ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
7 августа 2026 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

2026

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Методика оценки уровня зрелости деятельности в области технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее – Методика) разработана в соответствии с подпунктами 4 и 6.5 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

2. Настоящая Методика определяет порядок оценки уровня зрелости деятельности в области технической защиты информации, не составляющей государственную тайну, содержащейся в информационных системах (далее – защита информации), и(или) обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее – обеспечение безопасности значимых объектов КИИ).

3. Настоящая Методика применяется для оценки уровня зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), требования к которой установлены ФСТЭК России в соответствии с законодательством Российской Федерации о безопасности критической информационной инфраструктуры, об информации, информационных технологиях и о защите информации, о персональных данных[1].

---

[1] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 апреля 2025 г. № 117.

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. № 31.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 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. № 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. № 21.

4. Настоящая Методика применяется:

а) операторами информационных систем, владельцами значимых объектов критической информационной инфраструктуры (далее – операторы) – для оценки уровня зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), осуществляемой при эксплуатации информационных систем (значимых объектов КИИ);

б) подрядными организациями – для подтверждения уровня зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), осуществляемой при оказании услуг, проведении работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационных систем, а также при выполнении работ, оказании услуг по защите информации (в случае если при оказании услуг осуществляется доступ в информационные системы заказчика, либо осуществляется обработка информации, принадлежащей заказчику);

в) государственными органами, организациями, в том числе субъектами критической информационной инфраструктуры, являющими заказчиками услуг, работ (далее – органы (организации) – для установления требований к уровню зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), осуществляемой подрядными организациями при оказании услуг, проведении работ, в соответствии с нормативными правовыми актами, установленными ФСТЭК России;

г) ФСТЭК России – для оценки эффективности деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), осуществляемой операторами, на основе результатов проведенной ими оценки уровня зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ);

д) операторами информационных систем персональных данных – для подтверждения уровня зрелости деятельности в области обеспечения безопасности персональных данных, обрабатываемых в информационных системах

персональных данных, а также для установления требований к уровню зрелости осуществляемой подрядными организациями при оказании услуг, проведении работ, в соответствии с нормативными правовыми актами, установленными ФСТЭК России.

5. Операторами оценка уровня зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ) проводится в случаях, если они самостоятельно с использованием собственных сил и средств реализуют мероприятия (процессы) и соответствующие меры по защите информации (обеспечению безопасности значимых объектов КИИ). В случае, если оператор для обеспечения эксплуатации информационных систем, обработки информации и(или) реализации мероприятий (процессов) и мер по защите информации (обеспечению безопасности значимых объектов КИИ) привлекает подрядную организацию, оператор является заказчиком и устанавливает требования к уровню зрелости привлекаемой подрядной организации. Требования к уровню зрелости деятельности подрядной организации определяются в документах, на основании которых оказываются услуги, проводятся работы.

6. Оценка уровня зрелости может проводиться самостоятельно (внутренняя оценка уровня зрелости) или с привлечением внешней организации, имеющей лицензию на деятельность в области защиты конфиденциальной информации (в части услуг по контролю защищенности информации от несанкционированного доступа и ее модификации в средствах и системах информатизации) (внешняя оценка уровня зрелости). Внешняя оценка уровня зрелости имеет более высокую объективность ввиду независимости результата от управленческих, административных и иных решений руководителя (ответственного лица) оператора, в отношении которого проводится оценка.

II. УРОВЕНЬ ЗРЕЛОСТИ И ПОРЯДОК ЕГО ОЦЕНКИ

7. Уровень зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ) ($У_{зи}$) является показателем, характеризующим качество данной деятельности, и оказывающим существенное

влияние на эффективность и результативность реализуемых мероприятий (процессов) и мер по защите информации (обеспечению безопасности значимых объектов КИИ).

8. Оценка уровня зрелости ($У_{зи}$) включает:

а) определение оцениваемых направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) (*N*);

б) сбор и анализ исходных данных, необходимых для проведения оценки текущего уровня зрелости;

в) определение текущего уровня зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) ($У_{зит i}$);

г) определение целевого уровня зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) ($У_{зиц i}$);

д) построение диаграммы профиля уровней зрелости;

е) определение уровня зрелости деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зи}$ на основе результатов расчета текущего уровня зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$.

