Р А С П О Р Я Ж Е Н И Е

АДМИНИСТРАЦИИ
АЛЕКСАНДРОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
СТАВРОПОЛЬСКОГО КРАЯ

25 июня 2024 г. с. Александровское № 169-р

Об утверждении политики информационной безопасности администрации Александровского муниципального округа Ставропольского края, политики организации парольной защиты в администрации Александровского муниципального округа Ставропольского края, политики резервного копирования критически важной информации в администрации Александровского муниципального округа Ставропольского края, политики организации антивирусной защиты в администрации Александровского муниципального округа Ставропольского края

Во исполнение национального стандарта РФ (ГОСТ Р 50922-2006), а также Указа Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации":

1. Утвердить прилагаемые политики:

1.1. Политика информационной безопасности администрации Александровского муниципального округа Ставропольского края.

1.2. Политика организации парольной защиты в администрации Александровского муниципального округа Ставропольского края.

1.3. Политика резервного копирования критически важной информации в администрации Александровского муниципального округа Ставропольского края.

1.4. Политика организации антивирусной защиты в администрации Александровского муниципального округа Ставропольского края.

2. Настоящее распоряжение подлежит размещению на официальном сайте администрации Александровского муниципального округа в информационно-телекоммуникационной сети «Интернет».

3. Контроль за выполнением настоящего распоряжения возложить на управляющего делами администрации Александровского муниципального округа Ставропольского края Иванову Ю.В.

4. Настоящее постановление вступает в силу со дня его подписания.

Глава Александровского
муниципального округа
Ставропольского края А.В. Щекин

УТВЕРЖДЕНА
распоряжением администрации
Александровского муниципального
округа Ставропольского края
от 25 июня 2024 г. № 169-р

Политика информационной безопасности администрации Александровского муниципального округа Ставропольского края

Определения

Защита информации	деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
Информация	сведения (сообщения, данные) независимо от формы их представления
Информация ограниченного доступа	информация, доступ к которой ограничен федеральными законами
Информационная система	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Конфиденциальность информации	обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
Обладатель информации	лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким- либо признакам
Персональные данные	любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)

Обозначения и сокращения

ААМО СК	Администрация Александровского муниципального округа Ставропольского края
КИ	Конфиденциальная информация
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
СЗИ	Система защиты информации

СКЗИ	Средство криптографической защиты информации
СрЗИ	Средство защиты информации
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
КСПД	Корпоративная сеть передачи данных

1.1. Настоящий документ «Политика информационной безопасности администрации Александровского муниципального округа Ставропольского края» (далее — Политика) является доступным всем сотрудникам ААМО СК и всем пользователям его ресурсов. Представляет собой официально принятую руководством ААМО СК систему взглядов на обеспечение информационной безопасности в ААМО СК.

1.2. Основной задачей в области информационной безопасности ААМО СК признает совершенствование мер и средств обеспечения информационной безопасности информационных ресурсов ААМО СК в контексте развития законодательства и норм регулирования информационной деятельности.

1.3. В рамках своей деятельности ААМО СК обязуется предпринимать все возможные меры для защиты информации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности или других противоправных действий, связанных с нарушением информационной безопасности ААМО СК.

1.4. Требования информационной безопасности, которые предъявляются ААМО СК, соответствуют целям деятельности ААМО СК и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.5. Реализация и контроль исполнения требований, установленных настоящей Политикой, осуществляется работниками структурных подразделений ААМО СК, ответственных за информационную безопасность, в соответствии со своими должностными инструкциями и другими внутренними документами ААМО СК по информационной безопасности.

2. Цели и задачи обеспечения информационной безопасности

2.1. Целями обеспечения информационной безопасности ААМО СК являются:

- защита интересов ААМО СК, работников и иных субъектов

информационных отношений, взаимодействующих с ААМО СК, от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем ААМО СК, нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;

- обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов ААМО СК и предоставляемых сервисов;

- соблюдение правового режима использования массивов и программ обработки информации;

- предотвращение реализации угроз безопасности для деятельности ААМО СК.

2.2. Объектами информационных правоотношений являются:

- информационные ресурсы, в том числе с ограниченным доступом;
- процессы обработки информации в информационных системах ААМО СК, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;
- информационная инфраструктура, включающая системы обработки, хранения 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 хранилища информации.

2.3. Субъектами информационных отношений при использовании информационных систем ААМО СК, заинтересованными в обеспечении информационной безопасности, являются:
- ААМО СК, как собственник информационных ресурсов и оператор персональных данных;
- работники подразделений ААМО СК, как пользователи и поставщики информации в информационные системы;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах ААМО СК.

2.4. Субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности определенной части информации;
- целостности информации;
- своевременного доступа к необходимой им информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты соответствующей части информации от незаконного ее тиражирования и распространения.

2.5. Для достижения целей защиты и обеспечения указанных свойств информации, система обеспечения информационной безопасности ААМО СК должна обеспечивать решение следующих задач:

2.5.1. Защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (возможность использования системы и доступ к ее ресурсам должны иметь только зарегистрированные пользователи).

2.5.2. Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационных систем (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей).

2.5.3. Регистрацию и периодический контроль действий пользователей при использовании защищаемых ресурсов и периодический контроль корректности их действий.

2.5.4. Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения.

2.5.5. Защиту от несанкционированной модификации и контроль целостности используемых в ААМО СК программных средств и данных, а также защиту от несанкционированного внедрения вредоносных программ.

2.5.6. Защиту информации ограниченного доступа, хранимой, обрабатываемой в ААМО СК, от несанкционированного разглашения или искажения.

2.5.7. Обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации), а также определение автора при создании и модификации информации.

2.5.8. Обеспечение исправности применяемых в информационных системах ААМО СК средств защиты информации.

2.5.9. Своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации.

2.5.10.Создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации в ААМО СК.

2.6. Решение вышеперечисленных задач в ААМО СК осуществляется:

2.6.1. Учетом всех подлежащих защите информационных ресурсов (каналов связи, аппаратных и программных средств).

2.6.2. Регламентацией процессов обработки подлежащей защите информации, действий работников ААМО СК и персонала, осуществляющего обслуживание и модификацию программных и технических средств, на основе утвержденных организационно распорядительных документов по вопросам обеспечения информационной безопасности.

2.6.3. Назначением и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в ААМО СК.

2.6.4. Наделением каждого работника минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам.

2.6.5. Знанием и строгим соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства, требований организационно распорядительных документов по вопросам обеспечения информационной безопасности.

2.6.6. Персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам информационных систем.

2.6.7. Реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных.

2.6.8. Принятием мер по обеспечению физической целостности технических средств информационных систем и поддержанием необходимого уровня защищенности их компонентов.

