Приложение

УТВЕРЖДЕН
постановлением администрации
муниципального образования
Северский муниципальный район
Краснодарского края
от _____№_____

РЕГЛАМЕНТ
расчета показателя состояния технической защиты информации в информационных системах администрации муниципального образования Северский муниципальный район Краснодарского края

1. Общие положения

1.1. Настоящий Регламент расчета показателя состояния технической защиты информации в информационных системах администрации муниципального образования Северский муниципальный район Краснодарского края (далее – Регламент) определяет порядок оценки текущего состояния защиты информации в администрации муниципального образования Северский муниципальный район Краснодарского края (далее – Администрация), и степени его соответствия минимально необходимому уровню защиты информации от типовых актуальных угроз безопасности информации.

1.2. Настоящий Регламент разработан в соответствии с:

- приказом ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (далее – Приказ ФСТЭК России № 117);
- приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ ФСТЭК России № 21);
- методическим документом ФСТЭК России от 11 ноября 2025 г. «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

1.3. Настоящий Регламент предназначен для оценки текущего состояния защиты информации и разработки на основе такой оценки мер по повышению уровня защищенности, а также оценки эффективности деятельности по защите информации, организованной в Администрации.

1.4. В качестве минимально необходимого уровня защиты информации задан состав мер, реализация которых предусмотрена приказами ФСТЭК России № 117 и № 21, и который минимально достаточен для блокирования (нейтрализации) типовых актуальных угроз безопасности информации, реализуемых нарушителями с базовыми возможностями.

2. Показатель защищенности и его нормированное значение

2.1. В качестве показателя, характеризующего текущее состояние технической защиты информации в Администрации, используется показатель текущего состояния защищенности $К_{ЗИ}$ (далее – показатель защищенности, показатель $К_{ЗИ}$).

Показатель $К_{ЗИ}$ характеризует степень достижения Администрацией минимально необходимого уровня защиты информации от типовых актуальных угроз безопасности информации во временном интервале оценивания и заданных условиях эксплуатации информационных систем, в том числе информационных систем персональных данных, и иных объектов информатизации, эксплуатируемых в Администрации.

2.2. Объект информатизации, эксплуатируемый в Администрации, имеет минимальный уровень защищенности от типовых актуальных угроз безопасности информации, если значение показателя $К_{ЗИ}$ соответствует нормативному значению, равному единице ($К_{ЗИ}=1$).

2.3. Значение показателя $К_{ЗИ}$ не может быть ниже порогового значения, равного нулю (0) или превышать нормативное значение, равное единице (1).

2.4. Для оценки показателя защищенности $К_{ЗИ}$ определяются значения частных показателей безопасности k_{ji} (далее – частные показатели безопасности, частные показатели k_{ji}), где j — номер группы частных показателей безопасности, i — номер частного показателя в соответствующей группе показателей безопасности.

2.5. Значение показателя $К_{ЗИ}$, а также значения частных показателей безопасности являются критериями принятия в Администрации решений в части необходимости реализации мер по защите информации.

3. Порядок оценки показателя защищенности

3.1. Оценка показателя защищенности включает:

- сбор и анализ исходных данных;
- оценку значений частных показателей безопасности;

- расчет значения показателя защищенности и его сравнение с нормированным значением.

3.2. По результатам оценки показателя защищенности, производится подведение итогов и планирование последующих мероприятий по защите информации.

3.3. Оценка показателя защищенности производится в отношении всех объектов информатизации, эксплуатируемых в Администрации, и подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации.

3.4. Допускается проведение оценки показателя защищенности для объекта информатизации, представляющего совокупность объектов информатизации, эксплуатируемых в Администрации – информационной системы Администрации. Также в область оценки показателя защищенности включается информационно-телекоммуникационная инфраструктура центра обработки данных, в случае если объект информатизации функционирует на базе такой информационно-телекоммуникационной инфраструктуры.