9. Уровень зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ) $У_{зи}$ может иметь одно из четырех значений. Самый низкий уровень зрелости - «начальный», самый высокий — «верифицируемый». Отсутствие уровня зрелости характеризуется значением «нулевой (отсутствует)». Возможные значения уровня зрелости $У_{зи}$ и их характеристика приведены в таблице 1.

Таблица 1

Значение уровня зрелости $У_{зи}$	**Наименование и используемый для интерпретации цвет**	**Характеристика обобщенного уровня зрелости $У_{зи}$**
$У_{зи} < 1$	Нулевой (отсутствует)	Управление деятельностью не осуществляется, не соответствует

		требованиям. Мероприятия (процессы) и меры не реализованы
$1 \leq У_{зи} < 2$	Начальный	Управление деятельностью формально осуществляется, соответствует требованиям, допускаются отдельные недостатки. Мероприятия (процессы) и меры реализованы не в полной мере или с отдельными недостатками
$2 \leq У_{зи} < 3$	Системный	Управление деятельностью осуществляется на системном уровне, реализованы все требования к управлению деятельностью. Мероприятия (процессы) и меры реализуются в соответствии с установленными требованиями с учетом результатов выявления и оценки актуальных угроз и уязвимостей
$3 \leq У_{зи} < 4$	Контролируемый	Управление деятельностью осуществляется на системном уровне, реализованы все требования к управлению деятельностью. Мероприятия (процессы) и меры реализуются в соответствии с установленными требованиями, осуществляется периодическая проверка
$У_{зи} \geq 4$	Верифицируемый	Управление деятельностью осуществляется на системном уровне, реализованы все требования к управлению деятельностью. Мероприятия (процессы) и меры реализуются в соответствии с установленными требованиями и эффективность их реализации периодически проверяется с привлечением внешней (независимой) организации

10. Уровень зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ) $У_{зи}$ определяется после

расчета текущего уровня зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ и рассчитывается по формуле:

$$У_{зи} = \frac{\sum_{i=1}^{N} У_{зит i}}{N}, \text{ где}$$

N – количество направлений деятельности;

$i \in [1; N]$ – направление деятельности;

$У_{зит i} \in [0; 4]$ – текущий уровень зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ).

В соответствии с полученным числовым значением по таблице 1 определяется уровень зрелости $У_{зи}$ деятельности по защите информации (обеспечению безопасности значимых объектов КИИ).

11. Для операторов государственных информационных систем 3 класса защищенности, иных информационных систем государственных органов, государственных предприятий и учреждений, операторов информационных систем персональных данных 4 и 3 уровней защищенности, значимых объектов критической информационной инфраструктуры 3 категории значимости, а также подрядных организаций, оказывающих услуги, выполняющих работы при эксплуатации данных систем, рекомендуется устанавливать целевой уровень зрелости каждого (i) направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$ не ниже «1».

Для операторов государственных информационных систем 2 класса защищенности, операторов информационных систем персональных данных 2 уровня защищенности, значимых объектов критической информационной инфраструктуры 2 категории значимости, а также подрядных организаций, оказывающих услуги, выполняющих работы при эксплуатации данных систем, рекомендуется устанавливать целевой уровень зрелости каждого (i) направления

деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$ не ниже «2».

Для операторов государственных информационных систем 1 класса защищенности, операторов информационных систем персональных данных 1 уровня защищенности, значимых объектов критической информационной инфраструктуры 1 категории значимости, а также подрядных организаций, оказывающих услуги, выполняющих работы при эксплуатации данных систем, рекомендуется устанавливать целевой уровень зрелости каждого (*i*) направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$ не ниже «3».

III. ОЦЕНИВАЕМЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ) И ЦЕЛЕВОЙ УРОВЕНЬ ЗРЕЛОСТИ

12. При определении уровня зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ) $У_{зи}$ оценке подлежат базовые направления данной деятельности, представляющие собой установленные требованиями по защите информации (обеспечению безопасности) мероприятия (процессы) и соответствующие им меры по защите информации (обеспечению безопасности значимых объектов КИИ).

