КонсультантПлюс

"Методический документ "Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (утв. ФСТЭК России 02.05.2024)

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

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее - Методика) разработана 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.

2. Настоящая Методика 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.

3. Настоящая Методика применяется для оценки 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.

В качестве минимально необходимого уровня защиты информации (обеспечения безопасности объектов КИИ) задан состав мер, реализация которых предусмотрена нормативными правовыми актами Российской Федерации <1>, и который минимально достаточен для блокирования (нейтрализации) типовых актуальных угроз безопасности информации.

<1> Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. N 17.

Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых предприятиями оборонно-промышленного комплекса, утвержденные приказом ФСТЭК России от 28 февраля 2017 г. N 31.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. N 239.

Требования к обеспечению защиты информации в автоматизированных системах управления производственными процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2013 г. N 31.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные

приказом ФСТЭК России от 18 февраля 2013 г. N 21.

4. Несоответствие значения показателя, характеризующего текущее состояние защиты информации (обеспечения безопасности объектов КИИ), установленному в соответствии с настоящей Методикой нормированному значению указывает на наличие в органе (организации) возможности реализации актуальных угроз безопасности информации или предпосылок для их реализации.

5. Настоящая Методика применяется:

а) ФСТЭК России - для мониторинга в пределах своей компетенции текущего состояния защиты информации и обеспечения безопасности объектов КИИ в органах (организациях);

б) органом (организацией) - для оценки текущего состояния защиты информации и (или) обеспечения безопасности объектов КИИ и разработки на основе такой оценки мер по повышению уровня защищенности, а также оценки эффективности деятельности заместителя руководителя органа (организации), на которого возложены полномочия по обеспечению информационной безопасности органа (организации), и (или) структурного подразделения, осуществляющего функции по обеспечению информационной безопасности органа (организации) <2>.

<2> Указ Президента Российской Федерации от 1 мая 2022 г. N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"

6. Методика не применяется для оценки деятельности в области обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

II. ПОКАЗАТЕЛЬ ЗАЩИЩЕННОСТИ И ЕГО НОРМИРОВАННОЕ ЗНАЧЕНИЕ

7. В качестве показателя, характеризующего текущее состояние защиты информации (обеспечения безопасности объектов КИИ) в органе (организации), используется показатель текущего состояния защищенности $К_{зи}$ (далее - показатель защищенности $К_{зи}$, показатель $К_{зи}$).

Показатель $К_{зи}$ характеризует степень достижения органом (организацией) минимально необходимого уровня защиты информации (обеспечения безопасности объектов КИИ) от типовых актуальных угроз безопасности информации во временном интервале оценивания и заданных условиях эксплуатации информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, иных объектов информатизации.

8. Информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, иные объекты информатизации и содержащаяся в них информация (далее - информационные системы) органа (организации) имеют минимально необходимый уровень защищенности от типовых актуальных угроз безопасности информации, если значение показателя $К_{зи}$ соответствует нормированному значению:

$$К_{зи} = 1.$$

9. Полученное в соответствии с настоящей Методикой значение показателя защищенности $К_{зи}$ является критерием принятия в органе (организации) управленческих решений в части необходимости реализации первоочередных мер по защите информации (обеспечению безопасности объектов КИИ) от актуальных угроз безопасности информации и их приоритетности.

III. ПОРЯДОК ОЦЕНКИ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ

10. Оценка показателя защищенности $К_{зи}$ включает:

а) сбор и анализ исходных данных, необходимых для оценки показателя $К_{зи}$;

б) оценку значений частных показателей безопасности k_{ji};

в) расчет значения показателя $К_{ЗИ}$ и его сравнение с нормированным значением.

11. Оценка показателя $К_{ЗИ}$ проводится не реже одного раза в шесть месяцев. Периодичность и порядок проведения оценки показателя $К_{ЗИ}$ устанавливается органом (организацией) во внутренних регламентах.

12. Оценка показателя защищенности $К_{ЗИ}$ проводится в отношении всех информационных систем, подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации. Включение в область оценки иных информационных систем органа (организации) осуществляется по решению руководителя (ответственного заместителя руководителя) органа (организации).

