АДМИНИСТРАЦИЯ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
«МУНИЦИПАЛЬНЫЙ ОКРУГ
ЗАВЬЯЛОВСКИЙ РАЙОН
УДМУРТСКОЙ РЕСПУБЛИКИ»

УПРАВЛЕНИЕ «ПИРОГОВСКОЕ»

«УДМУРТ ЭЛЬКУНЫСЬ
ДЭРИ ЁРОС
МУНИЦИПАЛ ОКРУГ»
МУНИЦИПАЛ КЫЛДЫТЭТ
АДМИНИСТРАЦИЕЗ

«ПЕРОГГУРТ» КИВАЛТОННИ

П Р И К А З

10.02.2025 № 29

д. Пирогово

Об утверждении регламента оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации в Управлении «Пироговское» Администрации муниципального образования «Муниципальный округ Завьяловский район Удмуртской Республики»

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принимая во внимание методический документ «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденный приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 02.05.2024, руководствуясь Положением «Об Управлении «Пироговское» Администрации муниципального образования «Муниципальный округ Завьяловский район Удмуртской Республики»:

1. Утвердить Регламент оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации в Управлении «Пироговское» Администрации муниципального образования «Муниципальный округ Завьяловский район Удмуртской Республики» (прилагается).
2. Контроль за исполнением приказа оставляю за собой.

Начальник Управления З.В. Леонтьева

УТВЕРЖДЕН
приказом Управления «Пироговское»
Администрации
муниципального образования
«Муниципальный округ
Завьяловский район
Удмуртской Республики»
от 10.02.2025 № 29

РЕГЛАМЕНТ
оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации в Управлении «Пироговское» Администрации муниципального образования «Муниципальный округ Завьяловский район Удмуртской Республики»

1. Общие сведения

1.1. Настоящий Регламент разработан с учетом положений методического документа ФСТЭК России от 02.05.2024 «Методика оценки показателя состояния технической защиты информации».

1.2. Целью разработки данного Регламента является определение Управлением «Пироговское» Администрации муниципального образования «Муниципальный округ Завьяловский район Удмуртской Республики» (далее – Управление) порядка оценки показателя, характеризующего состояние технической защиты информации, не составляющей государственную тайну, и обеспечения безопасности объектов информатизации (далее – показатель КЗИ) в Управлении.

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

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

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

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

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

– развития (изменения) архитектуры объекта информатизации;

– запроса начальника Управления «Пироговское» Администрации муниципального образования «Муниципальный округ Завьяловский район Удмуртской Республики» о текущем значении показателя защищенности КЗИ;

– запроса ФСТЭК России.

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

2. Сокращения

2.1. **Ответственный за ИБ** – сотрудник Управления, на которого возложены

полномочия по обеспечению информационной безопасности.

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

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

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

2.5. **ФСБ России** – федеральная служба безопасности Российской Федерации.

3. Порядок оценки показателя

3.1. Оценка показателя КЗИ должна включать:

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

– определение значений частных показателей безопасности;

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

– подведение итогов и планирование мероприятий по результатам оценки показателя.

3.2. Оценка показателя КЗИ проводится в отношении всех объектов информатизации в Управлении, подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации. Включение в область оценки иных объектов информатизации в Управлении осуществляется по решению начальника Управления или ответственного за ИБ.

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

3.4. Оценка показателя КЗИ организуется ответственным за ИБ.

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

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

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

– доводит до начальника Управления документы, фиксирующие результаты расчета значений показателя КЗИ, если расчетное значение показателя КЗИ не соответствует нормативному значению;

– организует планирование мероприятий (разработка плана), направленных на выполнение мер по защите информации, которые не реализованы или реализация которых не обеспечивает защиту от типовых актуальных угроз безопасности информации, в соответствии с установленными в Управлении целями по обеспечению защиты информации. Срок реализации мероприятий, определенных в плане, не должен превышать срок до проведения следующей плановой оценки КЗИ.

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

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

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

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

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

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

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

– результаты проведения инвентаризации объектов информатизации;

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

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

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

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

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

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

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

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

4.3. По решению ответственного за ИБ для сбора и анализа исходных данных могут привлекаться сотрудники Управления, обладающие необходимыми компетенциями.

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

4.5. Задачи специалистов по ИБ:

– запрашивать у других сотрудников Управления требуемые для анализа документы и материалы;

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

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

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

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

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

5. Определение значений частных показателей безопасности

5.1. Для расчета показателя КЗИ определяются значения частных показателей безопасности. Перечень используемых частных показателей безопасности (их идентификаторы и наименования, а также максимальные значения для каждого из них) приведены в приложении к Регламенту.

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

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

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

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

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

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

6. Расчет показателя защищенности и его сравнение с нормированным значением

6.1. Расчет показателя КЗИ осуществляется по следующей формуле:

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

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

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

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

Таблица

Состояния защиты информации

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

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

7. Взаимодействие с ФСТЭК России в части результатов оценки показателя

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

7.1.1. Последних результатов оценки показателя КЗИ.

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

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

8. Ответственность

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