3.5. Оценка показателя защищенности организуется заместителем главы администрации муниципального образования Северский муниципальный район Краснодарского края, на которого возложены полномочия по обеспечению безопасности информации в Администрации.

3.6. Оценка показателя защищенности проводится структурным подразделением Администрации, осуществляющим функции по обеспечению безопасности информации в Администрации. Допускается проведение оценки показателя защищенности силами отдельных специалистов по защите информации (ответственных должностных лиц, осуществляющих функции по обеспечению безопасности информации).

3.7. О полученном по результатам расчета значении показателя $K_{ЗИ}$ информируется глава муниципального образования Северский муниципальный район Краснодарского края. В случае если значение показателя $K_{ЗИ}$ не соответствует нормированному значению, структурным подразделением Администрации, осуществляющим функции по обеспечению безопасности информации в Администрации, или специалистами по защите информации (ответственными должностными лицами, осуществляющими функции по обеспечению безопасности информации), подготавливаются перечень мероприятий по совершенствованию (улучшению) мер по защите информации, принимаемых в Администрации, и план реализации указанных мероприятий (план реализации мероприятий по достижению следующего уровня защиты от актуальных угроз), которые представляются главе муниципального образования Северский муниципальный район Краснодарского края для

принятия соответствующих решений совместно с полученным по результатам расчета значении показателя $К_{ЗИ}$.

3.8. Перечень мероприятий по совершенствованию (улучшению) мер по защите информации, принимаемых в Администрации, формируется на основе полученных частных показателей безопасности, отражающих не реализованные или реализованные не в полном объеме мероприятий по защите информации от типовых актуальных угроз безопасности информации, а также приоритетность их реализации.

3.9. Срок реализации мероприятий по совершенствованию (улучшению) мер по защите информации, принимаемых в Администрации, не может превышать срок до проведения следующей плановой оценки показателя защищенности.

3.10. Результаты оценки показателя защищенности представляются в территориальное управление ФСТЭК России (Управление ФСТЭК России по Северо-Кавказскому и Южному федеральным округам) в целях оценки текущего состояния защиты информации. Порядок предоставления результатов оценки показателя защищенности может быть уточнен отдельными распоряжениями федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации и распоряжениями органа исполнительной власти, уполномоченного в области обеспечения безопасности информации органов исполнительной власти Краснодарского края.

3.11. В случае запроса специалистами ФСТЭК России документов и материалов, используемых для оценки показателя защищенности, для подтверждения представленных результатов оценки, должностным лицом Администрации, ответственным за взаимодействие Администрации с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, формируются комплект документов и материалов, подтверждающих присвоение значений показателю защищенности и частным показателям безопасности, в соответствии с приложением 1 к настоящему Регламенту.

3.12. Плановая оценка показателя состояния защищенности в Администрации производится в срок – один раз в шесть месяцев.

3.13. Внеочередная оценка показателя защищенности производится в случаях:

- возникновения инцидента информационной безопасности на объекте информатизации, эксплуатируемом Администрации, и повлекшего наступление негативных последствий для Администрации;
- развития (изменения) архитектуры объекта информатизации, эксплуатируемого Администрации;
- запроса главы муниципального образования Северский муниципальный район Краснодарского края о текущем значении показателя защищенности;
- запроса ФСТЭК России.

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

4.1. Исходными данными, необходимыми для оценки показателя защищенности являются:

- акты, протоколы и иные документы, составленные по результатам государственного контроля в области защиты информации, проведенного федеральным органом исполнительной власти в области обеспечения безопасности или федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации;
- отчеты, протоколы и иные документы, составленные по результатам внутреннего контроля уровня защищенности информации, осуществляемого в рамках реализации положений Политики аудита информационной безопасности Администрации;
- отчеты, составленные по результатам внешней оценки соответствия в области защиты информации (внешнего аудита, осуществляемого в рамках реализации положений Политики аудита информационной безопасности Администрации, аттестационных мероприятий и мероприятий по контролю уровня защищенности информации, обрабатываемой на объектах информатизации Администрации), в том числе отчеты по результатам испытаний системы защиты методами тестирования на проникновение, учений, тренировок в области защиты информации;
- внутренние организационно-распорядительные документы, регламентирующие организацию защиты информации в Администрации;
- эксплуатационная документация на средства защиты информации, содержащая сведения об их настройках и конфигурации;
- результаты проведения инвентаризации информационных активов Администрации полученные по результатам проведения мероприятий в