В случае если информационные системы органа (организации) функционируют на базе информационно-телекоммуникационной инфраструктуры, данная информационно-телекоммуникационная инфраструктура включается в область оценки показателя защищенности $К_{ЗИ}$.

13. В органе (организации) оценка показателя $К_{ЗИ}$ организуется заместителем руководителя органа (организации), на которого возложены полномочия по обеспечению информационной безопасности органа (организации), и проводится структурным подразделением, специалистами по защите, осуществляющими функции по обеспечению информационной безопасности органа (организации). Указанная оценка может проводиться на основе результатов внутреннего контроля или внешней оценки соответствия (аудита безопасности), мониторинга информационной безопасности, оценки защищенности и (или) аттестации информационных систем, иных мероприятий по изучению и контролю уровня защищенности информации.

14. О полученном по результатам расчета значении показателя $К_{ЗИ}$, не соответствующем нормированному значению, информируется руководитель органа (организации) для принятия решения о необходимости совершенствования (улучшения) принимаемых в органе (организации) мер по защите информации (обеспечению безопасности объектов КИИ).

15. Результаты оценки показателя защищенности $К_{ЗИ}$ предоставляются органом (организацией) в ФСТЭК России по ее запросу в целях оценки текущего состояния защиты информации и обеспечения безопасности объектов в соответствии с подпунктом 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 могут быть запрошены отдельные исходные данные, используемые для оценки показателя защищенности $К_{ЗИ}$, подтверждающие получение представленных результатов оценки.

ФСТЭК России принимаются меры по обеспечению конфиденциальности информации, представляемой органами (организациями).

16. ФСТЭК России проводится анализ поступивших результатов оценки показателя $К_{ЗИ}$ и (или) исходных данных, используемых для его оценки, осуществляется верификация результатов его расчета и делается вывод о текущем состоянии защиты информации и (или) обеспечения безопасности объектов КИИ в органе (организации).

В случае если по запросу ФСТЭК России органом (организацией) результаты оценки показателя защищенности $К_{ЗИ}$ и (или) материалы (часть материалов), используемые для его оценки, в течение 30 дней не представлены, показателю $К_{ЗИ}$ и (или) соответствующим частным показателям безопасности k_{ji} присваивается значение 0.

Значение показателя $К_{ЗИ}$ органа (организации) может быть уточнено ФСТЭК России в соответствии с выводами о достаточности принимаемых мер по защите информации (обеспечению безопасности объектов КИИ), сделанными по результатам государственного контроля, проведенного в пределах ее полномочий, и (или) на основе результатов анализа документов, иных материалов, предоставленных по запросу ФСТЭК России органом (организацией).

О значении показателя защищенности $К_{ЗИ}$, определенном ФСТЭК России, в случае его не

соответствия нормированному значению информируется орган (организация).

17. В случае если значение показателя защищенности $К_{ЗИ}$ не соответствует нормированному значению, в органе (организации) на основе полученных значений частных показателей k_{ji} определяются меры по защите информации (обеспечению безопасности объектов КИИ), которые не реализованы или реализация которых не обеспечивает защиту от типовых актуальных угроз безопасности информации, и приоритетность их реализации, а также планируются мероприятия по реализации (совершенствованию) мер в соответствии с установленными целями по обеспечению защиты информации (обеспечению безопасности объектов КИИ).

18. Внеочередная оценка показателя защищенности $К_{ЗИ}$ проводится в органе (организации) в случаях:

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

б) развития (изменения) архитектуры информационных систем;

в) запроса руководителя органа (организации) о текущем значении показателя защищенности $К_{ЗИ}$;

г) запроса ФСТЭК России.

IV. СБОР И АНАЛИЗ ИСХОДНЫХ ДАННЫХ, НЕОБХОДИМЫХ ДЛЯ ОЦЕНКИ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ

19. Исходными данными, необходимыми для оценки показателя защищенности $К_{ЗИ}$ (далее - исходные данные), могут являться:

а) акты, протоколы, иные документы, составленные по результатам государственного контроля в области защиты информации (обеспечения безопасности объектов КИИ);

б) отчеты, протоколы, иные документы, составленные по результатам внутреннего контроля уровня защищенности информации (обеспечения безопасности объектов КИИ);