2.6.9. Использованием физических и технических (программно-аппаратных) средств защиты ресурсов ААМО СК и административной поддержкой их использования.

2.6.10. Контролем соблюдения пользователями информационных систем требований по обеспечению информационной безопасности.

2.6.11. Юридической защитой интересов ААМО СК при взаимодействии с юридическими и физическими лицами от противоправных и несанкционированных действий со стороны этих лиц.

2.6.12. Проведением анализа эффективности принятых мер и применяемых средств защиты информации в ААМО СК. Разработкой и реализацией предложений по совершенствованию СЗИ в ААМО СК.

3. Принципы обеспечения информационной безопасности

3.1. Принцип законности

3.1.1. При выборе защитных мероприятий, реализуемых системой обеспечения информационной безопасности, должно соблюдаться действующее законодательство.

3.1.2. Принятые меры защиты не должны препятствовать доступу к защищаемой информации со стороны государственных или правоохранительных органов, если такой доступ необходим в случаях, предусмотренных законодательством.

3.1.3. Программно-технические средства, применяемые в ААМО СК, должны иметь соответствующие лицензии, официально приобретаться ААМО СК у представителей разработчиков этих средств.

3.2. Принцип системности

3.2.1 При построении системы обеспечения информационной безопасности необходимо применять системный подход, который предполагает взаимосвязь процессов организации защиты информационных ресурсов ААМО СК, согласованное применение методов и средств защиты информационных ресурсов ААМО СК.

3.3. Принцип координации

3.3.1. При организации действий по обеспечению информационной безопасности руководство ААМО СК обеспечивает четкую взаимосвязь соответствующих структурных подразделений между собой, с представителями сторонних организаций, оказывающих услуги в рамках договорных обязательств.

3.32. При построении, внедрении и эксплуатации системы обеспечения информационной безопасности руководство ААМО СК обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

3.4. Принцип дружественности и простоты

3.4.1. Система обеспечения информационной безопасности в ААМО СК формируется таким образом, чтобы сделать максимально прозрачными для пользователей информационных систем ААМО СК процессы ее функционирования.

3.4.2. Система обеспечения информационной безопасности в ААМО СК выстраивается таким образом, чтобы ограничения организационного и технического характера, налагаемые на сотрудников ААМО СК в связи с реализацией защитных мер, существенно не затрудняли работу с ресурсами

информационных систем ААМО СК.

3.5. Принцип превентивности

Меры, применяемые ААМО СК с целью обеспечения информационной безопасности, должны носить упреждающий характер и не допускать реализацию соответствующих угроз и атак.

3.6. Принцип оптимальности и многоуровневости

3.6.1. Выбор единых программно-технических средств с целью сокращения расходов на создание и поддержку функционирования компонентов системы обеспечения информационной безопасности.

3.6.2. Применение разнородных программно-технических средств защиты, с целью построения целостной системы обеспечения информационной безопасности и устранения возможных уязвимостей.

3.6.3. Использование для создания разных рубежей обеспечения информационной безопасности средств, которые имеют схожие друг с другом функции, но разработанные различными производителями и имеющие различную логику построения защитных механизмов.

3.7. Принцип экономической целесообразности

3.7.1. Осуществление оценки уровня затрат на обеспечение безопасности, ценности информационных ресурсов и величины возможного ущерба для ААМО СК в случае нарушения конфиденциальности, целостности и доступности информационных ресурсов.

3.7.2. Выбор необходимого и достаточного уровня защиты информационных ресурсов, при котором затраты, риск и размер возможного ущерба являются приемлемыми.

3.8. Принцип непрерывности и недопустимости открытого состояния

Система обеспечения информационной безопасности в ААМО СК строится таким образом, чтобы процесс защиты информационных систем ААМО СК осуществлялся непрерывно и целен на протяжении всего жизненного цикла информационных систем.

3.8.1. Система обеспечения информационной безопасности в ААМО СК при любых возникающих обстоятельствах либо полностью выполняет свои функции, либо полностью блокирует доступ.

3.9. Принцип профессионализма

3.9.1. Привлечение для разработки и внедрения системы обеспечения информационной безопасности, при необходимости, специализированных организаций, наиболее подготовленных к конкретному виду деятельности и имеющих соответствующие лицензии на выполнения работ и практический опыт в данной области.

3.9.2. Организация профессиональной подготовки своих работников для эксплуатации компонентов системы обеспечения информационной безопасности.

3.10. Принцип выбора решений защиты

3.10.1. Ориентация на применение современных высокотехнологичных

решений и программно-технических средств защиты, хорошо зарекомендовавших себя, интуитивно понятных и не сложных в эксплуатации.

3.10.2. Использование оценки степени корректности функционирования и исполнения защитных функций, отказоустойчивости, проверки согласованности конфигурации различных компонентов и возможности осуществления централизованного администрирования при выборе решений по защите информационных систем.

3.11. Принцип развития

3.11.1. Развитие и обновление на регулярной основе существующей системы обеспечения информационной безопасности.

3.11.2. Ориентация на преемственность принятых ранее решений по защите, на анализ функционирования информационных систем и самой системы обеспечения информационной безопасности.

3.12. Принцип персональной ответственности и разделения обязанностей

3.12.1. Руководство ААМО СК определяет права и ответственность каждого конкретного работника (в пределах его должностных обязанностей) за обеспечение безопасности информационных ресурсов ААМО СК.

3.12.2. Система обеспечения информационной безопасности ААМО СК обеспечивает разделение полномочий в информационных системах, обязанностей и ответственности между работниками, исключающее возможность нарушения критически важных для ААМО СК процессов или создания уязвимостей в защите информационных ресурсов.

3.13. Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих функций в ААМО СК, в соответствии со своими должностными обязанностями.

4. Зоны ответственности участников процесса обеспечения информационной безопасности

4.1. Руководство ААМО СК

4.1.1. Создает условия, при которых каждый работник ААМО СК знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов.

4.1.2. Назначает работников, ответственных за создание и использование СЗИ, информации обрабатываемой в ААМО СК, реализацию процессов обеспечения информационной безопасности, а также их контроля.

4.1.3. Обеспечивает достаточную численность и квалификацию персонала, ответственного за построение и поддержание процессов обеспечения информационной безопасности, внедрение и управление СЗИ, а

также контроль и мониторинг текущего состояния системы обеспечения информационной безопасности ААМО СК.

4.1.4. Инициирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в ААМО СК.

4.1.5. Анализирует результаты работ по обеспечению информационной безопасности и на их основе принимает решения о необходимости развития системы обеспечения информационной безопасности, ее развития, о возможности принятия остаточных рисков информационной безопасности, о выделении ресурсов, необходимых для реализации Политики информационной безопасности.

