полномочия по обеспечению информационной безопасности.

2.2. Специалист по ИБ – сотрудник, осуществляющий функции по обеспечению информационной безопасности Министерства.

2.3. Объект информатизации – информационная система, автоматизированная система, информационно-телекоммуникационная сеть или иной объект информатизации Министерства.

2.4. ФСТЭК России – федеральная служба по техническому и экспортному контролю.

2.5. ФСБ России – федеральная служба безопасности Российской Федерации.

3. Порядок оценки показателя

3.1. Оценка показателя КЗИ должна включать:

– сбор и анализ исходных данных, необходимых для оценки показателя КЗИ;

– определение значений частных показателей безопасности;

– расчет значения показателя КЗИ и его сравнение с нормированным значением;

– подведение итогов и планирование мероприятий по результатам оценки показателя.

3.2. Оценка показателя КЗИ проводится в отношении всех объектов информатизации Министерства, подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации. Включение в область оценки иных объектов информатизации Министерства осуществляется по решению министра архитектуры и строительства Смоленской области или ответственного лица за ИБ.

3.3. В случае, если объекты информатизации Министерства функционируют на базе информационно-телекоммуникационной инфраструктуры, данная информационно-телекоммуникационная инфраструктура включается в область оценки показателя КЗИ.

3.4. Оценка показателя КЗИ организуется ответственным лицом за ИБ.

3.5. К проведению мероприятия по оценке показателя КЗИ привлекаются специалисты по ИБ Министерства. Состав привлекаемых специалистов по ИБ определяется ответственным лицом за ИБ и включается в акт оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации, разрабатываемый в соответствии с пунктом 6.5 настоящего Регламента.

3.6. Оценка может проводиться на основе результатов внутреннего контроля или внешней оценки соответствия (аудита безопасности), мониторинга информационной безопасности, оценки защищенности и (или) аттестации объектов информатизации, иных мероприятий по изучению и контролю уровня защищенности информации.

3.7. В процессе подведения итогов и планирования мероприятий по результатам оценки показателя ответственное лицо за ИБ:

– доводит до министра архитектуры и строительства Смоленской области документы, фиксирующие результаты расчета значении показателя КЗИ, если расчетное значение показателя КЗИ не соответствует нормативному значению;

– организует планирование мероприятий (разработка плана), направленных на выполнение мер по защите информации, которые не реализованы или реализация которых

не обеспечивает защиту от типовых актуальных угроз безопасности информации, в соответствии с установленными в Министерстве целями по обеспечению защиты информации. Срок реализации мероприятий, определенных в плане, не должен превышать срок до проведения следующей плановой оценки КЗИ.

4. Сбор и анализ исходных данных, необходимых для оценки показателя защищенности

4.1. Исходными данными, необходимыми для оценки показателя КЗИ (далее – исходные данные), являются:

– акты, протоколы, иные документы, составленные по результатам государственного контроля в области защиты информации и (или) обеспечения безопасности объектов информатизации;

– отчеты, протоколы, иные документы, составленные по результатам внутреннего контроля уровня защищенности информации и (или) обеспечения безопасности объектов информатизации;

– отчеты, составленные по результатам внешней оценки соответствия в области защиты информации и (или) обеспечения безопасности объектов информатизации;

– внутренние организационно-распорядительные документы, регламентирующие организацию защиты информации и (или) обеспечение безопасности объектов информатизации;

– эксплуатационная документация на средства защиты информации, содержащая сведения об их настройках и конфигурации;

– результаты проведения инвентаризации объектов информатизации;

– результаты опроса (интервьюирования) сотрудника Министерства о выполнении ими функций (задач) с использованием объектов информатизации и (или) по обеспечению информационной безопасности;

– результаты анализа функционирования (применения) отдельных программных, программно-аппаратных средств объектов информатизации;

– результаты работы инструментальных средств оценки (анализа) защищенности объектов информатизации и (или) мониторинга информационной безопасности.

4.2. Ответственное лицо за ИБ определяет для сбора и анализа исходных данных наиболее подготовленных специалистов по ИБ, обладающих следующими компетенциями:

– знание целей, задач, основ организации защиты информации и обеспечения безопасности объектов информатизации;

– знание состава и содержания организационно-распорядительных документов по вопросам защиты информации и обеспечения безопасности объектов информатизации;

– знание процессов организации защиты информации и обеспечения безопасности объектов информатизации, умение их внедрять;

– знание основных методов и способов защиты информации и обеспечения безопасности объектов информатизации, умение их практически реализовывать.

4.3. По решению ответственного лица за ИБ для сбора и анализа исходных данных могут привлекаться сотрудники из других структурных подразделений Министерства,

обладающие необходимыми компетенциями.

