УТВЕРЖДАЮ

Директор МКУ КМЦИКТ

«СТАРТ» В.В.Миклашевская

«19» _____ 2025 г.

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В МУНИЦИПАЛЬНОМ КАЗЕННОМ УЧРЕЖДЕНИИ
«КРАСНОДАРСКИЙ МЕТОДИЧЕСКИЙ ЦЕНТР
ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ
«СТАРТ»

г. Краснодар
2025 г.

Содержание

1. Общие положения 3

2. Термины и определения 4

3. Описание объекта защиты 5

4. Цели и задачи деятельности по обеспечению информационной безопасности 6

5. Основные положения по обеспечению информационной безопасности 6

6. Организационная основа деятельности по обеспечению информационной безопасности 9

7. Ответственность за соблюдение положений Политики 10

8. Контроль за соблюдением положений Политики 12

9. Заключительные положения 12

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается в том числе на:

– доктрине информационной безопасности РФ (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.);

– национальном стандарте Российской федерации ГОСТ Р ИСО/МЭК 27001-2006.

1.2. Настоящая Политика является документом, доступным любому сотруднику муниципальном казенном учреждении «Краснодарский методический центр информационно-коммуникационных технологий «Старт» (далее – МКУ КМЦИКТ «Старт») и пользователю его ресурсов, и представляет собой официально принятую руководством систему взглядов на обеспечение информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности.

1.3. Руководство осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития нормативно-правовой базы в области защиты информации. Соблюдение требований информационной безопасности позволит более качественно выполнять возложенные на него функции и обеспечит, соответствие информационных процессов МКУ КМЦИКТ «Старт» правовым и регулятивным требованиям.

1.4. Требования информационной безопасности, которые предъявляются МКУ КМЦИКТ «Старт», соответствуют интересам и целям его деятельности и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.5. Стратегия МКУ КМЦИКТ «Старт» в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности требований:

– российского законодательства в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных, и других правовых актов;

– нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения физической безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности и приватности;

– национальных стандартов Российской Федерации в области информационной безопасности.

1.6. Требования по обеспечению информационной безопасности МКУ КМЦИКТ «Старт» должны неукоснительно соблюдаться всеми сотрудниками МКУ КМЦИКТ «Старт» и другими, взаимодействующими с МКУ КМЦИКТ «Старт» сторонами.

1.7. Настоящая Политика является верхнеуровневым документом по информационной безопасности МКУ КМЦИКТ «Старт».

1.8. Документами, детализирующими положения Политики МКУ КМЦИКТ «Старт», являются частные политики по обеспечению информационной безопасности, положения, регламенты, инструкции, которые являются документами по обеспечению информационной безопасности второго уровня и последующего уровня, оформляются как отдельные внутренние нормативные документы МКУ КМЦИКТ «Старт», разрабатываются и согласовываются в соответствии с установленным в МКУ КМЦИКТ «Старт» порядком.

2. Термины и определения

2.1. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств. [Федеральный Закон РФ от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»]

2.2. Конфиденциальность – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта и процесса [ГОСТ Р ИСО/МЭК 27001-2006].

2.3. Целостность – свойство сохранять правильность и полноту активов [ГОСТ Р ИСО/МЭК 27001-2006].

2.4. Доступность – свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта [ГОСТ Р ИСО/МЭК 27001-2006].

2.5. Информационная безопасность – свойство информации сохранять конфиденциальность, целостность и доступность [ГОСТ Р ИСО/МЭК 27001-2006]

2.6. Модель угроз (информационной безопасности) – физическое, математическое представление свойств и характеристик угроз безопасности информации [ГОСТ Р 50922-2006].

2.7. Событие информационной безопасности – идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью. [ГОСТ Р ИСО/МЭК 27001-2006]

2.8. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность [ГОСТ Р ИСО/МЭК 27001-2006].

2.9. Система менеджмента информационной безопасности – часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности [ГОСТ Р ИСО/МЭК 27001-2006].

2.10. Угроза – потенциальная причина нежелательного инцидента, результатом которого может быть нанесение ущерба системе или организации.

2.11. Риск информационной безопасности – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесёт ущерб организации [ГОСТ Р ИСО/МЭК 27005-2010].

2.12. Анализ риска – систематическое использование информации для определения источников риска и количественной оценки риска [ГОСТ Р ИСО/МЭК 27001-2006].

2.13. Оценка риска – общий процесс анализа риска и его оценивания [ГОСТ Р ИСО/МЭК 27001-2006].