Оценка уровня зрелости проводится по следующим направлениям деятельности (областям оценки):

1) организация и управление деятельностью;

2) выявление и оценка угроз безопасности информации;

3) контроль конфигураций информационных систем;

4) управление уязвимостями;

5) управление обновлениями;

6) защита информации при обращении с информацией ограниченного доступа;

7) защита информации при применении конечных устройств;

8) защита информации при применении мобильных устройств;

9) защита удаленного доступа;

10) защита беспроводного доступа;

11) защита привилегированного доступа;

12) мониторинг информационной безопасности;

13) разработка безопасного программного обеспечения;

14) физическая защита;

15) непрерывность функционирования;

16) повышение уровня знаний и информированности;

17) защита информации при взаимодействии с подрядными организациями;

18) защита от компьютерных атак, направленных на отказ в обслуживании;

19) защита информации при использовании искусственного интеллекта;

20) защита информационных систем и содержащейся в них информации;

21) контроль уровня защищенности.

13. В область оценки могут включаться дополнительные направления деятельности по обеспечению информационной безопасности, установленные отраслевыми, ведомственными требованиями в области защиты информации и информационной безопасности.

В случае, если направления деятельности являются неприменимыми (неактуальными) для органа (организации) вследствие отсутствия применяемых технологий и (или) технологических и архитектурных особенностей информационных систем, а также значимых объектов критической информационной инфраструктуры, то они исключаются из области оценки.

14. Для каждого из оцениваемых направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) задается целевое значение уровня зрелости направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$, которое характеризует ожидаемый результат качества деятельности по защите информации (обеспечению безопасности значимых объектов КИИ).

15. Целевой уровень зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$

определяется оператором самостоятельно исходя из ожидаемых результатов качества деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), осуществляемой при эксплуатации информационных систем (значимых объектов КИИ), а также рекомендаций, указанных в пункте 11 настоящей Методики.

16. Оцениваемые направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) и их целевые значения уровней зрелости образуют профиль уровня зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ).

17. По результатам профилирования осуществляется построение диаграммы профиля уровней зрелости, на которой указываются значения текущих уровней зрелости каждого (*i*) направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ и значения целевого уровня зрелости каждого (*i*) направления деятельности органа (организации) по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$.

Графическая интерпретация целевых уровней зрелости направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц}$ на основе результатов определения текущих уровней зрелости направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ представлена на рисунке 1.

Рисунок 1 Профиль уровня зрелости на основе определения текущих уровней зрелости каждого из направлений деятельности

18. Определив текущий уровень зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ и сравнив их с целевым уровнем зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$, выявляются недостатки в организации и управлении деятельностью по защите информации (обеспечению безопасности значимых объектов КИИ), в обеспечении реализации мероприятий (процессов) и мер по защите информации (обеспечению безопасности значимых объектов КИИ), определяются направления совершенствования (улучшения) данной деятельности.

IV. СБОР И АНАЛИЗ ИСХОДНЫХ ДАННЫХ, НЕОБХОДИМЫХ ДЛЯ ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ

19. Исходными данными, необходимыми для оценки уровня зрелости $У_{зи}$ (далее – исходные данные), являются:

а) политика защиты информации (обеспечения безопасности значимых объектов КИИ);

б) приказы, распоряжения, указания, иные организационно-распорядительные документы, устанавливающие полномочия (функции) и права лиц, ответственных за обеспечение защиты информации (обеспечение безопасности значимых объектов КИИ);

в) приказы, распоряжения, указания, иные организационно-распорядительные документы, устанавливающие полномочия (функции) и права подразделений;

г) внутренние стандарты, регламенты по защите информации, иные организационно-распорядительные документы, регламентирующие деятельность по защите информации (обеспечению безопасности значимых объектов КИИ) и по обеспечению функционирования и эксплуатации информационных систем, и обработке информации;