4.4. Специалисты по ИБ не должны проводить оценку материалов, характеризующих (демонстрирующих, подтверждающих) результаты реализации ими собственных функций и (или) задач.

4.5. Задачи специалистов по ИБ:

– запрашивать в структурных подразделениях (филиалах, представительствах) Министерства требуемые для анализа документы и материалы;

– проводить опросы (интервьюирование) сотрудника Министерства о выполнении ими функций с использованием объектов информатизации и(или) по обеспечению информационной безопасности;

– осуществлять анализ функционирования отдельных программных, программно-аппаратных средств в объектах информатизации, в том числе средств защиты информации, средств инвентаризации объектов информатизации, инструментальных средств оценки защищенности и (или) мониторинга информационной безопасности.

4.6. В случае непредставления структурным подразделением и сотрудниками Министерства запрошенных для проведения оценки документов и материалов соответствующим частным показателям безопасности присваивается значение 0.

4.7. Результаты проведения опроса (интервьюирования) сотрудника Министерства о составе и порядке реализации ими функций (задач) в объектах информатизации и (или) обеспечении информационной безопасности документируются специалистами по ИБ в виде и в форме, определяемом самими специалистами по ИБ.

4.8. Собранные исходные данные подлежат анализу специалистами по ИБ с целью формирования выводов о реализации в Министерстве мероприятий (процессов) по защите информации (обеспечению безопасности объектов информатизации), о достаточности принимаемых мер по защите информации (обеспечению безопасности объектов информатизации). По результатам анализа исходных данных специалисты по ИБ формируют выводы о реализации мер, соответствующих частным показателям безопасности.

5. Определение значений частных показателей безопасности

5.1. Для расчета показателя КЗИ определяются значения частных показателей безопасности. Перечень используемых частных показателей безопасности (их идентификаторы и наименования, а также максимальные значения для каждого из них) приведены в Приложении № 1.

5.2. Частные показатели безопасности характеризуют реализацию в Министерстве отдельных мер по защите информации и обеспечения безопасности объектов информатизации от актуальных угроз безопасности информации, а также их соответствие целям обеспечения безопасности в Министерстве.

5.3. Определение значений частных показателей безопасности осуществляется специалистами по ИБ.

5.4. Частные показатели безопасности определяются для всех объектов информатизации, находящихся в распоряжении Министерства.

5.5. Определение значений частных показателей безопасности предусматривает присвоение им значений на основе результатов анализа материалов, подтверждающих выводы о достаточности реализованных мер по защите информации (обеспечению безопасности объектов информатизации) для блокирования (нейтрализации) актуальных угроз безопасности информации.

5.6. Если по результатам проведенного анализа материалов сделаны выводы, что меры по защите информации (обеспечению безопасности объектов информатизации) в Министерстве реализованы, соответствующему частному показателю присваивается максимальное значение, установленное для него (Приложение 1).

5.7. Если по результатам проведенного анализа материалов сделаны выводы, что соответствующая мера не реализована или реализована неэффективно (не в полном объеме), соответствующему частному показателю присваивается значение 0.

6. Расчет показателей защищенности и его сравнение с нормированным значением

6.1. Расчет показателя КЗИ осуществляется по следующей формуле:

КЗИ = (k11+k12+k13)*R1+(k21+k22+k23+k24)*R2+(k31+k32+k33+k34+k35+k36+k37)*R3+ +(k41+k42+k43)*R4

6.2. Если при очередном расчете показателя защищенности КЗИ фиксируется повторное (в течение 12 месяцев) невыполнение мер, предусмотренных частным показателем безопасности, и данному показателю безопасности повторно присвоено значение 0, то весовому коэффициенту этой группы показателей присваивается значение 0 (обнуляется вся группа показателей).

6.3. Рассчитанный показатель защищенности КЗИ сравнивается с нормированным значением, указанным в пункте 1.3 настоящего Регламента.

6.4. На основе результатов сравнения формируются выводы о текущем состоянии защиты информации в Министерстве. Возможные состояния защиты информации представлены в таблице 1.

Таблица 1 – Состояния защиты информации

Значение КЗИ	**Состояние защиты информации**
КЗИ=1	Обеспечивается минимальный уровень защиты от типовых актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как минимальный базовый («зеленый»)
0,75<КЗИ<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»)
КЗИ≤0,75	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности

Значение КЗИ	Состояние защиты информации
	информации. Уровень состояния защищенности характеризуется как критический («красный»)

6.5. Результаты оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации оформляются Актом оценки показателя состояния технической защиты и обеспечения безопасности объектов информатизации.