4.2. Компетентные подразделения ААМО СК

4.2.1. Подготавливают предложения по доработке Политики информационной безопасности в части технического обеспечения информационных систем ААМО СК.

4.2.2. Разрабатывают процедуры эффективного управления техническими и программными средствами информационных систем и применяют их в практической деятельности в отношении всех систем, действующих в ААМО СК.

4.2.3. Организуют проведение необходимого инструктажа работников структурных подразделений в части вопросов безопасной эксплуатации информационных систем.

4.2.4. Обеспечивают защиту доступа ко всему серверному и коммутационному оборудованию, носителям информации, которые используются в соответствующих структурных подразделениях.

4.2.5. Осуществляют мероприятия по поддержке сопровождения и использования информационных систем.

4.2.6. Обеспечивают отказоустойчивость всего программно-аппаратного комплекса и процедуру регламентированного восстановления работоспособности после отказов компонентов.

4.2.7. Регулярно обновляют программные и программно-аппаратные комплексы СЗИ в ААМО СК.

4.2.8. Осуществляют поддержку функционирования информационных систем и принимают необходимые меры по конфигурированию систем для обеспечения необходимого уровня информационной безопасности ААМО СК.

4.2.9. Контролируют работоспособность устройств бесперебойного питания критичных для ААМО СК информационных систем.

4.2.10. Обеспечивают физическую защиту помещений, в которых располагаются критичные для ААМО СК информационные системы.

4.2.11 Обеспечивают сопровождение устройств контроля доступа в помещения ААМО СК.

4.2.12. Обеспечивают защиту информационных ресурсов ААМО СК от случайного или намеренного уничтожения, искажения, разглашения.

4.2.13. Контролируют выполнение установленных правил и процедур обеспечения информационной безопасности в ААМО СК.

4.3. Руководители структурных подразделений ААМО СК

4.3.1. Обязаны соблюдать требования действующего законодательства Российской Федерации и внутренних документов ААМО СК в части обеспечения информационной безопасности.

4.3.2. Обеспечивают контроль за соблюдением норм и правил обеспечения информационной безопасности в своем структурном подразделении и информируют компетентное подразделение о любых подозрительных событиях или нарушениях действующих правил обеспечения информационной безопасности.

4.3.3. Обеспечивают соответствие действий работников подразделения Политике информационной безопасности, внутренним документам по информационной безопасности и любым другим распоряжениям руководства ААМО СК по вопросам информационной безопасности.

4.3.4. Организуют проведение необходимого инструктажа по вопросам выполнения правил информационной безопасности для всех работников своего структурного подразделения.

4.3.5. Контролируют выполнение работниками в своем структурном подразделении установленных правил в целях обеспечения физической безопасности компьютерного оборудования и носителей информации.

4.3.6. Своевременно информируют руководство о всех выявленных сбоях в работе информационных систем.

4.3.7. Контролируют доступ к необходимым информационными ресурсам работников своего структурного подразделения в соответствии с потребностью в пределах служебных обязанностей.

4.4 Работники ААМО СК

4.4.1. Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов, документов ААМО СК по вопросам информационной безопасности.

4.4.2. Соблюдают конфиденциальность данных, доступ к которым был ими получен.

4.4.3. Обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе.

4.4.4. Не допускают самовольного подключения и использования в автоматизированной информационной системе личного компьютерного и цифрового оборудования, а также носителей информации.

4.4.5. Не допускают самовольную установку программного обеспечения на компьютеры, входящие в состав информационной системы.

4.4.6. Своевременно информируют руководителя своего структурного подразделения о всех случаях нарушения информационной безопасности и о всех выявленных сбоях в работе программных и программно-аппаратных средств.

4.4.7. Проявляют осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.

4.5. Сторонние физические и юридические лица

Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов ААМО СК и других распоряжений руководства по вопросам информационной безопасности при исполнении договорных обязательств.

5. Основные требования по защите информации ограниченного доступа

5.1. Общие требования

5.1.1. В ААМО СК необходимо соблюдать режим безопасности, предусматривающий реализацию организационно-технических мероприятий, возложенных на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с требованиями законодательства Российской Федерации.

5.1.2. В ААМО СК осуществляется обработка и хранение информации ограниченного доступа (доступ к которой ограничен федеральными законами и служебной необходимостью).

5.1.3. В ААМО СК должен быть разработан перечень информации ограниченного доступа.

5.1.4. ААМО СК, как обладатель информации ограниченного доступа, при осуществлении своих прав обязано:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

5.1.5. ААМО СК, как обладатель информации ограниченного доступа, если иное не предусмотрено федеральными законами, вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам на установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий, если эти действия не противоречат федеральным законам и другим нормативно-правовым актам регуляторов.

5.1.6. ААМО СК, являясь обладателем информации ограниченного доступа, в случаях, установленных законодательством РФ, обязано обеспечить:

- предотвращение НСД к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов НСД к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность регламентированного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

5.1.7 Защита информации ограниченного доступа представляет собой принятие правовых, организационных и технических мер, направленных на:
- соблюдение конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);
- обеспечение целостности информации (исключение неправомерного уничтожения или модифицирования информации);
- реализацию права на доступ к информации (исключение неправомерного блокирования информации).

5.2. Организация защиты конфиденциальной информации

5.2.1. При организации в ААМО СК защиты информации ограниченного доступа, необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации.

5.2.2. В ААМО СК необходимо соблюдать режим защиты конфиденциальной информации (далее — КИ):
- ограничение доступа к КИ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию КИ, с работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- использование материальных носителей, содержащих КИ в соответствии с утвержденным порядком, исключающим несанкционированный доступ к ним.

5.2.3. Для обеспечения защиты КИ, ААМО СК вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству РФ, меры.

5.2.4. В целях охраны КИ, в рамках трудовых отношений необходимо:

- ознакомить под расписку работников, доступ которых к КИ, необходим для выполнения ими своих служебных обязанностей, с перечнем КИ, и установленным в ААМО СК режимом защиты КИ, а также мерами ответственности за его нарушение;
- создать работникам необходимые условия для соблюдения установленного режима защиты КИ.

5.2.5. Работники ААМО СК, обязаны выполнять установленный в ААМО СК режим защиты КИ, не разглашать информацию, составляющую КИ, и не использовать эту информацию в личных целях.

5.3. Особенности защиты персональных данных

5.3.1. При организации в ААМО СК защиты персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», который регулирует отношения, связанные с обработкой и хранением персональных данных граждан и определяет требования по защите их конфиденциальности.

5.3.2. ААМО СК самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом №152-ФЗ или другими федеральными законами.