д) план мероприятий по совершенствованию защиты информации (обеспечения безопасности значимых объектов КИИ), содержащейся в информационных системах;

е) отчеты, протоколы, иные документы, составленные по результатам проведения мероприятий и принятия мер по защите информации (обеспечению безопасности значимых объектов КИИ);

ж) результаты последней оценки уровня зрелости (при наличии);

з) отчеты, составленные по результатам проведения контроля и анализа защищенности информационных систем;

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

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

л) результаты наблюдения за деятельностью работников с использованием информационных систем;

м) результаты наблюдения за функционированием отдельных программных, программно-аппаратных средств информационной инфраструктуры;

н) результаты работы инструментальных средств оценки (анализа) защищенности информации и (или) мониторинга информационной безопасности, иных программных средств и систем и иные исходные данные по базовым направлениям (областям оценки).

20. Для оценки уровня зрелости $У_{зи}$ могут применяться следующие инструменты:

а) программные платформы, объединяющие управление корпоративными процессами, контроль рисков и соблюдение нормативных требований (GRC-системы);

б) программные платформы оркестрации, автоматизации и реагирования на инциденты информационной безопасности (SOAR, SecOps);

в) инструменты проектирования корпоративной архитектуры (Enterprise Architecture Tools);

г) языковые модели, адаптированные для работы с исходными данными, предусмотренными пунктом 19 настоящей Методики.

21. Для сбора и анализа исходных данных назначаются наиболее подготовленные специалисты (далее – специалисты по сбору и анализу исходных данных). Рекомендуется назначать специалистов, обладающих следующими компетенциями:

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

б) знание правил разработки, утверждения и отмены внутренних регламентов, стандартов, иных организационно-распорядительных документов по вопросам защиты информации (обеспечения безопасности значимых объектов КИИ), состав и содержание таких документов;

в) знание процессов организации и управления деятельностью по защите информации (обеспечению безопасности значимых объектов КИИ) и умение их практически реализовывать;

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

22. Специалисты по сбору и анализу исходных данных не должны проводить оценку материалов, характеризующих (демонстрирующих, подтверждающих) результаты реализации ими собственных функций и (или) задач (в случае проведения внутренней оценки уровня зрелости).

23. В ходе сбора и анализа исходных данных:

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

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

в) проводится анализ отчетов о результатах предыдущей оценки уровня зрелости (при наличии);

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

Подразделения и специалисты, привлекаемые к процессу сбора исходных данных, должны оказывать содействие и принимать исчерпывающие меры для предоставления исходных данных, требуемых для анализа.

24. В случае непредставления структурным подразделением, специалистами, привлекаемыми к процессу сбора исходных данных, запрошенных для проведения оценки документов и материалов, соответствующим направлениям деятельности присваиваются нулевые значения.

25. Результаты проведения опроса (интервьюирования) работников о составе и порядке реализации ими функций (задач) в информационных системах и (или) обеспечения информационной безопасности подлежат документированию.

26. Собранные исходные данные подлежат анализу специалистами по сбору и анализу исходных данных с целью формирования выводов о реализации

мероприятий (процессов) и мер по защите информации (обеспечению безопасности значимых объектов КИИ), об их достаточности и эффективности, соответствии целям защиты информации и требованиям по защите информации (обеспечению безопасности значимых объектов КИИ). По результатам анализа исходных данных специалисты осуществляют подтверждение выполнения требований к уровню зрелости, указанным в таблице 2.

V. ОПРЕДЕЛЕНИЕ ТЕКУЩИХ УРОВНЕЙ ЗРЕЛОСТИ ДЛЯ КАЖДОГО ИЗ НАПРАВЛЕНИЙ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ)

27. На основе изучения и анализа собранных исходных данных определяется текущий уровень зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$.

28. При оценке уровня зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ оценивается соответствие каждого (i) направления деятельности, приведенного в пункте 11 настоящей Методики, требованиям к его реализации, указанным в таблице 2.