в) отчеты, составленные по результатам внешней оценки соответствия в области защиты информации (обеспечения безопасности объектов КИИ);

г) внутренние организационно-распорядительные документы, регламентирующие организацию защиты информации (обеспечение безопасности объектов КИИ) в органе (организации);

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

е) результаты проведения инвентаризации информационных систем;

ж) результаты опроса (интервьюирования) работников органа (организации) о выполнении ими функций (задач) с использованием информационных систем и (или) по обеспечению информационной безопасности;

з) результаты анализа функционирования (применения) отдельных программных, программно-аппаратных средств информационных систем органа (организации);

и) результаты работы инструментальных средств оценки (анализа) защищенности информационных систем и (или) мониторинга информационной безопасности.

20. Для сбора и анализа исходных данных назначаются наиболее подготовленные специалисты из состава структурного подразделения, осуществляющего функции по обеспечению информационной безопасности органа (организации) (далее - специалисты по сбору и анализу исходных данных). Рекомендуется назначать специалистов, обладающих следующими компетенциями:

а) знание целей, задач, основ организации защиты информации (обеспечения безопасности объектов КИИ);

б) знание состава и содержания организационно-распорядительных документов по вопросам защиты информации (обеспечения безопасности объектов КИИ);

в) знание процессов организации защиты информации (обеспечения безопасности объектов КИИ) и умение их внедрять;

г) знание основных методов и способов защиты информации (обеспечения безопасности объектов КИИ) и умение их практически реализовывать.

По решению заместителя руководителя органа (организации), ответственного за обеспечение информационной безопасности, для сбора и анализа исходных данных могут привлекаться специалисты из других структурных подразделений, обладающие необходимыми компетенциями.

21. Специалисты по сбору и анализу исходных данных не должны проводить оценку материалов, характеризующих (демонстрирующих, подтверждающих) результаты реализации ими собственных функций и (или) задач.

22. Порядок назначения специалистов по сбору и анализу исходных данных, сроков сбора и анализа исходных данных определяется органом (организацией) во внутренних регламентах с учетом положений настоящей Методики.

23. Специалисты по сбору и анализу исходных данных:

а) запрашивают в структурных подразделениях (филиалах, представительствах) органа (организации) требуемые для анализа документы и материалы;

б) проводят опросы (интервьюирование) работников органа (организации) о выполнении ими функций с использованием информационных систем и (или) по обеспечению информационной безопасности;

в) осуществляют анализ функционирования отдельных программных, программно-аппаратных средств в информационных системах, в том числе средств защиты информации, средств инвентаризации информационных систем, инструментальных средств оценки защищенности и (или) мониторинга информационной безопасности.

Подразделения и специалисты органа (организации), привлекаемые для сбора исходных данных, оказывают содействие и принимают исчерпывающие меры для предоставления документов и материалов, требуемых для анализа.

В случае непредставления структурным подразделением и привлекаемыми специалистами органа (организации) запрошенных для проведения оценки документов и материалов соответствующим частным показателям безопасности k_{ji} присваивается значение 0.

24. Результаты проведения опроса (интервьюирования) работников органа (организации) о составе и порядке реализации ими функций (задач) в информационных системах и (или) обеспечении информационной безопасности подлежат документированию в виде и в форме, определяемыми органом (организацией).

25. Собранные исходные данные подлежат анализу специалистами по сбору и анализу исходных данных с целью формирования выводов о реализации в органе (организации) мероприятий (процессов) по защите информации (обеспечению безопасности объектов КИИ), о достаточности принимаемых мер по защите информации (обеспечению безопасности объектов КИИ). По результатам анализа исходных данных специалисты формируют выводы о реализации мер, соответствующих частным показателям безопасности k_{ji}.

26. Полученные результаты анализа исходных данных, а также результаты расчета значений показателя защищенности $К_{ЗИ}$ подлежат документированию в виде и по форме, определяемой органом

(организацией), и направляются в ФСТЭК России в случае поступления запроса.

V. ОПРЕДЕЛЕНИЕ ЗНАЧЕНИЙ ЧАСТНЫХ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ

27. Для оценки показателя защищенности $К_{ЗИ}$ определяются значения частных показателей безопасности k_{ji}, где j - номер группы частных показателей безопасности, i - номер частного показателя в соответствующей группе показателей безопасности.