5.3.3. Перечень мер, выполнение которых обеспечивает ААМО СК в качестве оператора персональных данных, должен включать:

- назначение в ААМО СК ответственного за организацию обработки персональных данных;
- издание ААМО СК документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона №152-ФЗ;
- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона №152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом №152-ФЗ;
- ознакомление работников ААМО СК, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ААМО СК в отношении обработки персональных данных, локальными

актами по вопросам обработки персональных данных и обучение, при необходимости, указанных работников.

5.3.4. ААМО СК при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.3.5. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз и нарушителей безопасности персональных данных при их обработке в информационных системах персональных данных (далее — ИСПДн);
- проведением классификации ИСПДн в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», и определение класса защищенности для ИСПДн;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает выбранные уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;
- учетом машинных носителей персональных данных;
- обнаружением фактов НСД к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
- установлением правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн.

5.3.6. Работники ААМО СК должны быть ознакомлены под роспись с документами ААМО СК, устанавливающими порядок обработки персональных данных, а также об их правах, обязанностях и ответственности.

6. Основные требования к процессам обеспечения информационной безопасности

6.1. Общие положения

Методическое руководство, разработку конкретных требований по защите информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации осуществляют компетентные подразделения ААМО СК.

6.2. Физическая безопасность и безопасность на рабочем месте

6.2.1. Система защиты зданий и помещений ААМО СК, объектов и технических средств информационных систем ААМО СК обеспечивает выполнение следующих функций:

- разграничение доступа работников в помещения ААМО СК в соответствии с их полномочиями и функциональными обязанностями;
- регистрацию фактов входа работников в помещения с повышенными требованиями к режиму их посещения (серверные помещения, архивы и т.д.);
- регистрацию фактов входа посторонних лиц в здания ААМО СК;
- предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;
- разрешительный режим вноса/выноса (ввоза/вывоза) компьютерного оборудования, средств записи и хранения информации.

6.2.2. Определяется перечень технических средств, находящихся в специальных контролируемых зонах.

6.2.3. К техническим средствам, которые выделяются в специальные контролируемые зоны необходимо отнести следующие группы ресурсов:

- основные информационные серверы и средства вычислительной техники, на которых осуществляется обработка и хранение информации ограниченного распространения;
- сетевое оборудование и серверы, обеспечивающие работу критических систем;
- файловые серверы, на которых хранятся данные, в том числе резервные;
- критичные для деятельности ААМО СК системы и коммуникационное оборудование, обеспечивающее внешние коммуникации ААМО СК.

6.2.4. Контролируемые зоны защищаются соответствующими системами контроля и управления доступом, обеспечивая доступ только авторизованному персоналу.

6.2.5. Доступ в контролируемые зоны сторонних лиц или представителей других организаций возможен только в сопровождении уполномоченного работника ААМО СК.

6.2.6. Размещение и эксплуатация рабочих станций, серверов и сетевого оборудования ААМО СК осуществляется в помещениях, оборудованных замками, средствами сигнализации и (при необходимости) постоянно находящихся под охраной или наблюдением.

6.2.7. Размещение технических средств вывода и отображения информации в помещениях ААМО СК производится с учетом исключения возможности визуального просмотра информации посторонними лицами и персоналом, не допущенным к работе с данной информацией.

6.2.8. Работники ААМО СК на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей с защищаемой информацией.

6.2.9. Технические средства и оборудование должны размещаться и храниться таким образом, чтобы сократить возможный риск его повреждения и угрозы несанкционированного доступа.

6.2.10. Помещения ААМО СК должны быть оборудованы детекторами огня и дыма, огнетушителями, системами кондиционирования воздуха, средствами охранно-пожарной сигнализации.

6.2.11. Основное техническое оборудование ААМО СК должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам ААМО СК в соответствии с рекомендациями производителя.

6.2.12. Пользователи портативных технических средств не должны оставлять техническое оборудование и носители информации без присмотра.

6.2.13. Портативные технические средства не должны оставаться за пределами контролируемой зоны ААМО СК дольше, чем того требует служебная необходимость, если иное не определено руководством ААМО СК.

6.3. Безопасность при работе с носителями информации

6.3.1. В ААМО СК должны соблюдаться меры по безопасной работе с электронными носителями информации с целью контроля их использования, для предотвращения несанкционированного копирования и разглашения защищаемой информации, внесения изменений или уничтожения указанной информации, а также внесения изменений в работу информационных систем.

6.3.2. Работники ААМО СК должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в ААМО СК в иных целях строго запрещено.

6.3.3. Электронные носители информации в ААМО СК должны быть учтены путем присвоения каждому носителю инвентаризационного номера и назначения владельца.

6.3.4. Электронные носители информации должны храниться в

помещениях, исключающих получение к ним НСД, при этом должен быть обеспечен контроль доступа к носителям.

6.3.5. Для контроля процессов использования и хранения электронных носителей информации должен быть разработан порядок плановой инвентаризации носителей.

6.3.6. В случае кражи или потери электронных носителей информации, а также иных инцидентов, которые могут привести к разглашению защищаемой информации, должны проводиться мероприятия по расследованию указанных инцидентов.

6.3.7. При снятии электронного носителя информации с эксплуатации, все данные, хранящиеся на нем, должны быть гарантированно стерты.

6.3.8. При утилизации электронных носителей информации должна быть обеспечена невозможность восстановления записанной на них информации.

6.3.9. Факт уничтожения информации и утилизации носителя информации фиксируется в соответствии с порядком, установленным в ААМО СК.

6.4. Техническое обслуживание оборудования

6.4.1.Технические средства всех систем ААМО СК должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

6.4.2. Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированным персоналом.

6.4.3. Техническое обслуживание оборудования и систем сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации.

6.5. Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности ААМО СК при взаимодействии с третьими лицами должны выполняться следующие мероприятия:

- заключение соглашения о неразглашении конфиденциальной информации;
- контроль за действиями третьих лиц;
- в договорах с третьими лицами предусматривать право ААМО СК на проведение аудита обеспечения безопасности той информации, которая передается третьим лицам.

6.6. Управление жизненным циклом информационных систем

6.6.1. Мероприятия по управлению жизненным циклом автоматизированных информационных систем должны быть направлены на обеспечение информационной безопасности при вводе в действие, эксплуатации, сопровождении и модернизации, вывода из эксплуатации информационных систем, автоматизирующих деятельность ААМО СК.

6.6.2. Основой при выборе или разработке информационных систем должны являться технические задания, содержащие требования

информационной безопасности для информационных систем.

6.6.3. Любое планируемое к внедрению изменение информационной системы предварительно должно быть протестировано на совместимость и отсутствие нарушений работоспособности системных компонентов.

6.6.4. Работы по модернизации автоматизированной информационной системы, в том числе по установке программного обеспечения и обновлений, должны проводиться в нерабочее время или время наименьшей рабочей нагрузки.

