Приложение 1
к распоряжению председателя
КСП МО СМР КК
От 08.06.2026 № 01-58

ПОЛИТИКА
защиты информации, обрабатываемой в информационной системе контрольно-счетной палаты муниципального образования Северский муниципальный район Краснодарского края

1. Общие положения

1.1.Настоящая Политика защиты информации, обрабатываемой в информационной системе контрольно-счетной палаты муниципального образования Северский муниципальный район Краснодарского края (далее – Политика) определяет цели, задачи и принципы защиты информации, обрабатываемой в информационной системе (далее – ИС) контрольно-счетной палаты муниципального образования Северский муниципальный район Краснодарского края (далее – КСП МО СМР КК), а также объекты защиты и категории лиц, участвующих в мероприятиях по защите информации, обрабатываемой в ИС КСП МО СМР КК, их обязанности (функции) и полномочия.

1.2.Настоящая Политика разработана в соответствии с положениями:

- Конституции Российской Федерации;
- Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа 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);

− приказа 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);

− методическими документами ФСТЭК России.

2. Область действия Политики

2.1.Требования настоящей Политики распространяются на все процессы обработки защищаемой информации в КСП МО СМР КК, технические средства обработки информации (далее – информационные активы) и средства обеспечения их функционирования, в том числе коммутационное оборудование и каналы связи (далее – информационно-телекоммуникационная инфраструктура) КСП МО СМР КК, обеспечивающие функционирование таких процессов.

2.2.Требования настоящей Политики являются обязательными для выполнения всеми работниками КСП МО СМР КК, взаимодействующими с информационными активами и информационно-телекоммуникационной инфраструктурой КСП МО СМР КК, а также распространяются на взаимоотношения с поставщиками, подрядными организациями и иными лицами, услуги которых связаны с использованием, обработкой или доступом к информации, информационным активам или информационно-телекоммуникационной инфраструктуре КСП МО СМР КК.

2.3.Организации, осуществляющие техническую поддержку и сопровождение ИС КСП МО СМР КК в рамках заключенных контрактов, а также иные организации, планирующие осуществлять взаимодействие (взаимодействующие) с ИС КСП МО СМР КК, должны быть ознакомлены с настоящей Политикой в части касающейся.

2.4.Требования настоящей Политики могут быть уточнены организационно-распорядительными документами (внутренними стандартами и регламентами) КСП МО СМР КК, регламентирующими частные мероприятия и меры по защите информации в ИС КСП МО СМР КК.

3. Цели, задачи и принципы защиты информации, обрабатываемой в ИС КСП МО СМР КК

3.1.Целями защиты обрабатываемой в ИС КСП МО СМР КК информации являются:

− обеспечение конфиденциальности обрабатываемой информации, недопущение несанкционированного доступа к информации, информационным

активам или информационно-телекоммуникационной инфраструктуре КСП МО СМР КК;

− обеспечение целостности, а также точности и полноты обрабатываемой в ИС КСП МО СМР КК информации;

− обеспечение доступности обрабатываемой информации, информационных активов и информационно-телекоммуникационной инфраструктуры КСП МО СМР КК для авторизованных лиц – пользователей ИС КСП МО СМР КК (работников КСП МО СМР КК), в том числе при межсетевом взаимодействии с иными информационными системами или предоставлении доступа внешним пользователям к обрабатываемой информации, информационным активам или информационно-телекоммуникационной-инфраструктуре КСП МО СМР КК.

3.2.Задачей защиты обрабатываемой в ИС КСП МО СМР КК информации являются определение угроз безопасности информации, их своевременное выявление и блокирование (нейтрализация) путем предотвращения несанкционированного доступа к информации или иных специальных воздействий на информацию или ее носители в целях ее добывания, искажения, уничтожения или блокирования доступа к информации или информационным активам и информационно-телекоммуникационной инфраструктуре КСП МО СМР КК.