Таблица 2

№	Вид требования j	Характеристика требования	Значения выполнения требования a		Весовой коэффициент w
1	Документирование $j = 1$	Степень стандартизации, регламентации, документирования направления деятельности	Регламенты, стандарты, политики не разработаны	0	0,15
			Регламенты, стандарты, политики утверждены, но не соответствуют установленным требованиям и(или) не доведены до заинтересованных лиц	0,5	
			Регламенты, стандарты, политики утверждены, полностью соответствуют установленным требованиям, актуализируются (вносятся изменения) на постоянной основе, доведены до всех заинтересованных лиц	1	
2	Выполнение $j = 2$	Степень фактического выполнения стандартов, регламентов и политик при реализации мероприятий (процессов) и мер по защите информации	Мероприятия (процессы), меры по защите информации не реализуются	0	0,2
			Мероприятия (процессы), меры по защите информации реализуются частично, имеются отдельные отклонения от регламентов, стандартов, политик	0,5	
			Мероприятия (процессы) реализуются в соответствии с регламентами, стандартами, политиками	1	
3	Инструменты $j = 3$	Степень применения инструментальных средств, программных платформ, систем при реализации мероприятий (процессов) и мер по защите информации	Мероприятия (процессы), меры по защите информации выполняются вручную, инструментальные средства не применяются	0	0,1
			Внедрены отдельные инструментальные средства для частичной реализации мероприятия (процесса), мер по защите информации	0,5	
			Мероприятие (процесс), меры по защите информации полностью реализуется с использованием инструментальных (средств)	1	

№	Вид требования j	Характеристика требования	Значения выполнения требования a		Весовой коэффициент w
4	Квалификация $j = 4$	Уровень компетенций (знаний и соответствующих им навыков) специалистов, участвующих в реализации мероприятий (процессов) и мер по защите информации	Мероприятие (процесс), меры по защите информации реализуется специалистами, не имеющими компетенций	0	0,1
			Мероприятие (процесс), меры по защите информации реализуется специалистами, прошедшими обучение, но не имеющими навыков (опыта) в их реализации	0,5	
			Мероприятие (процесс), меры по защите информации реализуется специалистами, обладающими необходимыми компетенциями: имеются значительный (более 1 года) опыт в реализации, и (или) получены сертификаты, подтверждающие уровень компетенции	1	
5	Контроль $j = 5$	Степень контролируемости мероприятий (процессов) и мер по защите информации	Контроль реализации мероприятий (процессов), мер по защите информации не осуществляется	0	0,15
			Контроль реализации мероприятий (процессов), мер по защите информации осуществляется преимущественно после компьютерных инцидентов	0,5	
			Контроль реализации мероприятий (процессов), мер по защите информации регламентирован, проводятся плановые проверки	1	
6	Обучение $j = 6$	Степень осведомлённости персонала в области защиты информации, направленной на снижение рисков, связанных с человеческим фактором	Обучение не проводится	0	0,1
			Обучение проводится эпизодически, по инициативе отдельных руководителей подразделений	0,3	
			Обучение проводится, но без системного подхода и измерения результатов	0,5	
			Обучение проводится в соответствии с утвержденной программой обучения, охватывающей разные категории работников. Проводится контроль знаний и умений обучающихся	1	

№	Вид требования j	Характеристика требования	Значения выполнения требования a		Весовой коэффициент w
7	Внешний аудит $j = 7$	Проведение оценки направления деятельности по защите информации (обеспечения безопасности КИИ) экспертами сторонней организации с целью подтверждения соответствия их установленным требованиям, выявления недостатков и формирования рекомендаций по улучшению	Внешние оценки реализации мероприятий (процессов), мер по защите информации не проводятся	0	0,1
			Внешние оценки реализации мероприятий (процессов), мер по защите информации проводятся, эпизодически, не системно	0,5	
			Внешние оценки мероприятий (процессов), мер по защите информации планируются, проводятся по графику на регулярной основе, результаты используются для повышения защищенности	1	
8	Актуализация $j = 8$	Проведение совершенствования (улучшения) мероприятий (процессов) и мер по защите информации	Совершенствование (улучшение) мероприятий (процессов), мер по защите информации не проводится	0	0,1
			Совершенствование (улучшение) мероприятий (процессов), мер по защите информации осуществляется не системно, эпизодически	0,5	
			Совершенствование (улучшение) мероприятий (процессов), мер по защите информации регламентировано, улучшения, обновления вносятся по плану	1	

29. Для каждого вида требования к реализации направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) оценивается степень его выполнения D_{ij} по формуле:

$$D_{ij} = w_j \cdot a_j, \text{ где}$$

$i \in [1; N]$ – направление деятельности.

