ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

МЕТОДИЧЕСКИЙ ДОКУМЕНТ
(ПРОЕКТ)

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. Методика может применяться для оценки уровня зрелости иных направлений деятельности по информационной безопасности, требования к реализации которых установлены отраслевыми, ведомственными актами (документами). В этом случае определенные настоящим методическим документом направления деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ) дополняются отраслевыми (ведомственными) направлениями деятельности по информационной безопасности.

5. Настоящая Методика применяется:

а) операторами информационных систем, значимых объектов критической информационной инфраструктуры (операторами) - 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;

в) государственными органами, организациями, в том числе субъектами критической информационной инфраструктуры, являющими заказчиками услуг, работ (заказчики) — для установления требований к уровню зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), осуществляемой подрядными организациями при оказании услуг, проведении работ;

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

г) ФСТЭК России — для оценки эффективности деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), осуществляемой операторами, подрядными организациями.

6. 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.

7. Оценка уровня зрелости может проводиться оператором 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 (подрядной организации), в отношении которых проходит оценка.

II. УРОВЕНЬ ЗРЕЛОСТИ И ПОРЯДОК ЕГО ОЦЕНКИ

8. Уровень зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ) ($У_{зи}$) является показателем, характеризующим качество данной деятельности и оказывающий существенное влияние на эффективность и результативность реализуемых мероприятий (процессов) и соответствующих мер по защите информации (обеспечения безопасности значимых объектов КИИ).

Определив текущий уровень зрелости $У_{зит}$ и сравнив его с целевым уровнем зрелости $У_{зиц}$, 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.

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. В ходе проверки оценивается возможность наступления негативных последствий (событий)

10. Уровень зрелости $У_{зи}$ определяется для отдельных направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ). Итоговый (общий) уровень зрелости $У_{зи}$ определяется по значениям уровней зрелости $У_{зиi}$ каждого из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ).

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

а) определение оцениваемых направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) и целевого уровня зрелости;

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

в) определение текущего уровня зрелости направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) и итогового (общего) уровня зрелости.

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) оценке подлежат отдельные направления данной деятельности, представляющие собой установленные требованиями по защите информации (обеспечению безопасности) мероприятия (процессы) и соответствующие меры по защите информации (обеспечению безопасности значимых объектов КИИ).

Оценка уровня зрелости проводится по следующим базовым направлениям (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. Для каждого из оцениваемых направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) заместителем руководителя органа (организации), ответственным за обеспечение информационной безопасности в органе (организации), задается целевое значение уровня зрелости $У_{зиц}$, который характеризует ожидаемый результат качества деятельности по защите информации (обеспечению безопасности значимых объектов КИИ).

14. Целевой уровень зрелости каждого направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) устанавливается на основе результатов определения текущего уровня зрелости соответствующего направления деятельности или в соответствии с итоговым (общим) уровнем зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ) в соответствии с таблицей 1.

В случае задания целевого уровня зрелости на основе результатов определения текущего уровня зрелости соответствующего направления по защите информации (обеспечению безопасности значимых объектов КИИ), целевое значение уровня зрелости каждого из направлений должно как минимум на одно значение быть выше текущего значения уровня зрелости направления, полученного по результатам проведенной оценки.

В случае задания целевого уровня зрелости на основе итогового (общего) уровня зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), значение уровня зрелости каждого направления соответствует значению обобщенного (итогового) уровня зрелости деятельности в области защиты информации (обеспечения безопасности значимых объектов КИИ), установленного в таблице 1.

15. 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). В профиль уровня зрелости могут включаться дополнительные направления деятельности по обеспечению информационной безопасности, установленные отраслевыми, ведомственными требованиями в области защиты информации и информационной безопасности.

В случае отсутствия необходимости реализации отдельных направлений деятельности ввиду особенностей функционирования оператора (подрядной организации) или его информационных систем, такие направления деятельности исключаются из профиля уровня зрелости.

16. По результатам профилирования осуществляется построение диаграммы профиля уровней зрелости, на которой указываются значения текущего уровня зрелости каждого направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) и значения целевого уровня зрелости каждого направления деятельности органа (организации) по защите информации (обеспечению безопасности значимых объектов КИИ).

Графическая интерпретация целевого уровня зрелости на основе результатов определения текущего уровня зрелости соответствующего направления по защите информации (обеспечению безопасности значимых объектов КИИ) представлена на рисунке 1.

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

17. 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, проводивших работы при эксплуатации данных систем рекомендуется задавать целевой уровень зрелости деятельности не ниже начального.

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, проводивших работы при эксплуатации данных систем рекомендуется устанавливать целевой уровень зрелости деятельности не ниже системного.

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, проводивших работы при эксплуатации данных систем рекомендуется устанавливать целевой уровень зрелости деятельности не ниже контролируемого.

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

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

е) результаты последней оценки уровня зрелости;

ж) отчеты, составленные по результатам проведения предыдущей внутренней, внешней оценки уровня зрелости;

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

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

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

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

м) 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).

19. 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).

20. 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.

21. 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).

22. 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;

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.

23. 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.

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

25. 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 критериев оценки.

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

26. На основе изучения и анализа собранных исходных данных определяются текущие уровни зрелости каждого направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ).

27. При оценке уровней зрелости направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) проверяется соответствие каждого направления деятельности, приведенного в пункте 12 настоящей Методики, требованиям к его реализации, указанным в таблице 2.