3.3.Достижение целей защиты информации, обрабатываемой в ИС КСП МО СМР КК, осуществляется путем соблюдения следующих принципов защиты информации:

− законность – выполнение мероприятий и принятие мер по защите информации должно обеспечиваться в соответствии с требованиями законодательства Российской Федерации;

− комплексность (системность) – к защите информации должен применяться комплексный подход, включающий в себя совокупность технических, организационных и правовых мер;

− разумная достаточность – проводимые мероприятия и принимаемые меры по защите информации должны быть соразмерны рискам информационной безопасности и возможным негативным последствиям;

− непрерывность – обеспечение безопасности информации должно быть построено в виде постоянно действующего циклического процесса;

− своевременность – обеспечение безопасности информации должно носить превентивный характер по отношению к угрозам безопасности информации;

− совершенствование – реализация мероприятий и мер по защите информации должна учитывать их адаптацию к внедряемым технологиям обработки информации и новым угрозам безопасности информации;

− адаптивность (гибкость) – при реализации мероприятий и мер по защите информации должна осуществляться их адаптация к изменяющимся технологиям обработки информации и угрозам безопасности информации;

− управляемость – при обеспечении безопасности информации должна сохраняться способность к анализу, контролю и корректировке реализуемых мероприятий и мер по защите информации.

4. Деятельность по защите информации, обрабатываемой в ИС КСП МО СМР КК

4.1.Проведение мероприятий и принятие мер по защите информации обеспечивается для всех объектов защиты с учетом технологических и инфраструктурных особенностей КСП МО СМР КК.

4.2.Перечень объектов защиты информации ИС КСП МО СМР КК:

− защищаемая информация, обрабатываемая в ИС КСП МО СМР КК, в том числе хранимая компонентами информационных активов пользователей ИС КСП МО СМР КК – дисковыми накопителями автоматизированных рабочих мест, электронными машинными носителями информации или передаваемая по каналам связи;

− технологическая информация, возникающая в процессе обработки защищаемой информации;

− системное и прикладное программное обеспечение информационных активов;

− информационные активы КСП МО СМР КК: автоматизированные рабочие места пользователей и их компоненты (периферийные устройства);

− программные и программно-аппаратные средства защиты информации;

− информационно-телекоммуникационная инфраструктура КСП МО СМР КК: коммутационное оборудование и каналы связи между ними.

4.3.Проводимые мероприятия по защите информации включают в себя:

− реализацию базовых мер защиты информационных систем и содержащейся в них информации соответствующего класса защищенности;

− адаптацию базовых мер защиты информационных систем и содержащейся в них информации применительно к архитектуре ИС КСП МО СМР КК и применяемым информационным технологиям с учетом особенностей их реализации в ИС КСП МО СМР КК;

- верификацию адаптированных базовых мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

4.4.Класс (уровень) защищенности информационных систем устанавливается комиссией по классификации по требованиям защиты информации КСП МО СМР КК. По результатам работы проект Акта классификации представляется председателю КСП МО СМР КК или уполномоченному им ответственному лицу, для утверждения.

4.5.Перечень актуальных угроз безопасности информации, перечень потенциальных (возможных) нарушителей безопасности информации, их характеристика и возможности по реализации угроз безопасности информации приводятся в моделях угроз безопасности информации, разрабатываемых с учетом положений методического документа «Методика оценки актуальности угроз безопасности информации», утвержденного ФСТЭК России 5 февраля 2021 г.

4.6.Обеспечение защиты информации в КСП МО СМР КК достигается реализацией следующих базовых групп мер защиты информации:

- идентификация и аутентификация;
- управление доступом;
- регистрация событий безопасности;
- защита виртуализации и облачных вычислений;
- защита технологий контейнерных сред и их оркестрации;
- защита сервисов электронной почты;
- защита веб-технологий;
- защита программных интерфейсов взаимодействия приложений;
- защита конечных устройств;
- защита мобильных устройств;
- защита технологий интернета вещей;
- защита точек беспроводного доступа;
- антивирусная защита;
- обнаружение и предотвращение вторжений на сетевом уровне;
- сегментация и межсетевое экранирование;
- защита от компьютерных атак, направленных на отказ в обслуживании;
- защита каналов передачи данных и сетевого взаимодействия.

4.7.В случае если информационная технология, защита которой осуществляется посредством реализации базовых групп мер, указанных в пункте 4.6 настоящей Политики, не применима для ИС КСП МО СМР КК, то такие меры/группы мер не подлежат реализации в рамках защиты информационных систем и содержащейся в них информации.

4.8.Реализация мер по защите информационных систем и содержащейся в них информации, подлежащих реализации в ИС КСП МО СМР КК, должна обеспечивать защиту от нарушителей с базовым повышенным уровнем возможностей.