$j \in [1; 8]$ – вид требования;

w – весовой коэффициент вида требования;

a – значение уровня выполнения требования к уровню зрелости.

Характеристики видов требований, весовые коэффициенты w, значение уровня выполнения требования к уровню зрелости a представлены в таблице 2.

30. Итоговое значение выполнения всех требований к реализации каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) (P_i) определяется по формуле:

$$P = \sum_{i=1}^{N} \sum_{j=1}^{8} D_{ij}, \text{ где}$$

8 — количество видов требований;

$i \in [1; N]$ – направление деятельности;

D_{ij} – степень выполнения вида требования;

$j \in [1; 8]$ – вид требования.

31. Достижение текущего уровня зрелости по каждому из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ подтверждается, если он соответствует нормированным значениям, определенным в таблице 3. В соответствии с полученным значением (D_{ij}) определяется значение уровня зрелости направления (P_i) в границах, определенных в таблице 3.

Таблица 3

Текущий уровень зрелости направления, ($У_{зит_i}$)	**Степень выполнения вида требования, (D_{ij})**								**Значение уровня зрелости направления, (*Pi*)**
	Документирование	**Выполнение**	**Инструменты**	**Квалификация**	**Контроль**	**Обучение**	**Внешний аудит**	**Актуализация**	
0									$Р_{ЗН} < 0,2$
1	$D_{i_1} \geq 0,075$	$D_{i_2} \geq 0,1$	$D_{i_3} \geq 0,05$						$Р_{ЗН} \geq 0,225$
2	$D_{i_1} \geq 0,075$	$D_{i_2} \geq 0,1$	$D_{i_3} \geq 0,05$	$D_{i_4} \geq 0,05$	$D_{i_5} \geq 0,075$				$Р_{ЗН} \geq 0,35$
3	$D_{i_1} = 0,15$	$D_{i_2} = 0,2$	$D_{i_3} \geq 0,05$	$D_{i_4} \geq 0,05$	$D_{i_5} = 0,15$	$D_{i_6} \geq 0,05$			$Р_{ЗН} \geq 0,65$
4	$D_{i_1} = 0,15$	$D_{i_2} = 0,2$	$D_{i_3} \geq 0,05$	$D_{i_4} \geq 0,05$	$D_{i_5} = 0,15$	$D_{i_6} = 0,1$	$D_{i_7} = 0,1$	$D_{i_8} = 0,1$	$Р_{ЗН} \geq 0,9$

32. По результатам расчета текущего уровня зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ в соответствии с пунктом 10 настоящей Методики рассчитывается уровень зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ) $У_{зи}$.

33. Проведенная оценка уровня зрелости деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зи}$ используется для ретроспективного сравнения результатов оценки текущего уровня зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ органа (организации) с предыдущими оценками соответствующего уровня зрелости.

По результатам ретроспективного сравнения уровней зрелости делаются следующие выводы:

а) позитивная динамика изменения уровня зрелости – зафиксирован рост значения уровня зрелости органа (организации) в сторону следующего уровня;

б) положительная динамика изменения уровня зрелости – зафиксирован рост оценок уровня зрелости по отдельным направлениям;

в) нулевая динамика – отсутствуют изменения по всем показателям оценки;

г) негативная динамика изменения уровня зрелости – зафиксировано снижение результатов оценки по одному или более критерием оценки.

34. Оператором по результатам расчёта текущих уровней зрелости каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ и определения целевых значений уровней зрелости каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$ определяются мероприятия (процессы) и меры по защите информации (обеспечению безопасности значимых объектов КИИ) по достижению целевых уровней зрелости $У_{зиц i}$, а также разрабатывается план по реализации (совершенствованию) мероприятий (процессов) и мер в соответствии с установленными целями и требованиями по защите информации (обеспечению безопасности значимых объектов КИИ).