6.6.5. При выводе из эксплуатации автоматизированных информационных систем должно обеспечиваться гарантированное удаление обрабатываемой и хранимой в них информации с использованием специализированных программных средств или путем физического уничтожения носителей информации.

6.6.6 Все процедуры обеспечения информационной безопасности, установленные в ААМО СК в отношении информационных систем, должны выполняться и контролироваться ответственными за информационную безопасность лицами.

6.7. Антивирусная защита

6.7.1. В целях предупреждения, обнаружения и устранения вредоносных программ в ААМО СК на постоянной основе должны использоваться средства антивирусной защиты.

6.7.2. Обязательному антивирусному контролю должна подлежать любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация, хранимая на подключаемых съемных носителях, при непосредственном обращении к ней.

6.7.3. При установке программного обеспечения на серверы информационных систем ААМО СК или их обновлении должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

6.7.4. Сигнатурные базы вредоносного программного обеспечения и антивирусные средства защиты должны регулярно обновляться.

6.7.5. Пользователи информационных систем ААМО СК не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

6.7.6. В ААМО СК необходимо определить процедуру для обработки и восстановления инфицированных данных и отслеживание источника заражения.

6.8.Контроль доступа к информационным системам

6.8.1. Все работники ААМО СК, допущенные к работе с информационными системами несут персональную ответственность за нарушения установленного порядка обработки информации, правил

хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы.

6.8.2. Уровень полномочий пользователя в информационной системе ААМО СК должен определяться в соответствии с его должностными обязанностями и производственной необходимостью.

6.8.3. Доступ пользователей к информационным системам ААМО СК должен контролироваться администратором системы.

6.8.4. Осуществление регулярного контроля выполнения политик и иных документов, касающихся регламентации допуска работников ААМО СК к информационным системам.

6.9. Идентификация и аутентификация

6.9.1. Доступ пользователей к информационным системам должен предоставляться только после успешного завершения процедур идентификации, аутентификации и авторизации.

6.9.2. Получение пользователем имени в системе и парольной информации, которые обеспечивают доступ пользователя к ресурсам системы, должно осуществляться по представлению руководителей структурных подразделений.

6.10. Безопасность пароля

6.10.1. С целью обеспечения защиты от несанкционированного доступа к информационным системам устанавливаются требования к выбору парольной информации, обеспечивающие достаточную степень стойкости паролей.

6.10.2. Для обеспечения конфиденциальности парольной информации пользователю запрещается хранить значения своих паролей на бумажном носителе в открытом виде и в свободном доступе.

6.10.3. Для обеспечения конфиденциальности парольной информации пользователям запрещается передавать значения своих паролей третьим лицам.

6.10.4. При вводе пароля пользователем для доступа к информационной системе ААМО СК должно исключаться отображение парольной информации на экране монитора в открытом виде.

6.10.5. Процедура смены парольной информации в информационных системах ААМО СК должна проводиться на регулярной основе.

6.11. Регистрация событий

Осуществление регистрации событий безопасности на всех компонентах информационных систем ААМО СК, в которых обрабатывается, хранится или по средствам которых передается защищаемая информация.

6.12. Использование СКЗИ

6.12.1. Решение об использовании СКЗИ в интересах защиты собственных информационных ресурсов принимается руководством ААМО СК в соответствии с законодательством Российской Федерации.

6.12.2. При эксплуатации СКЗИ и ключевой информации все сотрудники

ААМО СК должны выполнять требования нормативных правовых актов, издаваемых федеральным органом исполнительной власти в области обеспечения безопасности, документов ААМО СК по обеспечению безопасности использования СКЗИ, а также эксплуатационной документации производителя СКЗИ.

6.13. Безопасность информационной сети

6.13.1. Установление надлежащего контроля в отношении локальной вычислительной сети и всех внешних информационных коммуникаций ААМО СК для обеспечения защиты данных и защиты информационных систем ААМО СК от НСД.

6.13.2. Должны быть определены цели использования сети Интернет и требования к процедуре использования ресурсов сети Интернет. Использование сети Интернет работников в личных целях должно быть строго запрещено.

6.13.3. Доступ к информационным сервисам сети Интернет предоставляется работникам ААМО СК только в случае производственной необходимости.

6.13.4. Подключение к сети Интернет должно осуществляться только при организации защиты соединения путем установки МЭ и специальных программных средств защиты.

6.13.5. Разрешительные политики доступа в Интернет должны технически реализовываться специализированным программным обеспечением.

6.13.6. Контроль использования работниками ресурсов сети Интернет должен осуществляться уполномоченными работниками на постоянной основе.

6.14. Использование корпоративной электронной почты

6.14.1. Система корпоративной электронной почты должна использоваться в ААМО СК с целью организации обмена электронными сообщениями между работниками, а также между работниками ААМО СК и внешними абонентами.

6.14.2. В ААМО СК должны быть четко определены требования к использованию системы корпоративной электронной почты.

6.14.3. Предоставление и прекращение доступа к ресурсам корпоративной электронной почты должно осуществляться только на основе оформленной заявки.

6.14.4. В ААМО СК должно быть установлено специальное программное обеспечение, осуществляющее контроль всех входящих сообщений на наличие вредоносного программного обеспечения.

6.14.5. В ААМО СК должны быть предусмотрены механизмы архивирования и резервного копирования корпоративной электронной почты в автоматическом режиме.

6.15. Резервное копирование и восстановление данных

6.15.1. Осуществление резервного копирования для:

- файловых серверов и серверов приложений, критичных для деятельности ААМО СК;
- операционных систем файловых серверов и прикладных программ;
- приложений, критичных для деятельности ААМО СК;
- рабочих данных.

6.15.2. Частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и допустимое время восстановления.

6.15.3. Резервное копирование и восстановление ресурсов информационных систем ААМО СК должны проводить уполномоченные работники ААМО СК.

6.15.4. Резервное копирование должно осуществляться в автоматическом режиме с применением специализированного программно-аппаратного комплекса.

7. Основные требования к процессам управления информационной безопасностью

7.1. Управление рисками

7.1.1. Выбор требований по информационной безопасности и защитных механизмов, применяемых в системе информационной безопасности, должен основываться на проведении анализа рисков нарушения основных свойств безопасности для наиболее критичных информационных ресурсов ААМО СК.

7.1.2. Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения свойств целостности, конфиденциальности и доступности для ресурсов информационной системы ААМО СК.

7.1.3. Результатом проведения анализа рисков должен быть комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность ААМО СК при реализации той или иной угрозы и обеспечивающих достаточный уровень защищенности информационных систем ААМО СК.

7.2. Управление инцидентами информационной безопасности

7.2.1. Для обеспечения эффективного разрешения инцидентов информационной безопасности в ААМО СК, минимизации потерь и уменьшения риска возникновения повторных инцидентов должно осуществляться эффективное управление инцидентами информационной безопасности.