4.9.В целях подтверждения достаточности принятых мер защиты информационных систем и содержащейся в них информации до начала обработки и (или) хранения информации в ИС КСП МО СМР КК должна быть проведена аттестация на соответствие требованиям по защите информации в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. № 77.

4.10. При отсутствии возможности реализации отдельных мероприятий и (или) принятия мер по защите информации, разрабатываются и внедряются компенсирующие меры, позволяющие обеспечить блокирование (нейтрализацию) актуальных для ИС КСП МО СМР КК угроз безопасности информации. При этом применение компенсирующих мер должно быть обоснованно на этапе создания ИС КСП МО СМР КК, а при проведении аттестационных испытаний должна быть подтверждена их эффективность для блокирования (нейтрализации) актуальных для ИС КСП МО СМР КК угроз безопасности информации.

4.11. Технические меры по защите информации должны приниматься на аппаратном, системном, прикладном уровнях, а также в информационно-телекоммуникационной инфраструктуре КСП МО СМР КК. На аппаратном и системном уровнях защита информации должна обеспечиваться посредством применения встроенных в аппаратное обеспечение и системное программное обеспечение средств защиты информации (при наличии технической возможности). На прикладном и сетевом (инфраструктурном) уровнях защита информации должна обеспечиваться применением встроенных в прикладное программное обеспечение средств защиты информации и (или) применением наложенных и сетевых средств защиты информации.

4.12. Для защиты информации должны применяться сертифицированные средства защиты информации в соответствии с инструкциями (правилами) по их эксплуатации, установленными разработчиками в эксплуатационной документации. Применяемые средства защиты информации должны быть обеспечены со стороны их разработчиков поддержкой безопасности на территории Российской Федерации, включая выпуск и применение обновлений программного обеспечения, обеспечивающих устранение выявленных уязвимостей, дефектов и недостатков.

4.13. Средства защиты информации, применяемые в КСП МО СМР КК, должны соответствовать требованиям, установленным к 6 классу защиты и уровню доверия или более высокому классу защиты и (или) уровню доверия, а также соответствовать требованиям пункта 6 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

5. Категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия

5.1.В деятельности по защите информации участвуют следующие категории лиц:

− Председатель КСП МО СМР КК или назначенное им лицо, ответственное за организацию деятельности по защите информации;

− отдельные работники КСП МО СМР КК, на которых возложены обязанности (функции) по защите информации;

− отдельные работники КСП МО СМР КК, на которых возложены обязанности по обеспечению эксплуатации информационных активов и информационно-телекоммуникационной инфраструктуры КСП МО СМР КК.

5.2.Защиту информации в КСП МО СМР КК организует председатель КСП МО СМР КК или по его решению ответственное лицо.

5.3.Председатель КСП МО СМР КК или назначенное им лицо, ответственное за организацию деятельности по защите информации, исполняет следующие функции:

− организует разработку политики, направленной в том числе на обеспечение и поддержание стабильного функционирования ИС КСП МО СМР КК и процессов обработки информации в КСП МО СМР КК в случае наступления негативных последствий при реализации угроз безопасности информации, отвечает за согласование и утверждение такой политики, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;

− организует работу по обеспечению безопасности информации, обрабатываемой в ИС КСП МО СМР КК, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, формулированию перечня негативных последствий, проведению мероприятий по их недопущению, отслеживанию и контролю эффективности (результативности) таких мероприятий, а также по необходимому информационному обмену;

− организует реализацию и контроль проведения мероприятий и мер по защите информации, с учетом требований и рекомендаций федерального органа

исполнительной власти в области обеспечения безопасности и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации;

− организует контроль за выполнением требований нормативных правовых актов, нормативно-технической документации, и соблюдением установленного порядка выполнения работ по защите информации;

− организует повышение осведомленности, формирование и развитие навыков и умений пользователей ИС КСП МО СМР КК в области защиты информации, в том числе планирует мероприятия по проведению обучения и повышения квалификации работников КСП МО СМР КК, на которых возложены обязанности (функции) по защите информации;

− организует контроль исполнения пользователями ИС КСП МО СМР КК требований по защите информации, установленными внутренними стандартами и регламентами КСП МО СМР КК;

− организует планирование мероприятий по обеспечению информационной безопасности в КСП МО СМР КК;

− организует подготовку локальных правовых актов, иных организационно-распорядительных документов по вопросам обеспечения защиты информации в КСП МО СМР КК;

− организует проведение контроля за состоянием защищенности информации, обрабатываемой в ИС КСП МО СМР КК, включая оценку защищенности информационных активов и информационно-телекоммуникационной инфраструктуры КСП МО СМР КК.