Таблица 2

№	Вид требования	Характеристика требования	Значения выполнения требования a		Весовой коэффициент w
1	Документирование	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, соответствуют требованиям и на постоянной основе актуализируются (вносятся изменения)	1	
2	Выполнение	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	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	
4	Квалификация	Уровень компетенций (знаний и соответствующих им навыков) специалистов, участвующих в реализации мероприятий	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	

№	Вид требования	Характеристика требования	Значения выполнения требования a		Весовой коэффициент w
		(процессов) и мер по защите информации	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	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	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	
			Базовое обучение проводится, но без системного подхода и измерения результатов	0,5	
			Утверждена программа обучения, охватывающая разные категории работников	1	
7	Внешний аудит	Проведение оценки направления деятельности по защите информации (обеспечения безопасности КИИ) экспертами сторонней организации с целью подтверждения соответствия их установленным требованиям, выявления недостатков и	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	

№	Вид требования	Характеристика требования	Значения выполнения требования a		Весовой коэффициент w
		формирования рекомендаций по улучшению			
8	Актуализация	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	

28. Для каждого вида требования к реализации направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) рассчитывается значение его выполнения по формуле:

$$D_{\text{ко}_i} = w_i \cdot a_i, \text{ где}$$

$i \in [1; 8]$ – индекс критериев оценки уровня зрелости;

w – весовой коэффициент критериев оценки уровня зрелости;

a – значение выполнения требования к уровню зрелости.

Характеристики критериев, весовые коэффициенты w, a представлены в таблице 2.

29. Итоговое значение для всех требований к реализации каждого направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) определяется по формуле:

$$P_{\text{зн}_k} = \sum_{i=1}^{m} D_{\text{ко}_i}, \text{ где}$$

m=8 — количество критериев оценки уровня зрелости;

$i \in [1; m]$ – индекс критериев оценки уровня зрелости;

$k \in [1; \text{н}]$ – индекс направлений деятельности.

30. Достижение направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) уровня зрелости подтверждается, если для него выполняются требования в соответствии с таблицей 3. При неполном соответствии направления деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) хотя бы одному требованию не допускается подтверждение этого направления деятельности соответствующему уровню зрелости.

Таблица 3

Уровни зрелости, *(У)*	**Требования уровня зрелости,** ($ДКО_i$)								$P_{ЗН}$
	Документирование	**Выполнение**	**Инструменты**	**Квалификация**	**Контроль**	**Обучение**	**Внешний аудит**	**Актуализация**	**Значение уровня зрелости направления**
0									$Р_{ЗН}<0,2$
1	$D_{КО}\geq0,075$	$D_{КО}\geq0,1$	$D_{КО}\geq0,05$						$Р_{ЗН}\geq0,225$
2	$D_{КО}\geq0,075$	$D_{КО}\geq0,1$	$D_{КО}\geq0,05$	$D_{КО}\geq0,05$	$D_{КО}\geq0,075$				$Р_{ЗН}\geq0,35$
3	$D_{КО}=0,15$	$D_{КО}=0,2$	$D_{КО}\geq0,05$	$D_{КО}\geq0,05$	$D_{КО}=0,15$	$D_{КО}\geq0,05$			$Р_{ЗН}\geq0,65$
4	$D_{КО}=0,15$	$D_{КО}=0,2$	$D_{КО}\geq0,05$	$D_{КО}\geq0,05$	$D_{КО}\geq0,15$	$D_{КО}\geq0,05$	$D_{КО}\geq0,05$	$D_{КО}\geq0,05$	$Р_{ЗН}\geq0,75$

31. Итоговый (общий) уровень зрелости $У_{зи}$ определяется после расчета уровня зрелости на каждом из направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) и выполняется по формуле:

$$У_{зи} = \frac{\sum_{k=1}^{н}(k \cdot Y_k)}{\sum_{k=1}^{н} k}, \text{ где}$$

н – количество направлений деятельности;

$k \in [1; н]$ – индекс направлений деятельности;

$Y_k \in [0; 4]$ –уровень зрелости на каждом из направлений деятельности.

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

32. Проведенная оценка уровня зрелости органа (организации) используется для ретроспективного сравнения текущих результатов оценки уровня зрелости направлений деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) органа (организации) с предыдущими оценками уровня зрелости. По результатам ретроспективного сравнения уровней зрелости делаются следующие выводы:

а) позитивная динамика изменения уровня зрелости – зафиксирован рост значений 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.

33. В случае если обобщенный уровень зрелости $У_{зи}$ не соответствует целевому уровню зрелости $У_{зиц}$ в органе (организации) 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).

При достижении органом (организацией) целевого уровня зрелости должен быть определен новый целевой уровень зрелости органа (организации).

VI. ДОКУМЕНТИРОВАНИЕ РЕЗУЛЬТАТОВ ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ

34. По результатам оценки уровня зрелости разрабатывается отчет, в котором содержатся сведения о порядке проведения оценки 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, принимающих участие в проведении оценки уровня зрелости;

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

д) результаты определения текущего уровня зрелости по каждому направлению деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) и итогового (общего) уровня зрелости с подробной информацией о реализации требований, предусмотренных таблицей 2;

е) сравнительную диаграмму текущего уровня зрелости по направлению деятельности по защите информации (обеспечению безопасности значимых объектов КИИ) и итогового (общего) уровня зрелости $У_{зи}$;

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

з) план мероприятий по совершенствованию защиты информации, содержащейся в информационных системах, в котором в том числе указываются наименования мероприятий, сроки их выполнения, подразделения (работники), ответственные за реализацию каждого мероприятия. Результатом реализации мероприятий плана должно быть достижение значения уровня зрелости $У_{зи}$ целевого уровня зрелости $У_{зиц}$.

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.