7. Взаимодействие с ФТЭК России в части результатов оценки показателя

7.1. Ответственное лицо за ИБ обязано, в случае получения запросов с ФСТЭК России, обеспечить предоставление в сроки, установленные запросом, но не превышающие 30 дней:

7.1.1. Последних результатов оценки показателя КЗИ.

7.1.2. Отдельных исходных данных, используемых для оценки показателя КЗИ, подтверждающих получение представленных результатов оценки.

7.2. В случае получения от ФСТЭК России сведений о том, что в результате верификации ФТСЭК России результатов расчета показателя КЗИ значение было уточнено, ответственное лицо за ИБ должен обеспечить проведение внеочередной оценки показателя КЗИ.

8. Ответственность

8.1. Ответственное лицо за ИБ и специалисты по ИБ несут персональную ответственность за ненадлежащее исполнение или неисполнение положений, предусмотренных настоящим Регламентом.

Приложение № 1
к регламенту оценки показателя КЗИ Министерства архитектуры и строительства Смоленской области

Перечень используемых частных показателей безопасности и их значения

Идентификатор группы	Наименование групп показателей	Весовой коэффициент группы показателей	Идентификатор частного показателя	Наименование показателя безопасности	Значение частного показателя
R1	Организация и управление	0,1	k11	На заместителя руководителя органа (организации) возложены[1] полномочия ответственного лица за обеспечение информационной безопасности органа (организации) и определены его обязанности	0,30
			k12	Определены функции (обязанности) структурного подразделения (или отдельных сотрудников), ответственного за обеспечение информационной безопасности органа (организации)	0,40
			k13	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[2]	0,30
R2	Защита пользователей	0,25	k21	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
			k22	Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации	0,30

[1]) Возложение полномочий и (или) определение структурного подразделения (сотрудника) органа (организации) подтверждается изданием соответствующего локального правового акта.

[2]) В случае если подрядные организации не привлекаются, частному показателю безопасности k13 присваивается значение из приложения.

Идентификатор группы	Наименование групп показателей	Весовой коэффициент группы показателей	Идентификатор частного показателя	Наименование показателя безопасности	Значение частного показателя
				не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)[3]	
			k23	Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию	0,20
			k24	Отсутствуют активные учетные записи сотрудников органа (организации) и сотрудников, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения	0,20
R3	Защита информационных систем	0,35	k31	На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет[4], контролируется межсетевыми экранами уровня L3/L4)	0,20
			k32	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
			k33	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	0,10

[3]) В случае отсутствия технической возможности реализации на объектах информатизации или в технических средствах двухфакторной аутентификации соответствующему показателю безопасности присваивается значение из приложения.
[4]) В случае отсутствия в объектах информатизации устройств, интерфейсов, взаимодействующих с сетью Интернет, соответствующим показателям безопасности присваиваются значения из приложения.

Идентификатор группы	Наименование групп показателей	Весовой коэффициент группы показателей	Идентификатор частного показателя	Наименование показателя безопасности	Значение частного показателя
				отношении таких уязвимостей реализованы компенсирующие меры	
			k34	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
			k35	Обеспечена проверка вложений в электронных письмах электронной почты[5] на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств)	0,15
			k36	Обеспечено централизованное управление средствами антивирусной защиты[6] (не менее чем 80% пользовательских устройств[7] 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
			k37	Реализована очистка входящего из сети Интернет сетевого трафика от аномалий на уровне[8] L3/L4 (заключен договор с провайдером)	0,10
R4	Мониторинг информацион	0,3	k41	Реализован централизованный сбор событий безопасности и оповещение о	0,40

[5]) В случае если в объектах информатизации не используется электронная почта, частному показателю безопасности k35 присваиваются значение из приложения.

[6]) Если в органе (организации) используются автономные рабочие места, на них должны быть установлены автономные средства антивирусной защиты (тип «Г»). В этом случае частному показателю безопасности k36 присваивается значение из приложения.

[7]) Если объекты информатизации содержат пользовательские устройства, в которых конструктивно отсутствуют интерфейсы для возможного внедрения вредоносного программного обеспечения, частному показателю безопасности k36 присваивается значение из приложения.

[8]) Если в объектах информатизации отсутствуют веб-сайт или иные сервисы, подверженные DDos-атакам, частному показателю безопасности k37 присваивается значение из приложения.

Идентификатор группы	Наименование групп показателей	Весовой коэффициент группы показателей	Идентификатор частного показателя	Наименование показателя безопасности	Значение частного показателя
	ной безопасности и реагирование			неудачных попытках входа для привилегированных учетных записей	
			k42	Реализован централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с сетью Интернет	0,35
			k43	3. Утвержден документ, определяющий порядок реагирования на компьютерные инциденты	0,25