5.4.Председатель КСП МО СМР КК или назначенное им лицо, ответственное за организацию деятельности по защите информации, исполняет обладает следующими полномочиями:

− давать указания и поручения работникам КСП МО СМР КК в части обеспечения безопасности информации, обрабатываемой в ИС КСП МО СМР КК;

− запрашивать от работников КСП МО СМР КК информацию и материалы, необходимые для реализации возложенных полномочий в части обеспечения безопасности информации, обрабатываемой в ИС КСП МО СМР КК;

− участвовать в заседаниях (совещаниях) комиссий КСП МО СМР КК, принятии решений по вопросам защиты информации в КСП МО СМР КК, а также по внесению предложений по совершенствованию деятельности по защите информации;

− участвовать в разработке организационно-распорядительной документации, внутренних стандартов и регламентов по защите информации;

− принимать решения по вопросам обеспечения информационной безопасности в КСП МО СМР КК;

− взаимодействовать с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, и иными органами власти по вопросам обеспечения защиты информации, в том числе по вопросам совершенствования законодательства Российской Федерации в области защиты информации;

− вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности;

− инициировать проверки уровня (состояния) защищенности информации, обрабатываемой в ИС КСП МО СМР КК;

− организовывать разработку предложений по внесению изменений в процессы обработки информации в ИС КСП МО СМР КК, состав и порядок реализации мероприятий и мер по защите информации в ИС КСП МО СМР КК, принятию иных мер, направленных на недопущение негативных последствий реализации угроз безопасности информации.

5.5.Председатель КСП МО СМР КК или назначенное им лицо, ответственное за организацию деятельности по защите информации, назначают отдельного специалиста, на которого возлагаются обязанности (функции) по защите информации (далее – лицо, ответственное за обеспечение защиты информации в КСП МО СМР КК).

5.6.Лицо, ответственное за обеспечение защиты информации в КСП МО СМР КК, исполняет следующие функции:

− разрабатывает, координирует, реализует и обеспечивает контроль за реализацией мероприятий и мер по защите информации;

− разрабатывает предложения по совершенствованию организационно-распорядительных документов по защите информации и представление их на утверждение лицу, ответственному за организацию деятельности по защите информации;

− анализирует и выявляет угрозы безопасности информации в ИС КСП МО СМР КК, в том числе уязвимостей программного обеспечения, программно-аппаратных средств и принимает меры по их устранению;

− разрабатывает и реализует организационных мер и технических мер по защите информации, в соответствии с установленными для ИС КСП МО СМР КК требований внутренних стандартов и регламентов по защите информации;

− определяет перечень событий информационной безопасности, подлежащих реагированию (инцидентов информационной безопасности), и обеспечивает своевременное выявление и реагирование на такие события (инциденты);

− обеспечивает своевременность процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак;

− проводит контроль за состоянием защищенности ИС КСП МО СМР КК и подготавливает предложения по повышению состояния защищенности в части реализуемых мероприятий и мер по защите информации;

− подготовка отчетной документации о состоянии деятельности по защите информации;

− обеспечивает повышение осведомленности, формирование и развитие навыков и умений пользователей ИС КСП МО СМР КК в области защиты информации, в том числе обеспечивает реализацию мероприятий по обучению и повышению квалификации работников КСП МО СМР КК, на которых возложены обязанности (функции) по защите информации.