соответствии с положениями Политики использования информационных активов Администрации;

- результаты опроса (интервьюирования) сотрудников Администрации о выполнении ими функций (задач) с использованием информационных систем;
- результаты опроса (интервьюирования) сотрудников структурного подразделения Администрации, осуществляющего функции по обеспечению безопасности информации в Администрации, или специалистов по защите информации (ответственных должностных лиц, осуществляющих функции по обеспечению безопасности информации) Администрации;
- результаты анализа функционирования (применения) отдельных программных, программно-аппаратных средств обработки информации, применяемых в составе объектов информатизации, эксплуатируемых в Администрации;
- результаты работы инструментальных средств оценки (анализа) защищенности информационных систем и (или) мониторинга информационной безопасности, эксплуатируемых в Администрации.

4.2. Для сбора и анализа исходных данных назначаются наиболее подготовленные специалисты из состава структурного подразделения, осуществляющего функции по обеспечению информационной безопасности. Во избежание возникновения конфликта интересов при проведении сбора и анализа исходных данных назначается нечетное количество ответственных лиц, допускающее проведение перекрестной проверки собираемых данных.

4.3. По решению заместителя главы муниципального образования Северский муниципальный район Краснодарского края, на которого возложены полномочия по обеспечению безопасности информации в Администрации, для сбора и анализа исходных данных могут привлекаться специалисты из других структурных подразделений, обладающие необходимыми компетенциями.

4.4. Ответственные лица, назначенные для сбора и анализа исходных данных, не должны проводить оценку материалов, характеризующих (демонстрирующих, подтверждающих) результаты реализации ими собственных функций и (или) задач.

4.5. Ответственные лица, назначенные для сбора и анализа исходных данных:

- запрашивают в структурных подразделениях (филиалах, территориальных обособленных функциональных подразделениях) Администрации требуемые для анализа документы и материалы;

- проводят опросы (интервьюирование) сотрудников Администрации о выполнении ими функций с использованием информационных систем и (или) по обеспечению информационной безопасности;
- осуществляют анализ функционирования отдельных программных, программно-аппаратных средств обработки информации, в том числе эксплуатируемых средств защиты информации, а также анализ отчетов средств оценки (анализа) защищенности и иных средств мониторинга информационной безопасности.

4.6. Подразделения и специалисты Администрации, 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 Администрации запрошенных для проведения оценки документов и материалов соответствующим частным показателям безопасности выставляется пороговое значение равное нулю (0).

4.7. Результаты проведения опроса (интервьюирования) сотрудников Администрации о составе и порядке реализации ими функций (задач) в информационных системах и (или) обеспечении информационной безопасности подлежат документированию в форме бланка ответов (ответного листа), с отметками о правильности ответов проверяемого, данных во время опроса (интервьюирования).

4.8. Собранные исходные данные подлежат анализу ответственными лицами, назначенными для сбора и анализа исходных данных, с целью формирования выводов о реализации в Администрации мероприятий (процессов) по защите информации, о достаточности принимаемых мер по защите информации. По результатам анализа исходных данных ответственными лицами, назначенными для сбора и анализа исходных данных, формируются выводы о реализации мер, соответствующих частным показателям безопасности.

4.9. Полученные результаты расчета значений показателя защищенности подлежат документированию в форме, представленной в приложении 2 к настоящему Регламенту.

5. Порядок определения значений частных показателей безопасности

5.1. Для оценки показателя защищенности определяются значения частных показателей безопасности.