35. В случае соответствия текущего уровня зрелости по каждому из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ целевому уровню зрелости каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$ определяются новый целевой уровень зрелости по данному направлению деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$, определяются мероприятия (процессы) и меры по защите информации (обеспечению безопасности значимых объектов КИИ), которые не реализованы или реализованы с недостаточным качеством, устанавливается их приоритетность и разрабатывается план по реализации (совершенствованию) мероприятий (процессов) и мер в соответствии с установленными целями и требованиями по защите информации (обеспечению безопасности значимых объектов КИИ).

36. В случае, если при повторном расчёте уровня зрелости деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зи}$ текущие уровни зрелости каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$ не соответствуют целевым уровням зрелости каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$, оператором определяются мероприятия (процессы) и меры по защите информации (обеспечению безопасности значимых объектов КИИ), которые не реализованы или реализованы с недостаточным качеством, устанавливается их приоритетность и разрабатывается план по реализации (совершенствованию) мероприятий (процессов) и мер в соответствии с установленными целями и требованиями по защите информации (обеспечению безопасности значимых объектов КИИ).

VI. ДОКУМЕНТИРОВАНИЕ РЕЗУЛЬТАТОВ ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ

34. По результатам оценки уровня зрелости $У_{зи}$ разрабатывается отчет, в котором содержатся сведения о проведенной оценке по каждому направлению деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) с пояснением соответствия их реализации требованиям.

35. Отчет должен содержать:

а) сведения об операторе, включая сведения о действующих в организации требованиях по защите информации (обеспечению безопасности значимых объектов КИИ);

б) дату проведения оценки уровня зрелости;

в) сведения о лицах, проводивших оценку уровня зрелости (ФИО, должность, наименование организации, контактная информация);

г) сведения о лицах, участвовавших в проведении оценки уровня зрелости (ФИО, должность, наименование организации, контактная информация), в том числе предоставлявших исходные данные для проведения оценки;

д) сведения о результатах предыдущей оценки уровня зрелости, достигнутых значениях, графическую интерпретацию уровня зрелости (при ее проведении);

е) исходные данные, на основании которых проводилась оценка уровня зрелости $У_{зи}$;

ж) сведения об используемых методах и инструментах для оценки уровня зрелости $У_{зи}$;

з) перечень направлений деятельности (областей оценки), по которым проводится оценка уровня зрелости $У_{зи}$;

и) результаты оценки степени выполнения вида требования D_{ij} и расчета значений уровня зрелости направления $Р_{зн}$ для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ);

к) результаты определения текущего уровня зрелости по каждому из направлений деятельности по защите информации (обеспечению безопасности

значимых объектов КИИ) $У_{зит i}$ с подробной информацией о реализации требований, предусмотренных таблицей 2 (в том числе с указанием подтверждающих документов, применяемых инструментальных средствах, отчетной документации, результатов проведенных мероприятий по защите информации (обеспечению безопасности значимых объектов КИИ)), заключение (вывод) о достижении текущего уровня зрелости $У_{зит i}$, а также расчет уровня зрелости $У_{зи}$;

л) графическую интерпретацию целевых уровней зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зиц i}$ на основе результатов определения текущих уровней зрелости для каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) $У_{зит i}$;

м) направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ), по которым не достигнуты целевые значения, с указанием видов требований, по которым выявлены недостатки;

н) рекомендации по совершенствованию защиты информации, содержащейся в информационных системах, и (или) обеспечения безопасности значимых объектов КИИ, в котором в том числе указываются наименования мероприятий, сроки их выполнения, подразделения (работники), ответственные за реализацию каждого мероприятия.

36. Отчет подписывается специалистами, проводившими оценку, и утверждается руководителем либо ответственным лицом за защиту информации (обеспечение безопасности значимых объектов КИИ). Оператор несет ответственность за качество и объективность проведенной оценки уровня зрелости.