2.14. Менеджмент риска – скоординированные действия по руководству и управлению организацией в отношении риска [ГОСТ Р ИСО/МЭК 27001-2006].

3. Описание объекта защиты

3.1. Основными объектами защиты системы информационной безопасности в МКУ КМЦИКТ «Старт» являются:

3.1.1. Информационные ресурсы, содержащие конфиденциальную информацию независимо от формы и вида ее представления, включая:

- служебную информацию;
- персональные данные сотрудников;
- персональные данные лиц, не являющихся сотрудниками;
- открытую (общедоступную) информацию.

3.1.2. Сотрудники МКУ КМЦИКТ «Старт», являющиеся пользователями информационных систем МКУ КМЦИКТ «Старт»;

3.1.3. Информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

4. Цели и задачи деятельности по обеспечению информационной безопасности

4.1. Целью деятельности по обеспечению информационной безопасности является снижение угроз информационной безопасности до приемлемого уровня.

4.2. Основные задачи деятельности по обеспечению информационной безопасности :

- выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
- исключение либо минимизация выявленных угроз;
- предотвращение инцидентов информационной безопасности.

5. Основные положения по обеспечению информационной безопасности

5.1. Требования по обеспечению информационной безопасности в МКУ КМЦИКТ «Старт» обязательны к соблюдению всеми работниками МКУ КМЦИКТ «Старт» и пользователями информационных систем.

5.2. Неисполнение или некачественное исполнение сотрудниками обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в МКУ КМЦИКТ «Старт» порядком либо требованиями действующего законодательства.

5.3. Стратегия МКУ КМЦИКТ «Старт» в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства, до специализированных мер информационной безопасности по каждому выявленному риску, основанных на оценке рисков информационной безопасности.

5.4. С целью поддержки заданного уровня защищенности, МКУ КМЦИКТ «Старт» придерживается процессного подхода в построении системы менеджмента информационной безопасности. Система менеджмента информационной безопасности МКУ КМЦИКТ «Старт» основывается на осуществлении следующих основных процессов (планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование) соответствующих требованиям и положениям национальных стандартов по обеспечению информационной безопасности. Реализация этих процессов осуществляется в виде непрерывного цикла – «планирование – реализация – проверка – совершенствование – планирование», направленного на постоянное совершенствование деятельности по обеспечению информационной безопасности и повышение ее эффективности.

5.5. При планировании мероприятий по обеспечению информационной безопасности осуществляются:

5.5.1. Определение и распределение ролей персонала, связанного с обеспечением информационной безопасности (ролей информационной безопасности).

5.5.2. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.

5.5.3. Менеджмент рисков информационной безопасности, включающий:

– анализ влияния на информационную безопасность МКУ КМЦИКТ «Старт» применяемых в деятельности МКУ КМЦИКТ «Старт» технологий, а также внешних событий;

– выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;

– определение моделей угроз и нарушителя информационной безопасности;

– выявление, анализ и оценка значимых угроз информационной безопасности;

– выявление возможных негативных последствий, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов;

– идентификацию и анализ рисковых событий информационной безопасности;

– оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для МКУ КМЦИКТ «Старт»;

– обработку результатов оценки рисков информационной безопасности;

– оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для МКУ КМЦИКТ «Старт» в случае наступления рисковых событий;

– оценку влияния защитных мер на цели основной деятельности МКУ КМЦИКТ «Старт»;

– оценку затрат на реализацию защитных мер;

– рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;

– разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности МКУ КМЦИКТ «Старт» и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;

– документальное оформление целей и задач обеспечения информационной безопасности МКУ КМЦИКТ «Старт», поддержка в актуальном состоянии нормативно – методического обеспечения деятельности в сфере информационной безопасности.

5.6. В рамках реализации деятельности по обеспечению информационной безопасности осуществляются:

5.7.1 Менеджмент инцидентов информационной безопасности, включающий:

– сбор информации о событиях информационной безопасности;

– выявление и анализ инцидентов информационной безопасности;

– расследование инцидентов информационной безопасности;

– оперативное реагирование на инцидент информационной безопасности;

– минимизация негативных последствий инцидентов информационной безопасности;

– оперативное доведение до руководства информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;

– выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;

– пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;

– повышение уровня знаний персонала в вопросах обеспечения информационной безопасности;

– обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем МКУ КМЦИКТ «Старт» и информации, обрабатываемой в них;

– применение средств криптографической защиты информации;

– обеспечение бесперебойной работы автоматизированных систем и сетей связи;

– обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;

– применение средств защиты от вредоносных программ;

– обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем МКУ КМЦИКТ «Старт», связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);

– обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;

– контроль доступа в здания и помещения.