5.2. Частные показатели безопасности характеризуют реализацию в Администрации отдельных мер по защите информации от актуальных угроз

безопасности информации, а также их соответствие целям обеспечения безопасности в Администрации.

5.3. Частные показатели безопасности определяются в отношении всех объектов информатизации, эксплуатируемых в Администрации, и подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации.

5.4. Допускается определение частных показателей безопасности для объекта информатизации, представляющего совокупность объектов информатизации, эксплуатируемых в Администрации – информационной системы Администрации.

В случае, если заместителем главы муниципального образования Северский муниципальный район Краснодарского края, на которого возложены полномочия по обеспечению безопасности информации в Администрации принято решение о раздельном проведении оценки показателя защищенности объектов информатизации, эксплуатируемых в Администрации, и подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации, определение частных показателей безопасности производится также раздельно. При получении по результатам расчета для таких объектов информатизации различных значений по одной и той же группе частных показателей, то при расчете показателя защищенности необходимо учитывать минимальное значение частных показателей безопасности из полученных в рамках одной и той же группы.

5.5. Перечень частных показателей безопасности, их наименования и максимальные значения приведены в таблице 1.

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

5.7. Если по результатам проведенного анализа материалов сделаны выводы, что меры по защите информации реализованы, соответствующему частному показателю безопасности 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 безопасности присваивается значение 0.

Таблица 1 – Перечень частных показателей безопасности, их наименования и максимальные значения

Номер группы показателей (j)	**Наименование групп показателей**	**Номер (i) и наименование частного показателя безопасности (частного показателя k_{ji})**	**Значение частного показателя безопасности (частного показателя k_{ji})**	**Значение весового коэффициента группы показателей (R_j)**
1	Организация и управление	1. На заместителя руководителя органа (организации) возложены[1] 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[2]	0,30	
2		2. Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)[3]	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[4], контролируется межсетевыми экранами уровня L3/L4)	0,20	0,35
		2. На устройствах и интерфейсах, доступных из сети Интернет, отсутствуют	0,25	

[1]) Возложение полномочий и (или) определение структурного подразделения (сотрудников) подтверждается изданием соответствующего локального правового акта.
[2]) В случае если подрядные организации не привлекаются, частному показателю безопасности k_{13} присваивается значение из таблицы 1.
[3]) В случае отсутствия технической возможности реализации в информационной системе или в технических средствах двухфакторной аутентификации соответствующему показателю безопасности присваивается значение из таблицы 1.
[4]) В случае отсутствия устройств, интерфейсов, взаимодействующих с сетью Интернет, соответствующим показателям безопасности присваиваются значения из таблицы 1.

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование частного показателя безопасности (частного показателя k_{ji})	Значение частного показателя безопасности (частного показателя k_{ji})	Значение весового коэффициента группы показателей (R_j)
		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		
		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	0,15	
		4. Обеспечена проверка вложений в электронных письмах электронной почты[5] на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств)	0,15	
		5. Обеспечено централизованное управление средствами антивирусной защиты[6] (не менее чем 80% пользовательских устройств и серверов[7] контролируются средствами антивирусной защиты с централизованным управлением). При этом обеспечены контроль и установка обновлений баз данных признаков вредоносного программного обеспечения не реже чем 1 раз в месяц	0,15	
		6. Реализована очистка входящего из сети Интернет сетевого трафика от компьютерных атак, направленных на отказ в обслуживании, на уровне[8] L3/L4 (заключен договор с провайдером)	0,10	
4	Мониторинг информационной	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	0,35	

[5]) В случае если не используется электронная почта, частному показателю безопасности k_{35} присваиваются значение из таблицы 1.

[6]) Если 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.

[7]) Если информационные системы содержат устройства, в которых конструктивно отсутствуют интерфейсы для возможного внедрения вредоносного программного обеспечения, частному показателю безопасности k_{36} присваивается значение из таблицы 1.