5.7.Лицо, ответственное за обеспечение защиты информации в КСП МО СМР КК, обладает следующими полномочиями:

− контролировать исполнение работниками КСП МО СМР КК требований по защите информации, обрабатываемой в ИС КСП МО СМР КК;

− запрашивать и получать от работников КСП МО СМР КК информацию и материалы, необходимые для реализации возложенных полномочий в части обеспечения безопасности информации, обрабатываемой в ИС КСП МО СМР КК;

− участвовать в заседаниях (совещаниях) комиссий КСП МО СМР КК, принятии решений по вопросам защиты информации в КСП МО СМР КК, а также по внесению предложений по совершенствованию деятельности по защите информации;

− участвовать в разработке организационно-распорядительной документации, внутренних стандартов и регламентов по защите информации;

− взаимодействовать с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, и иными органами власти по вопросам обеспечения защиты информации, в том числе по вопросам совершенствования законодательства Российской Федерации в области защиты информации;

− вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в

соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности;

− проводить проверки уровня (состояния) защищенности информации, обрабатываемой в ИС КСП МО СМР КК;

− подготавливать предложения по внесению изменений в процессы обработки информации в КСП МО СМР КК, состав и порядок реализации мероприятий и мер по защите информации в ИС КСП МО СМР КК, принятию иных мер, направленных на недопущение негативных последствий реализации угроз безопасности информации.

5.8.Председатель КСП МО СМР КК или назначенное им лицо, ответственное за организацию деятельности по защите информации назначают отдельного специалиста, на которого возлагаются обязанности (функции) по обеспечению эксплуатации информационных активов и информационно-телекоммуникационной инфраструктуры КСП МО СМР КК (лицо, ответственное за обеспечение эксплуатацию ИС КСП МО СМР КК).

5.9.Лицо, ответственное за эксплуатацию ИС КСП МО СМР КК, исполняет следующие функции:

− обеспечивать учёт информационных активов и компонентов информационно-телекоммуникационных инфраструктуры КСП МО СМР КК, находящихся в зоне его ответственности, в соответствии с установленным порядком учета и эксплуатации;

− обеспечивать надежное функционирование информационных активов и компонентов информационно-телекоммуникационных инфраструктуры КСП МО СМР КК, находящихся в зоне его ответственности;

− обеспечивать настройку программного обеспечения и программно-аппаратных комплексов в соответствии с требованиями эксплуатационной документации;

− обеспечивать процессы резервного копирования и восстановления информации, а также учёта процессов резервирования и восстановления;

− обеспечивать процесс устранения уязвимостей информационных систем, выявленных администратором информационной безопасности;

− обеспечивать процессы мониторинга и анализа событий безопасности информации с целью выявления инцидентов информационной безопасности.

5.10. Лицо, ответственное за обеспечение защиты информации в КСП МО СМР КК, обладает следующими полномочиями:

− требовать от пользователей ИС КСП МО СМР КК соблюдения установленной технологии обработки информации и выполнения требований внутренних стандартов и регламентов по защите информации;

− контролировать исполнение работниками КСП МО СМР КК требований по защите информации, обрабатываемой в ИС КСП МО СМР КК;

− запрашивать и получать от работников КСП МО СМР КК информацию и материалы, необходимые для реализации возложенных полномочий в части обеспечения безопасности информации, обрабатываемой в ИС КСП МО СМР КК;

− подготавливать предложения по внесению изменений в процессы обработки информации в КСП МО СМР КК, состав и порядок реализации мероприятий и мер по защите информации в ИС КСП МО СМР КК, принятию иных мер, направленных на недопущение негативных последствий реализации угроз безопасности информации.

6. Ответственность за неисполнение положений настоящей Политики

6.1.Лица, не выполняющие или ненадлежаще выполняющие требования настоящей Политики, или нарушающие иные требования о защите информации, установленные организационно-распорядительными документами КСП МО СМР КК привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и (или) уголовной ответственности в порядке, установленном законодательством Российской Федерации.

7. Заключительные положения

7.1.Настоящая Политика вступает в силу с момента ее утверждения и действует до момента ее отмены.

7.2.Если в результате изменения законодательных и нормативных актов Российской Федерации отдельные разделы/пункты Политики вступают в противоречие с ними, то такие разделы/пункты утрачивают силу, и до момента внесения изменений в Политику участники процесса руководствуются действующим законодательством Российской Федерации.

7.3.Настоящая Политика подлежит пересмотру в случаях:

− изменения законодательных и нормативных актов Российской Федерации, касающихся процессов, описанных в Политике;

− существенных изменений процессов, описанных в Политике;

− в ходе периодического анализа исполнения настоящей Политики, но не реже чем один раз в три года.