Частные показатели безопасности k_{ji} характеризуют реализацию в органе (организации) отдельных мер по защите информации (обеспечению безопасности объектов КИИ) от актуальных угроз безопасности информации, а также их соответствие целям обеспечения безопасности в органе (организации).

28. Определение значений частных показателей безопасности k_{ji} осуществляется специалистами, проводившими сбор и анализ исходных данных.

29. Перечень используемых частных показателей безопасности k_{ji}, их наименования и максимальные значения приведены в таблице 1.

30. Частные показатели безопасности k_{ji} определяются для всех информационных систем, подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации, находящихся в распоряжении органа (организации).

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

32. Если по результатам проведенного анализа материалов сделаны выводы, что меры по защите информации (обеспечению безопасности объектов КИИ) в органе (организации) реализованы, соответствующему частному показателю присваивается значение, установленное для него в таблице 1.

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.

Таблица 1

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	
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) <5>	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	
3.	Защита информационных систем	1. На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет <6>, 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 <7> на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств)	0,15	
		6. Обеспечено централизованное управление	0,15	

		средствами антивирусной защиты <8> (не менее чем 80% пользовательских устройств <9> 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		
		7. Реализована очистка входящего из сети Интернет сетевого трафика от аномалий на уровне <10> L3/L4 (заключен договор с провайдером)	0,10	
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	

<3> Возложение полномочий и (или) определение структурного подразделения (работников) в органе (организации) подтверждается изданием соответствующего локального правового акта.

<4> В случае если подрядные организации не привлекаются, частному показателю безопасности k_{13} присваивается значение из таблицы 1.

<5> В случае отсутствия технической возможности реализации в информационной системе или в технических средствах двухфакторной аутентификации соответствующему показателю безопасности присваивается значение из таблицы 1.

<6> В случае отсутствия в информационных системах устройств, интерфейсов, взаимодействующих с сетью Интернет, соответствующим показателям безопасности присваиваются значения из таблицы 1.

<7> В случае если в информационных системах органа (организации) не используется электронная почта, частному показателю безопасности k_{35} присваиваются значение из таблицы 1.

<8> 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 k_{36} присваивается значение из таблицы 1.

<9> Если информационные системы содержат пользовательские устройства, в которых конструктивно отсутствуют интерфейсы для возможного внедрения вредоносного программного обеспечения, частному показателю безопасности k_{36} присваивается значение из таблицы 1.

<10> Если в информационных системах отсутствуют веб-сайт или иные сервисы, подверженные DDos-атакам, частному показателю безопасности k_{37} присваивается значение из таблицы 1.

VI. РАСЧЕТ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ И ЕГО СРАВНЕНИЕ С НОРМИРОВАННЫМ ЗНАЧЕНИЕМ

33. Расчет показателя защищенности $К_{ЗИ}$ осуществляется по следующей формуле:

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

где R_j - весовой коэффициент j-й группы частных показателей безопасности, определяемый в соответствии с таблицей 1.

34. Если при очередном расчете показателя защищенности $К_{ЗИ}$ фиксируется повторное (в течение 12 месяцев) невыполнение мер, предусмотренных частным показателем безопасности k_{ji}, и данному показателю безопасности повторно присвоено значение 0, то весовому коэффициенту этой группы показателей R_j присваивается значение 0 (обнуляется вся группа показателей).

35. Рассчитанный в соответствии с пунктом 33 показатель защищенности $К_{ЗИ}$ сравнивается с нормированным значением. На основе результатов сравнения формируются выводы (таблица 2) о текущем состоянии защиты информации (обеспечения безопасности объектов КИИ) в органе (организации).

Таблица 2

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")
$К_{ЗИ} \leq 0,75$	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")

36. В случае если по результатам расчета получено значение показателя защищенности $К_{ЗИ}$, характеризующее текущее состояние защищенности в органе (организации) как низкое ("оранжевый") или критическое ("красный"), разрабатывается план реализации мероприятий по достижению следующего уровня защиты от актуальных угроз. Срок реализации мероприятий, определенных в плане, не должен превышать срок до проведения следующей плановой оценки показателя $К_{ЗИ}$.