7.2.2. Для управления инцидентами информационной безопасности должна быть создана система учета произошедших инцидентов, которая

представляет собой комплекс средств и мероприятий для сбора и консолидации информации об инцидентах.

7.2.3. В отношении каждого произошедшего инцидента должен выполняться его анализ, и разработка эффективных мер реагирования на данный инцидент.

7.3. Мониторинг текущего уровня информационной безопасности

7.3.1. Для обеспечения высокого уровня контроля в отношении системы обеспечения информационной безопасности в ААМО СК на постоянной основе должен проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности.

7.3.2. Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов.

7.3.3. При проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в ААМО СК, уполномоченные работники должны придерживаться следующих принципов:

- не нарушать функционирование текущей деятельности ААМО СК;
- действовать в соответствии с внутренними документами ААМО СК по информационной безопасности;
- не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;
- оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности.

7.3.4. Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к функционированию защитных мер, должна консолидироваться и храниться в местах, исключающих получение к ней несанкционированного доступа.

7.3.5. Мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться, по возможности, с использованием встроенных механизмов настройки и аудита событий в программных и программно-технических средствах, используемых в информационных системах ААМО СК.

7.4. Аудит системы обеспечения информационной безопасности

7.4.1. В целях оценки текущего уровня информационной безопасности уполномоченные работники ААМО СК на регулярной основе должны проводить аудит информационной безопасности.

7.4.2. Внутренние аудиты или самооценки должны выполняться, по возможности, работниками ААМО СК.

7.4.3. Результатом выполнения аудитов по информационной безопасности должны стать отчеты о выполненном аудите информационной

безопасности, которые разрабатываются специалистами ААМО СК.

7.4.4. По результатам аудита уполномоченные работники и ответственные подразделения ААМО СК должны определить действия, необходимые для устранения обнаруженных несоответствий в процессе аудита и вызвавших их причин.

7.5. Управление персоналом

7.5.1. Организация такого процесса управления персоналом, который обеспечит доверительное отношение к работникам, а также организует комплексное противодействие угрозам информационной безопасности, исходящим от персонала ААМО СК.

7.5.2. Выполнение обязательных проверок при приеме новых работников на работу с точки зрения достоверности сообщаемых ими данных и с позиции оценки их профессиональных навыков.

7.5.3. Организация работы в направлении повышения осведомленности и обучения в области информационной безопасности.

7.5.4. Повышение осведомленности работников ААМО СК:

- по существующим в ААМО СК политикам информационной безопасности;
- по применяемым в ААМО СК защитным мерам;
- по правильному использованию защитных мер в соответствии с внутренними документами ААМО СК.

8. Заключение

8.1. Настоящая Политика является внутренним документом администрации Александровского муниципального округа, общедоступной и подлежит размещению на официальном сайте администрации.

8.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики. Контроль исполнения требований настоящей Политики осуществляется ответственным лицом за обеспечение безопасности персональных данных администрации Александровского муниципального округа.

8.3. Ответственность должностных лиц администрации, имеющих доступ к конфиденциальной информации, за невыполнение требований норм, регулирующих обработку и защиту информации, определяется в соответствии с законодательством Российской Федерации и внутренними документами администрации Александровского муниципального округа.

УТВЕРЖДЕНА
распоряжением администрации
Александровского муниципального
округа Ставропольского края
от 25 июня 2024г. № 169-р

Политика организации парольной защиты в администрации Александровского муниципального округа Ставропольского края

1. Термины и определения

Термины, определения и сокращения, применяемые в настоящем документе, используются в соответствие с документом Политика информационной безопасности администрации Александровского муниципального округа Ставропольского края «Обозначения и сокращения».

2. Основные положения

Настоящий документ «Политика организации парольной защиты в администрации Александровского муниципального округа Ставропольского края» (далее — Политика) регламентирует организационно-техническое обеспечение процессов создания, использования, смены, прекращения действия паролей учетных записей пользователей и администраторов, а также контроля действий при работе с паролями.

2.1. Реализация требований Политики производится в установленном порядке администратором информационной безопасности.

2.2. Политика подлежит пересмотру с периодичностью 1 раз в год для приведения системы защиты в соответствие реальным условиям. Также может проводиться внеплановый пересмотр при изменении перечня решаемых задач, конфигурации технических и программных средств, а также при изменении требований законодательства в области информационной безопасности.

3. Общие требования

3.1. Каждому субъекту (пользователю), присваиваются персональные идентификаторы для доступа к техническим средствам и информационным ресурсам (логин/пароль). Логин (имя) формируется путём написания на латинице фамилии пользователя с приставкой первой буквы или нескольких букв имени, в зависимости имеющихся схожих имен и фамилий, разделенных точкой. Например, *Иванов Иван Иванович*, будет иметь персональный идентификатор: *i.ivanov.*

3.2. При первом доступе пользователь обязан изменить выданный ему пароль, руководствуясь требованиями к сложности пароля, указанные в п.4 настоящей Политики.

3.3. Недопустимо хранение паролей в открытом виде на любых видах носителей информации.

3.4. При использовании аппаратно-технических средств аутентификации (iButton. USB-Token, смарт-карта) допускается хранение таких средств только в сейфах, либо в запираемых шкафах (ящиках).

4. Правила формирования пароля

Формирование паролей производится централизованно Администратором ИБ, либо выбираются пользователями с учетом следующих требований:

- длина пароля не менее 6-ти символов;
- длина пароля для административных учетных записей не менее 10-ти символов;
- алфавит пароля не менее 70 символов;
- пароль должен содержать буквы в верхнем нижнем регистрах, десятичные цифры и/или специальные символы (@, #, $, &, *, % л т. п.);
- пароль не должен содержать имя учетной записи пользователя или какую-либо его часть или включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения, наименования АРМ и т. д.) а также общепринятые сокращения (LAN, USER и т. п.).

5. Правила ввода пароля

Ввод пароля осуществляется согласно следующих прав:

- ввод пароля должен осуществятся непосредственно пользователем (владельцем пароля);
- при вводе пароля символы не должны отображаться на экране в явном виде;
- в целях предотвращения неверного ввода пароля пользователь должен убедится в правильности языка ввода (раскладки клавиатуры), а также исключить возможность просмотра, набираемого на клавиатуре пароля посторонними лицами или техническими средствами;
- количество ввода неправильного пароля до блоков 5 и до 5 попыток;
- при плановой/внеплановой смене пароля необходимо произвести ввод старого пароля затем ввод нового пароля.

6. Порядок смены пароля

6.1. Плановая смена паролей производится не реже одного раза в 90 дней для пользовательских учетных записей и не реже одного раза в 45 дней для административных учетных записей. При смене пароля новая парольная комбинация отличатся от последних 4-х используемых комбинаций.

6.2. Внеплановая смена личного пароля пользователя в случае прекращения его полномочий (увольнение, переход на другую работу и т.д) должна производится администратором ИБ немедленно, после окончания последнего сеанса работы данного пользователя. Внеплановая полная смена паролей всех пользователей должна производиться в случае увольнения администратора или администратора безопасности.

7. Ответственность при организации парольной защиты

7.1. Лица, имеющие доступ к КСПД обязаны четко знать и строго выполнять требования настоящей Политики.

7.2. Пользователь обязан помнить свой логин и пароль.

7.3. Пользователю запрещается разглашать или передавать свой пароль сторонним лицам.

7.4. Пользователь обязан своевременно сообщать администратору ИБ об утере, компрометации, несанкционированных попытках изменения и несанкционированном изменении сроков действия пароля.

7.5. Администратор информационной безопасности:

- несёт ответственность за корректное и непрерывное функционирование подсистемы парольной защиты;
- несёт ответственность за настройку конфигурации подсистемы парольной защиты.

7.6. Администратор информационной безопасности и системный администратор принимают участие в мероприятиях по реагированию н инциденты информационной безопасности, связанные с нарушением требований организации парольной защиты.

УТВЕРЖДЕНА
распоряжением администрации
Александровского муниципального
округа Ставропольского края
от 25 июня 2024 г. № 169-р

Политика резервного копирования критически важной информации в администрации Александровского муниципального округа Ставропольского края

1. Список терминов и определений

- ИТ-инфраструктура – совокупность аппаратного и программного обеспечения администрации Александровского муниципального округа, а также правил и методов их настройки, обеспечивающих технологию совместной работы сотрудников.
- Администратор файлового сервера – сотрудник отдела информационных технологий и защиты информации администрации Александровского муниципального округа, осуществляющий управление файловым сервером.
- Сотрудник технической поддержки – сотрудник отдела информационных технологий и защиты информации администрации Александровского муниципального округа.
- Заявка – запрос сотрудника в отдел информационных технологий и защиты информации на решение какой-либо технической проблемы. Заявка содержит описание проблемы.
- Ресурс файлового сервера (далее Ресурс) – это каталог на файловом сервере, предназначенный для хранения файлов в целях, указанных в заявке на создание ресурса.
- Ответственный за информационные ресурсы – начальник отдела, принимающий решения (подготавливает заявку) о создании новых Ресурсов.
- «Helpdesk» – система, обеспечивающая прием и обработку заявок сотрудников.
- ИСМ – информационная система мониторинга ИТ-инфраструктуры.
- ЭЦП – электронная цифровая подпись.
- GPG – программное обеспечение для шифрования и ЭЦП данных.
- Согласование Заявки – направление электронного сообщения в «Helpdesk».
- Ответственный за ресурс – сотрудник указанный ответственным в заявке на создание ресурса.

2. Общие положения

Настоящая «Политика проведения резервного копирования (восстановления) программ и данных, хранящихся на серверах ИТ-инфраструктуры» (далее — Политика) разработана с целью:

- определения порядка резервирования данных для последующего восстановления работоспособности автоматизированных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации.

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

- резервное копирование;
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных и приложений.

Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги на файловых серверах);
- групповая информация пользователей (общие каталоги отделов);
- информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);
- персональные профили пользователей сети;
- информация автоматизированных систем, в т.ч. баз данных;
- справочно-информационная информация систем общего использования («Консультант +» и т.п.);
- рабочие копии установочных компонент программного обеспечения рабочих станций;
- регистрационная информация системы информационной безопасности автоматизированных систем.

Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений в соответствии с «Перечнем сведений составляющих коммерческую тайну» Определяется внутренним регламентом, по необходимости.

3. Порядок резервного копирования

Резервное копирование автоматизированных систем производится на основании следующих данных:

- состав и объем копируемых данных, периодичность проведения резервного копирования (из Перечня резервируемых данных - по Приложению 1 данного документа);
- максимальный срок хранения резервных копий - 1 месяц;
- хранение 3-х следующих архивов;
- архив на 1-е число текущего месяца;
- архив среда-четверг, либо пятница-суббота текущей недели;
- архив сделанный в текущую ночь. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне (Приложение 1), в установленные сроки и с заданной периодичностью. Методика проведения резервного копирования описана в методике резервного копирования.

О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается в отдел информационных технологий и защиты информации служебной запиской в течение рабочего дня после обнаружения указанного события. Ответственным является администратор резервного копирования (согласно Приложению 2).

4. Контроль результатов резервного копирования

Контроль результатов всех процедур резервного копирования осуществляется ответственными должностными лицами, указанными в Приложении 2, в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки лицо, ответственное за контроль результатов, приостанавливает действия и выводит копируемую систему из сети для выяснения обстоятельств.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

5. Ротация носителей резервной копии

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также перемещение их, осуществляются администратором резервного копирования по запросу и в присутствии ответственного сотрудника (согласно Приложению 2).

В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна стираться с использованием программного обеспечения PGP.

6. Восстановление информации из резервных копий

В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации, согласованной с

Ответственным за информационные ресурсы.

Процедура восстановления информации из резервной копии осуществляется в соответствии с методикой восстановления информации (Методика восстановления данных).

После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

7. Методика резервного копирования

Для организации системы резервного копирования используется программное обеспечение (далее - ПО) фирмы Synology. С целью оптимизации расходов на развертывание системы резервного копирования, запись резервной копии осуществляется на жесткий диск.

С помощью указанного ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, осуществляются операции по загрузке и выгрузке носителей информации, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.

Настройка всех трех серверов одинакова. Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в ночное время. Существуют 2 набора резервных копий:

1. Месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – месяц. Хранится на сервере резервного копирования.
2. Недельная копия. Записывается в ночь на среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы. Хранится на сервере.

Различаются три принципиально разных источника информации, подлежащей резервированию:

1. Информация, хранимая на серверах (образ диска).
2. Конфигурационные файлы активного сетевого оборудования.
3. Базы данных Прикладной информационной системы. Для резервирования информации, хранимой в DELO Server, общие папки, (см. пункт 1-й, выше), используется ПО Active Backup for Business с установленным агентом, посредством которого формируются задания на проведение резервного копирования информации. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

Для резервирования конфигурационных файлов активного сетевого оборудования (см. пункт 2-й, выше), используется прямой SSH доступ к устройству с последующем резервированием конфигурации на TFTP сервер.

При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

Для резервирования информации, хранимой в базах данных Прикладной информационной системы (см. пункт 1-й, выше), в качестве промежуточного звена автоматизации используются средства конфигурирования Прикладной информационной системы и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных Прикладной информационной системы. Посредством ПО Active Backup for Business формируются задания на проведение резервного копирования этого каталога. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

8. Методика восстановления данных

Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы или ее компонент, выполняется на основании заявки, оформленной через систему HelpDesk, либо личным обращением в отдел информационных технологий и защиты информации.

Восстановление информации, относящейся к базам Прикладной информационной системы, происходит при тесном взаимодействии с администратором Прикладной информационной системы.

УТВЕРЖДЕНА
распоряжением администрации
Александровского муниципального
округа Ставропольского края
от 25 июня 2024 г. № 169-р

Политика организации антивирусной защиты в администрации Александровского муниципального округа Ставропольского края

1. Термины и определения

Термины, определения и сокращения, применяемые в настоящем документе, используются в соответствие с документом Политика информационной безопасности администрации Александровского муниципального округа Ставропольского края «Обозначения и сокращения».

2. Основные положения

2.1. Настоящий документ «Политика антивирусной защиты» (далее - Политика) - определяет систему мер, направленных на защиту инфраструктуры информационных систем КСПД ТО от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (троянских программ, логических бомб и т.п.), а также устанавливает единые требования к организации системы антивирусной защиты информационных систем и всех типов автоматизированных рабочих мест, требования к конфигурации применяемых программных средств и процедуры их эксплуатации.

2.2. Реализация требований Политики производится лицами, назначенными в установленном порядке администраторами информационной безопасности администрации либо подразделением (или организацией), привлекаемым для выполнения данных функций.

2.3. Политика подлежит регулярному пересмотру с периодичностью 1 раз в год для приведения системы защиты в соответствие реальным условиям. Также может проводиться внеплановый пересмотр при изменении перечня решаемых задач, конфигурации технических и программных средств.

2.4. Настоящая Политика:

- определяет единые требования по организации антивирусной защиты во всех информационных системах и отдельных АРМ, входящих в состав или подключенных к КСПД ТО;

- определяет необходимые и достаточные меры антивирусной защиты для поддержания бесперебойной и безопасной работы пользователей КСПД ТО;

- определяет распределение административных ролей сотрудников Участников процессов ИБ при организации антивирусной защиты объектов КСПД ТО;

- определяет обязанности пользователей КСПД ТО и администраторов информационной безопасности администрации в рамках организации антивирусной защиты;

- применяется ко всем информационным системам и отдельным АРМ, подключенным к КСПД ТО;

- обязательна к исполнению всеми партнерами, исполнителями по заключенным с Участниками процессов ИБ контрактам/ договорам и другими лицами и организациями, постоянно использующим или имеющим периодическое подключение к сетевым или информационным ресурсам КСПД ТО.

ПРИЛОЖЕНИЕ 1

к распоряжению администрации
Александровского муниципального
округа Ставропольского края
от 25 июня 2024 г. № 169-р

Перечень резервируемой информации

№ п/п	Адрес хранения информации	Примечание
1	\\aamr.local\SystemState	Состояние контроллера домена
2	\\aamr.local\c$	Системный диск контроллера домена
3	\\ Shared\Shara_AAMR	Файл-сервер - персональные данные пользователей и данные отделов
4	\\sr-delo\c$	Системный диск с БД и настройками системы межведомственного электронного документооборота ДЕЛО
5	\\hyper-V\c$	Системный диск гипервизора

ПРИЛОЖЕНИЕ 2

к распоряжению администрации
Александровского муниципального
округа Ставропольского края
от 25 июня 2024 г. № 169-р

Перечень лиц ответственных за резервное копирование

№ п/п	Выполняемая роль	Ответственный сотрудник
1	Первоначальная настройка системы резервного копирования (создание медиа-сетов, расписаний, selection lists, оповещений). Запуск в промышленную эксплуатацию системы резервного копирования.	Начальник отдела ИТ и ЗИ ААМО СК Главный специалист отдела ИТ и ЗИТ ААМО СК
2	Внесение существенных изменений в настройку системы резервного копирования.	Начальник отдела ИТ и ЗИ ААМО СК Главный специалист отдела ИТ и ЗИТ ААМО СК
3	Анализ логов резервного копирования, отслеживание необходимости изменений настроек резервного копирования, обеспечение ротирования носителей.	Начальник отдела ИТ и ЗИ ААМО СК

№ п/п	Выполняемая роль	Ответственный сотрудник
4	Ротирование носителей, проверка корректности резервной копии, обеспечения хранения резервной копии вне офиса на случай катастрофы.	Главный специалист отдела ИТ и ЗИТ ААМО СК

УТВЕРЖДЕНА
распоряжением администрации
Александровского муниципального
округа Ставропольского края
от 25 июня 2024 г. № 169-р

Политика организации антивирусной защиты в администрации Александровского муниципального округа Ставропольского края

1. Термины и определения

Термины, определения и сокращения, применяемые в настоящем документе, используются в соответствие с документом Политика информационной безопасности администрации Александровского муниципального округа Ставропольского края «Обозначения и сокращения».

2. Основные положения

2.1. Настоящий документ «Политика антивирусной защиты» (далее - Политика) - определяет систему мер, направленных на защиту инфраструктуры информационных систем КСПД ТО от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (троянских программ, логических бомб и т.п.), а также устанавливает единые требования к организации системы антивирусной защиты информационных систем и всех типов автоматизированных рабочих мест, требования к конфигурации применяемых программных средств и процедуры их эксплуатации.

2.2. Реализация требований Политики производится лицами, назначенными в установленном порядке администраторами информационной безопасности администрации либо подразделением (или организацией), привлекаемым для выполнения данных функций.

2.3. Политика подлежит регулярному пересмотру с периодичностью 1 раз в год для приведения системы защиты в соответствие реальным условиям. Также может проводиться внеплановый пересмотр при изменении перечня решаемых задач, конфигурации технических и программных средств.

2.4. Настоящая Политика:

- определяет единые требования по организации антивирусной защиты во всех информационных системах и отдельных АРМ, входящих в состав или подключенных к КСПД ТО;
- определяет необходимые и достаточные меры антивирусной защиты для поддержания бесперебойной и безопасной работы пользователей КСПД ТО;
- определяет распределение административных ролей сотрудников Участников процессов ИБ при организации антивирусной защиты объектов КСПД ТО;
- определяет обязанности пользователей КСПД ТО и администраторов информационной безопасности администрации в рамках организации антивирусной защиты;

- применяется ко всем информационным системам и отдельным АРМ, подключенным к КСПД ТО;

- обязательна к исполнению всеми партнерами, исполнителями по заключенным с Участниками процессов ИБ контрактам/ договорам и другими лицами и организациями, постоянно использующим или имеющим периодическое подключение к сетевым или информационным ресурсам КСПД ТО.