5.7. В целях проверки деятельности по обеспечению информационной безопасности в МКУ КМЦИКТ «Старт» осуществляются:

– контроль правильности реализации и эксплуатации защитных мер;

– контроль изменений конфигурации систем и подсистем;

– мониторинг факторов рисков и соответствующий их пересмотр;

– контроль реализации и исполнения требований сотрудниками действующих внутренних нормативных документов по обеспечению информационной безопасности;

– контроль деятельности сотрудников и других пользователей информационных систем МКУ КМЦИКТ «Старт», направленный на выявление и предотвращение конфликтов интересов.

5.8. В целях совершенствования деятельности по обеспечению информационной безопасности в МКУ КМЦИКТ «Старт» осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности.

6. Организационная основа деятельности по обеспечению информационной безопасности

6.1. В целях выполнения задач по обеспечению информационной безопасности, в соответствии с рекомендациями международных и российских стандартов по безопасности в МКУ КМЦИКТ «Старт» должны быть определены следующие роли:

– ответственный за защиту информации (далее - Ответственный сотрудник);

– пользователи информационных систем.

При необходимости могут быть определены и другие роли по информационной безопасности.

6.2. Основными функциями Ответственного сотрудника в вопросах информационной безопасности являются:

– назначение ответственных лиц в области информационной безопасности;

– координация и внедрение информационной безопасности в МКУ КМЦИКТ «Старт».

6.3. Основными задачами работников при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению информационной безопасности МКУ КМЦИКТ «Старт» являются:

– соблюдение требований информационной безопасности, устанавливаемых нормативными документами МКУ КМЦИКТ «Старт»;

– выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;

– выявление и реагирование на инциденты информационной безопасности;

– информирование в установленном порядке ответственных лиц о выявленных угрозах и рисковых событиях информационной безопасности;

– прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;

– мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;

– информирование своего руководства и Ответственного сотрудника о выявленной угрозе в информационной среде МКУ КМЦИКТ «Старт».

7. Ответственность за соблюдение положений Политики

7.1. Общее руководство обеспечением информационной безопасности МКУ КМЦИКТ «Старт» осуществляет Ответственный сотрудник.

7.2. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности лежит на начальнике информационно-технического отдела МКУ КМЦИКТ «Старт».

7.3. Ответственность работников за нарушение политики обработки и защиты информации ограниченного доступа, определена действующим законодательством:

– виды дисциплинарных взысканий, порядок их применения и снятия установлены главой 30 ТК РФ;

– согласно статье 24 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении норм, регулирующих обработку ПДн, несут дисциплинарную, административную, гражданскую, уголовную и иную предусмотренную законодательством Российской Федерации ответственность;

– к административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах и за нарушение правил защиты информации могут привлекаться как само Учреждение и его должностные лица, так и конкретные работники, исполняющие соответствующие трудовые функции;

– лица, виновные в нарушении правил обработки или защиты информации ограниченного доступа, могут привлекаться к административной ответственности по следующим основаниям:

- неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих его права и свободы, либо несвоевременное предоставление таких документов и материалов, непредоставление иной информации в случаях,

предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации (ст. 5.39 КоАП);

- нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП);
- нарушение правил защиты информации (ст. 13.12 КоАП);
- разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, когда ее разглашение влечет уголовную ответственность), лицом, получившим к ней доступ в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

– уголовная ответственность за нарушение правил обработки информации ограниченного доступа может наступить в следующих случаях:

- неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ);
- создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ст. 273 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб или повлекшее тяжкие последствия (ст.274 УК РФ).
- незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан (ст. 137 УК РФ);
- неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной

информации, если эти деяния причинили вред правам и законным интересам граждан (ст. 140 УК РФ).

8. Контроль за соблюдением положений Политики

8.1. Общий контроль состояния информационной безопасности осуществляется Ответственным сотрудником.

8.2. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности МКУ КМЦИКТ «Старт», по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

9. Заключительные положения

9.1. Требования настоящей Политики могут развиваться другим внутренними нормативными документами, которые дополняют и уточняют ее.

9.2. В случае изменения действующего законодательства и иных нормативных актов, а также Положения МКУ КМЦИКТ «Старт» настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Положению МКУ КМЦИКТ «Старт». В этом случае Ответственный сотрудник обязан незамедлительно инициировать внесение соответствующих изменений.

9.3. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

– пересмотр положений настоящей Политики должен осуществляться не реже одного раза в 24 месяца;

– внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.