[8]) Если в информационных системах отсутствуют веб-сайт или иные сервисы, подверженные DDoS-атакам, частному показателю безопасности k_{37} присваивается значение из таблицы 1.

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование частного показателя безопасности (частного показателя k_{ji})	Значение частного показателя безопасности (частного показателя k_{ji})	Значение весового коэффициента группы показателей (R_j)
	безопасности и реагирование	всех устройствах, взаимодействующих с сетью Интернет		
		3. Утвержден документ, определяющий порядок реагирования на компьютерные инциденты	0,25	

5.8. В случае если в результате проведения мероприятий по выявлению недостатков (уязвимостей) сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычислительных машин, мероприятий по испытанию систем защиты информации информационных систем методами тестирования на проникновение, учений, тренировок в области защиты информации получен первоначальный доступ к информационной системе с использованием учетных записей пользователей такой системы, для 2 группы показателей весовому коэффициенту R2 присваивается значение 0.

В случае если первоначальный доступ к информационной системе получен с использованием уязвимостей программного и программно-аппаратного обеспечения для 3 группы показателей весовому коэффициенту R3 присваивается значение 0.

В случае если в результате реализации указанных ранее мероприятий достигнуты конкретные цели по выявлению недостатков (уязвимостей) информационной системы, тестированию на проникновения, учений, тренировок, а также подтверждена возможность реализации недопустимых событий, для 2 и 3 группы показателей весовым коэффициентам R2 и R3 присваивается значение 0.

6. Расчет показателя защищенности и его сравнение с нормированным значением

6.1. Расчет показателя защищенности 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.

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

6.3. Рассчитанный в соответствии с пунктом 6.1 показатель защищенности сравнивается с нормированным значением. На основе результатов сравнения формируются выводы о текущем состоянии защиты информации, основанные на заданных параметрах в таблице 2.

Таблица 2 – Зависимость вывода от значения показателя защищенности

Значение показателя защищенности (показателя защищенности $К_{ЗИ}$)	**Вывод о текущем состоянии защиты информации**
$К_{ЗИ} = 1$	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»)**

6.4. В случае если по результатам расчета получено значение показателя защищенности, характеризующее текущее состояние защищенности как

минимальное базовое («зеленый»), внесение изменений (корректировка) мероприятий по защите информации по частным показателям безопасности не производится.

6.5. В случае если по результатам расчета получено значение показателя защищенности, характеризующее текущее состояние защищенности как низкое («оранжевый») или критическое («красный»), структурным подразделением Администрации, осуществляющим функции по обеспечению безопасности информации в Администрации, или специалистами по защите информации (ответственными должностными лицами, осуществляющими функции по обеспечению безопасности информации), подготавливаются перечень мероприятий по совершенствованию (улучшению) мер по защите информации, принимаемых в Администрации, и план реализации указанных мероприятий (план реализации мероприятий по достижению следующего уровня защиты от актуальных угроз), которые представляются главе муниципального образования Северский муниципальный район Краснодарского края для принятия соответствующих решений совместно с полученным по результатам расчета значении показателя $К_{ЗИ}$.

6.6. Перечень мероприятий по совершенствованию (улучшению) мер по защите информации, принимаемых в Администрации, формируется на основе полученных частных показателей безопасности, отражающих не реализованные или реализованные не в полном объеме мероприятий по защите информации от типовых актуальных угроз безопасности информации, а также приоритетность их реализации.

6.7. Срок реализации мероприятий по совершенствованию (улучшению) мер по защите информации, принимаемых в Администрации, не может превышать срок до проведения следующей плановой оценки показателя защищенности.

6.8.Заместителем главы муниципального образования Северский муниципальный район Краснодарского края, на которого возложены полномочия по обеспечению безопасности информации в Администрации обеспечивается контроль реализации мероприятий по защите информации и своевременного исполнения пунктов плана по реализации указанных мероприятий (плана реализации мероприятий по достижению следующего уровня защиты от актуальных угроз).

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская