Р А С П О Р Я Ж Е Н И Е
администрации Апанасенковского муниципального округа
Ставропольского края

с.Дивное

01 декабря 2021 г. № 358-р

Об утверждении внутренних нормативных-правовых актов по защите персональных данных отдела по информатизации и информационной безопасности администрации Апанасенковского муниципального округа Ставропольского края

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

1. Утвердить следующий перечень нормативных-правовых актов:

1.1. Инструкцию администратора информационных систем администрации Апанасенковского муниципального округа Ставропольского края.

1.2. Инструкцию администратора информационной безопасности администрации Апанасенковского муниципального округа Ставропольского края.

1.3. Инструкцию ответственного за обеспечение безопасности и обработку персональных данных в администрации Апанасенковского муниципального округа Ставропольского края.

1.4. Инструкцию пользователя информационных систем администрации Апанасенковского муниципального округа Ставропольского края.

1.5. Инструкцию по организации антивирусной защиты в информационных системах администрации Апанасенковского муниципального округа Ставропольского края.

1.6. Инструкцию по парольной защите в информационных системах администрации Апанасенковского муниципального округа Ставропольского края.

1.7. Инструкцию по допуску лиц в помещения администрации Апанасенковского муниципального округа Ставропольского края, в которых осуществляются обработка информации ограниченного доступа и эксплуатация криптографических средств защиты информации.

1.8. Инструкцию об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в администрации Апанасенковского муниципального округа Ставропольского края.

1.9. Функциональные обязанности ответственного пользователя средств криптографической защиты информации администрации Апанасенковского муниципального округа Ставропольского края.

1.10. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним правовыми актами администрации Апанасенковского муниципального округа Ставропольского края.

1.11. Правила рассмотрения запросов субъектов персональных данных.

1.12. Правила обработки персональных данных в администрации Апанасенковского муниципального округа Ставропольского края.

1.13. Порядок доступа сотрудников администрации Апанасенковского муниципального округа Ставропольского края в помещения, в которых ведется обработка персональных данных.

1.14. Регламент резервного копирования и восстановления данных.

2. Контроль за выполнением настоящего распоряжения возложить на первого заместителя главы администрации Апанасенковского муниципального округа Ставропольского края Андрегу А.И.

3. Настоящее распоряжение вступает в силу со дня его подписания.

Исполняющий обязанности
главы Апанасенковского
муниципального округа
Ставропольского края А.И.Андрега

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ИНСТРУКЦИЯ

администратора информационных систем администрации Апанасенковского муниципального округа Ставропольского края

Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационных систем (далее – Администратор ИС) администрации Апанасенковского муниципального округа Ставропольского края.

1.2. Администратор ИС назначается распоряжением администрации Апанасенковского муниципального округа Ставропольского края.

1.3. Функционально Администратор ИС подчиняется своему непосредственному руководителю и (по направлению – обеспечения безопасности информации) ответственному за обеспечение безопасности и обработку персональных данных администрации Апанасенковского муниципального округа Ставропольского края.

1.4. Администратор ИС руководствуется положениями федеральных законов и нормативных актов органов государственной власти, ведомственных организационно-распорядительных актов, нормативных актов администрации Апанасенковского муниципального округа Ставропольского края, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

1.5. Внесение изменений в настоящую Инструкцию осуществляется на периодической и внеплановой основе:

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

внеплановое внесение изменений в настоящую Инструкцию может производиться в случае изменения действующего законодательства и иных нормативных актов в области обеспечения безопасности информации.

1.6. Ответственным за внесение изменений в настоящую Инструкцию является руководитель ответственного за обеспечение информационной безопасности подразделения.

1.7. Контроль за выполнением требований настоящей инструкции осуществляет руководитель ответственного за обеспечение информационной безопасности подразделения.

Обязанности администратора информационных систем

Администратор ИС обязан:

обеспечивать работоспособность средств вычислительной техники (СВТ) информационных систем (далее – ИС), проводить организационно-технические мероприятия по их обслуживанию;

осуществлять настройку компонентов ИС, включая прикладное программное обеспечение и специальное программное обеспечение;

рассматривать целесообразность применения новых технологий для повышения

эффективности функционирования ИС;

подготавливать обоснования и спецификации для закупки, заказывать новые элементы в ИС и расходные материалы;

поддерживать резерв расходных материалов;

изучать рынок программных средств и предоставлять рекомендации по приобретению и внедрению системного и прикладного программного обеспечения;

выполнять своевременное обновление ПО элементов ИС и системы защиты информации (в пределах своей компетенции) по мере появления новых версий;

выполнять учет информационных ресурсов ИС (перечень информационных ресурсов разрабатывается и согласовывается совместно с руководителями структурных подразделений и администратором информационной безопасности (далее – АИБ) согласно «Регламенту резервного копирования и восстановления данных»;

выполнять резервное копирование данных ресурсов и, в случае необходимости – восстановление данных;

проводить инструктаж пользователей по внедряемым и используемым технологиям или прикладному программному обеспечению, если это требует от пользователей дополнительных навыков и знаний. Возможен инструктаж не только в устной форме, но и в письменной, либо в электронном виде, путем создания инструкций, файлов справок, описаний, руководств пользователя и прочее, с последующим обязательным доведением до каждого пользователя;

совместно с АИБ, обеспечивать контроль выполнения пользователями положений «Инструкции пользователя информационных систем администрации Апанасенковского муниципального округа Ставропольского края»;

предоставлять доступ к информационным ресурсам ИС пользователям по заявке пользователя, которому необходим доступ к ИС по согласованию с АИБ;

оказывать помощь АИБ при анализе работы элементов ИС/СЗИ с целью выявления и устранения неисправностей, а также оптимизации их функционирования;

оказывать помощь АИБ в осуществлении контроля действий пользователей ИС по работе с паролями;

предоставлять АИБ любую затребованную им информацию о настройках, конфигурации, составу и структуре ИС и механизмов защиты информации ИС;

выполнять действия по изменению элементов ИС, необходимость в которых определяется согласованным решением, определенным совместно с АИБ;

участвовать совместно с АИБ в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;

сопровождать сотрудников внешних организаций, которые выполняют работы по обслуживанию ИС;

в случае обнаружения попытки НСД в отношении защищаемых ресурсов со стороны пользователей или внешних нарушителей, оповещать АИБ;

осуществлять контроль технологических процессов обработки защищаемой информации;

планировать дальнейшее развитие структуры и функциональности ИС, а также вносить предложения о совершенствовании работы и повышении эффективности функционирования СВТ ИС и системы защиты информации.

Администратор ИС обязан в случае увольнения, все носители защищаемой информации ИС, которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы в администрации Апанасенковского муниципального округа Ставропольского края, передать АИБ.

Права администратора информационных систем

Администратор ИС имеет право:

анализировать работу любых элементов ИС для выявления и устранения неисправностей, а также для оптимизации ее функционирования;

отключать любые элементы ИС при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей после согласования и заблаговременного предупреждения пользователей ИС;

отключать элементы системы защиты информации (СЗИ) при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке после согласования с АИБ;

в установленном порядке изменять конфигурацию элементов ИС;

требовать от сотрудников администрации Апанасенковского муниципального округа Ставропольского края соблюдения правил работы в ИС, приведенных в «Инструкции пользователя информационных систем администрации Апанасенковского муниципального округа Ставропольского края»;

вносить свои предложения по совершенствованию функционирования ИС.

Ответственность администратора информационных систем

Администратор ИС несет ответственность:

за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими инструктивными документами Администратор ИС несет ответственность в соответствии с действующим трудовым законодательством Российской Федерации;

за правонарушения, совершенные в процессе своей деятельности Администратор ИС несет ответственность в пределах, определенных действующим административным, уголовным и гражданским законодательством РФ;

за разглашение сведений конфиденциального характера и другой защищаемой информации ИС, Администратор ИС несет ответственность в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

На Администратора ИС возлагается персональная ответственность за работоспособность и надлежащее функционирование всех элементов ИС.

Администратор ИС _____

ФИО

_____

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений в инструкции

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

№ п/п	Фамилия, инициалы сотрудника	Должность	Дата ознакомления	Расписка сотрудника в ознакомлении

_____

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ИНСТРУКЦИЯ

администратора информационной безопасности администрации Апанасенковского муниципального округа Ставропольского края

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности администрации Апанасенковского муниципального округа Ставропольского края (далее - Администрация).

1.2. Администратор информационной безопасности (далее – АИБ) назначается распоряжением администрации Апанасенковского муниципального округа Ставропольского края и функционально подчиняется своему непосредственному руководителю и (по направлению – обеспечения безопасности информации) ответственному за обеспечение безопасности и обработку персональных данных администрации Апанасенковского муниципального округа Ставропольского края.

1.3. АИБ руководствуется требованиями нормативных документов Российской Федерации, ведомственных организационно-распорядительных документов, нормативных актов администрации Апанасенковского муниципального округа Ставропольского края, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

1.4. АИБ в пределах своих функциональных обязанностей обеспечивает работоспособность информационных систем (далее – ИС) администрации Апанасенковского муниципального округа Ставропольского края, безопасность информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (далее – СВТ) в ИС.

1.5. Внесение изменений в настоящую Инструкцию осуществляется на периодической и внеплановой основе:

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

внеплановое внесение изменений в настоящую Инструкцию может производиться в случае изменения действующего законодательства и иных нормативных актов в области обеспечения безопасности информации.

1.6. Ответственным за внесение изменений в настоящую Инструкцию является руководитель ответственного за обеспечение информационной безопасности подразделения.

1.7. Контроль за выполнением требований настоящей инструкции осуществляет руководитель ответственного за обеспечение информационной безопасности подразделения.

2. Обязанности администратора информационной безопасности

АИБ обязан:

знать перечень установленных в подразделении СВТ и перечень задач, решаемых с их использованием;

осуществлять контроль изменений (в том числе и несанкционированных) аппаратного обеспечения автоматизированных рабочих мест и серверов;

устанавливать и настраивать средства защиты информации, а также выполнять другие возложенные на него работы в соответствии с распорядительными, инструктивными и методическими материалами в части, его касающейся;

рассматривать целесообразность применения новых технологий для повышения эффективности функционирования ИС;

выполнять своевременное обновление средств защиты информации по мере появления таких обновлений;

обеспечивать контроль за выполнением пользователями требований «Инструкции пользователя информационных систем администрации Апанасенковского муниципального округа Ставропольского края»;

осуществлять контроль работы пользователей ИС, выявление попыток НСД к защищаемым информационным ресурсам и техническим средствам ИС;

осуществлять настройку средств защиты информации, выполнять другие действия по изменению элементов ИС;

осуществлять учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в «Журнале учета носителей персональных данных в администрации Апанасенковского муниципального округа Ставропольского края». Учтенные носители информации выдавать пользователям под роспись в «Журнале учета выдачи электронных носителей персональных данных в администрации Апанасенковского муниципального округа Ставропольского края». Использование неучтенных носителей, равно как их выдача/прием без записи в соответствующем журнале – категорически запрещается;

осуществлять текущий и периодический контроль работы средств и систем защиты информации;

осуществлять текущий контроль технологического процесса обработки защищаемой информации;

периодически осуществлять тестирование всех функций системы защиты с помощью тестовых программ, имитирующих попытки НСД, а также при изменении программной среды и персонала ИС;

участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;

участвовать в проведении работ по восстановлению работоспособности средств и систем защиты информации;

проводить проверку регистраций событий безопасности;

проводить обучение персонала и пользователей вычислительной техники правилам работы с СВТ и средствами защиты информации по следующим вопросам:

обеспечение антивирусной защиты при работе в ИС;

порядок парольной защиты при работе в ИС;

участвовать в разработке нормативных и методических материалов, связанных с функционированием СВТ и применением средств защиты информации, выполнением мероприятий по обеспечению защиты информации;

рассматривать заявки пользователей на доступ к информационным ресурсам ИС;

осуществлять контроль технологических процессов обработки защищаемой информации;

разрабатывать предложения по изменению нормативных документов, регламентирующих процессы обработки и обеспечения безопасности информации;

осуществлять периодические проверки состояния защиты информации в ИС (в соответствии с «Планом мероприятий по обеспечению безопасности информации в инфор-

мационных системах администрации Апанасенковского муниципального округа Ставропольского края»);

вести учет всех средств защиты информации и технической документации к ним, используемых в администрации Апанасенковского муниципального округа Ставропольского края;

оказывать помощь в разработке администратору ИС и согласовывать перечень информационных ресурсов ИС, подлежащих резервному копированию, а также осуществлять контроль выполнения резервного копирования информационных ресурсов администратором ИС;

осуществлять надежное хранение резервных копий;

осуществлять контроль действий пользователей ИС с паролями.

В случае увольнения, АИБ обязан передать начальнику отдела, в штате которого он состоит все носители защищаемой информации ИС, которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы в ИС.

3. Права администратора информационной безопасности

АИБ имеет право:

отключать любые элементы СЗИ при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке;

в установленном порядке изменять конфигурацию элементов ИС и СЗИ;

требовать от сотрудников администрации Апанасенковского муниципального округа Ставропольского края соблюдения правил работы в ИС, приведенных в «Инструкции пользователя информационных систем администрации Апанасенковского муниципального округа Ставропольского края»;

требовать от пользователей безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований внутренних документов администрации Апанасенковского муниципального округа Ставропольского края, регламентирующих вопросы обеспечения безопасности и защиты информации;

обращаться к ответственному за обеспечение безопасности и обработку персональных данных с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации;

вносить свои предложения по совершенствованию функционирования ИС;

инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения ИБ в ИС.

4. Ответственность администратора информационной безопасности

АИБ несет ответственность:

за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими инструктивными документами в соответствии с действующим законодательством Российской Федерации, трудовым законодательством Российской Федерации, за полноту и качество проводимых им работ по обеспечению защиты информации;

за правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

за разглашение сведений конфиденциального характера и другой защищаемой информации ИС в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

На АИБ возлагается персональная ответственность за работоспособность средств защиты информации ИС.

Администратор ИБ _____ ФИО

_____

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

№ п/п	Фамилия, инициалы сотрудника	Должность	Дата ознакомления	Расписка сотрудника в ознакомлении

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ИНСТРУКЦИЯ

ответственного за обеспечение безопасности
и обработку персональных данных в администрации
Апанасенковского муниципального округа Ставропольского края

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность Ответственного за обеспечение безопасности и обработку персональных данных в администрации Апанасенковского муниципального округа Ставропольского края.

1.2. Ответственный за обеспечение безопасности и обработку персональных данных назначается распоряжением администрации Апанасенковского муниципального округа Ставропольского края и функционально подчиняется руководителю ответственного за обеспечение информационной безопасности подразделения.

1.3. Ответственный за обеспечение безопасности и обработку персональных данных руководствуется требованиями нормативных документов Российской Федерации, организационно-распорядительных документов, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

1.4. Ответственный за обеспечение безопасности и обработку персональных данных должен осуществлять организацию работы и общий контроль безопасности персональных данных в администрации Апанасенковского муниципального округа Ставропольского края и контролировать выполнения требований нормативных документов сотрудниками.

1.5. Внесение изменений в настоящую Инструкцию осуществляется на периодической и внеплановой основе:

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

внеплановое внесение изменений в настоящую Инструкцию может производиться в случае изменения действующего законодательства и иных нормативных актов в области обработки и обеспечения безопасности персональных данных.

1.6. Ответственным за внесение изменений в настоящую Инструкцию является руководитель ответственного за обеспечение информационной безопасности подразделения.

1.7. Контроль за выполнением требований настоящей инструкции осуществляет руководитель ответственного за обеспечение информационной безопасности подразделения.

2. Обязанности ответственного за обеспечение безопасности и обработку персональных данных

Ответственный за обеспечение безопасности и обработку персональных данных обязан:

руководствоваться в своей деятельности Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Россий-

ской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», другими нормативными правовыми актами и настоящей должностной инструкцией;

осуществлять внутренний контроль за соблюдением требований законодательства РФ при обработке персональных данных объекта автоматизации, в том числе требований к защите персональных данных;

осуществить сбор согласий на обработку персональных данных с сотрудников объекта автоматизации;

ознакомиться под роспись со всеми нормативными документами администрации Апанасенковского муниципального округа Ставропольского края, регламентирующими процессы обработки и обеспечения безопасности персональных данных;

осуществить ознакомление под роспись с нормативными документами администрации Апанасенковского муниципального округа Ставропольского края ответственных и прочих лиц, в части их касающейся;

осуществлять доведение до сведения сотрудников администрации Апанасенковского муниципального округа Ставропольского края законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

осуществлять организацию приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;

осуществлять предоставление субъекту персональных данных по его просьбе информацию;

осуществлять разъяснения субъекту персональных данных юридических последствий отказа предоставления его персональных данных;

провести классификацию информационных систем;

проводить инструктаж сотрудникам администрации Апанасенковского муниципального округа Ставропольского края по следующим темам:

1) «Порядок организации и проведения работ по обработке и защите персональных данных, обрабатываемых в информационных системах»;

2) «Обработка персональных данных без использования средств автоматизации» (на основании Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 – для сотрудников, ответственных за обеспечение сохранности материальных носителей ПДн);

осуществлять периодические проверки состояния защиты персональных данных;

осуществлять пересмотр, при необходимости, нормативных документов, регламентирующих процессы обработки и обеспечения безопасности персональных данных.

1.8. Ответственный за обеспечение безопасности и обработку персональных данных является ответственным лицом при проведении проверок администрации Апанасенковского муниципального округа Ставропольского края регулирующими органами по вопросам обеспечения безопасности персональных данных.

3. Права ответственного за обеспечение безопасности и обработку персональных данных

Ответственный за обеспечение безопасности и обработку персональных данных имеет право:

требовать от пользователей безусловного соблюдения установленной технологии обработки персональных данных и выполнения требований внутренних документов объ-

екта автоматизации, регламентирующих вопросы обеспечения безопасности персональных данных;

инициировать проведение служебных расследований по фактам нарушения установленных требований;

привлекать для выполнения требований по обеспечению безопасности персональных данных любых сотрудников администрации Апанасенковского муниципального округа Ставропольского края.

4. Ответственность ответственного за обеспечение безопасности и обработку персональных данных

Ответственный за обеспечение безопасности и обработку персональных данных несет ответственность:

за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими инструктивными документами в соответствии с действующим законодательством Российской Федерации, трудовым законодательством Российской Федерации, за полноту и качество проводимых им работ по обеспечению защиты персональных данных;

за правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

за разглашение сведений конфиденциального характера и другой защищаемой информации объекта автоматизации в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

на ответственного за обеспечение безопасности и обработку персональных данных возлагается персональная ответственность за выполнение требований к обработке и обеспечению безопасности персональных данных в администрации Апанасенковского муниципального округа Ставропольского края.

Ответственный за обработку ПДн _____ ФИО

_____

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

№ п/п	Фамилия, инициалы сотрудника	Должность	Дата ознакомления	Подпись сотрудника

_____

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ИНСТРУКЦИЯ

пользователя информационных систем
администрации Апанасенковского муниципального округа
Ставропольского края

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, и ответственность пользователя информационных систем (далее – ИС) администрации Апанасенковского муниципального округа Ставропольского края (далее – Администрация).

1.2. Пользователь ИС подчиняется своему непосредственному руководителю, администратору ИС, администратору информационной безопасности (далее – Администратор ИБ), ответственному за обеспечение безопасности и обработку персональных данных администрации Апанасенковского муниципального округа Ставропольского края.

1.3. Пользователь ИС руководствуется положениями федеральных законов и нормативных актов органов государственной власти, ведомственных организационно-распорядительных актов, нормативных актов администрации Апанасенковского муниципального округа Ставропольского края, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

1.4. Внесение изменений в настоящую Инструкцию осуществляется на периодической и внеплановой основе:

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

внеплановое внесение изменений в настоящую Инструкцию может производиться в случае изменения действующего законодательства и иных нормативных актов в области обеспечения безопасности информации.

1.5. Ответственным за внесение изменений в настоящую Инструкцию является руководитель ответственного за обеспечение информационной безопасности подразделения.

1.6. Контроль за выполнением требований настоящей инструкции осуществляет Администратор ИБ.

2. Функции и обязанности пользователя ИС

Каждый сотрудник администрации Апанасенковского муниципального округа Ставропольского края, имеющий доступ к аппаратным средствам, программному обеспечению и данным, содержащимся в ИС, несет персональную ответственность за свои действия и обязан:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;

выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам, техническим средствам, полученным в установленном порядке;

знать и строго выполнять правила работы со средствами защиты информации, установленными в ИС;

хранить в тайне свой пароль (пароли);

исполнять требования «Инструкции по парольной защите в информационных системах администрации Апанасенковского муниципального округа Ставропольского края», «Инструкции по организации антивирусной защиты в информационных системах администрации Апанасенковского муниципального округа Ставропольского края», а также других документов, регламентирующих вопросы работы ИС и обеспечения безопасности информации в части, его касающейся;

немедленно ставить в известность Администратор ИБ и начальника отдела в случае утери личных реквизитов доступа, при компрометации личных паролей, подозрении на совершение попыток несанкционированного доступа (НСД) к персональным электронно-вычислительным машинам, обнаружении несанкционированных изменений в конфигурации программных или аппаратных средств ИС;

немедленно ставить в известность администратора ИС при обнаружении отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИС, выхода из строя или неустойчивого функционирования устройств ПЭВМ (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных ТС защиты информации;

при обработке на ПЭВМ защищаемой информации присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним ПЭВМ в отделе;

при обработке на ПЭВМ защищаемой информации и необходимости использовать носители информации, применять только учтенные носители.

Сотрудникам запрещается:

использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;

хранить и обрабатывать личную информацию на ПЭВМ и серверах ИС;

при работе в сети Интернет:

1) использовать информационные ресурсы сети Интернет, содержание которых нарушает действующее законодательство Российской Федерации;

2) использовать информационные ресурсы сети Интернет для целей, не связанных с областью производственной деятельности пользователя;

3) использовать информационные ресурсы сети Интернет в личных целях;

4) вносить изменения в состав и/или процесс работы внешних информационных ресурсов, если такие изменения не санкционированы собственником (владельцем) соответствующего ресурса;

самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИС или устанавливать дополнительно любые программные и аппаратные средства;

оставлять без присмотра включенную ПЭВМ, не активизировав средства защиты от НСД;

оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа;

оставлять без личного присмотра в легкодоступном месте на рабочем месте или где бы то ни было свои машинные носители и распечатки, содержащие сведения ограниченного распространения;

использовать в работе неучтенные носители информации для обработки защищаемой информации;

умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты, об обнаружении такого рода ошибок – ставить в известность Администратор ИБ и начальника своего отдела.

Администратор ИБ _____ ФИО

_____

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений в инструкции

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

№ п/п	Фамилия, инициалы сотрудника	Должность	Дата ознакомления	Расписка сотрудника в ознакомлении

ЗАЯВКА

на внесение изменений в состав программного (аппаратного) обеспечения (ненужное зачеркнуть)

Прошу произвести установку (изменение настроек) (ненужное зачеркнуть)

_____

_____

_____

(перечень ПО (аппаратных средств) и необходимых настроек)

для решения задач:

_____

_____

_____

_____

следующим пользователям:

_____

_____

_____

(фамилия, имя, отчество)

«___» _____ 2021 г. _____ _____

(подпись) (Фамилия, инициалы)

_____

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ИНСТРУКЦИЯ

по организации антивирусной защиты в информационных системах
администрации Апанасенковского муниципального
округа Ставропольского края

1. Общие положения

1.1. Инструкция по организации антивирусной защиты в информационных системах (далее – ИС) администрации Апанасенковского муниципального округа Ставропольского края (далее – администрация) определяет требования к организации защиты ИС от угроз информационной безопасности, связанных с воздействием компьютерных вирусов, а также устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИС, за их выполнение.

1.2. Требования настоящей Инструкции распространяются на всех сотрудников администрации, являющихся пользователями ИС.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов проводятся организуемые администратором информационной безопасности (далее – администратор ИБ) семинары и персональные инструктажи (при необходимости) пользователей ИС.

1.4. Доведение Инструкции до сотрудников администрации в части их касающейся осуществляется администратором ИБ под роспись в журнале или самом документе. Лист ознакомления с Инструкцией представлен в Приложении 2.

1.5. Внесение изменений в настоящую Инструкцию осуществляется на периодической и внеплановой основе:

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

внеплановое внесение изменений может проводиться в случае приобретения администрацией новых средств защиты, существенно изменяющих порядок работы с ними, либо по результатам контрольных мероприятий.

1.6. Ответственным за внесение изменений в настоящую Инструкцию является руководитель ответственного за обеспечение информационной безопасности подразделения.

1.7. Ответственность за выполнение положений настоящей Инструкции несут все пользователи ИС. Ответственность сотрудников администрации за несоблюдение требований настоящей Инструкции, повлекших за собой разглашение или утрату информации, обрабатываемую в ИС, определяется законодательством РФ, внутренними нормативными документами администрации, а также должностными инструкциями работников администрации.

1.8. Общий контроль выполнения требований данной Инструкции возлагается на руководителя ответственного за обеспечение информационной безопасности подразделения.

1.9. Ответственность за организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на администратора ИБ.

2. Применение средств антивирусной защиты

2.1. Антивирусный контроль дисков и файлов ИС после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.2. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИС (сканирование).

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, Flash накопитель, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

2.4. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

3. Функции администратора ИБ по обеспечению антивирусной безопасности

Администратор ИБ обязан:

проводить при необходимости инструктажи пользователей ИС по вопросам применения средств антивирусной защиты;

настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств;

предварительно проверять устанавливаемое (обновляемое) ПО на отсутствие вирусов;

при необходимости производить обновление антивирусных программных средств;

производить получение и рассылку (при необходимости) обновлений антивирусных баз;

при необходимости разрабатывать инструкции по работе пользователей с программными средствами системы антивирусной защиты;

проводить работы по обнаружению и обезвреживанию вирусов;

участвовать в работе комиссии по расследованию причин заражения ПЭВМ и серверов;

хранить эталонные копии антивирусных программных средств;

осуществлять периодический контроль за соблюдением пользователями ПЭВМ требований настоящей Инструкции;

разрабатывать инструкции по работе пользователей с системой антивирусной защиты информации;

проводить периодический контроль работы программных средств системы антивирусной защиты информации на ПЭВМ (серверах).

4. Функции пользователей ИС

Пользователи ИС:

получают по ЛВС или от администратора ИБ носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз);

проводят обновления антивирусных баз на ПЭВМ (в случае отсутствия механизмов централизованного распространения антивирусных баз);

при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник отдела самостоятельно или вместе с администратором ИБ должен провести внеочередной ан-

тивирусный контроль ПЭВМ. При необходимости он должен привлечь администратора ИБ для определения факта наличия или отсутствия компьютерного вируса;

в случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники отделов обязаны:

1) приостановить работу;

2) немедленно поставить в известность о факте обнаружения зараженных вирусом файлов начальника отдела и администратора ИБ, владельца зараженных файлов, а также смежные отделы, использующие эти файлы в работе;

3) совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

4) провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора ИБ);

5) по факту обнаружения зараженных вирусом файлов составить служебную записку администратору ИБ, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

Администратор ИБ _____
ФИО

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений в инструкции

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

№ п/п	Фамилия, инициалы сотрудника	Должность	Дата ознакомления	Расписка сотрудника в ознакомлении

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ИНСТРУКЦИЯ

по парольной защите в информационных системах администрации Апанасенковского муниципального округа Ставропольского края

1. Общие положения

1.1. Инструкция по парольной защите в информационных системах (далее – ИС) администрации Апанасенковского муниципального округа Ставропольского края (далее – Администрация), включает в себя взаимоувязанный комплекс организационно-технических мер, регламентирующих генерацию и/или выбор, использование, хранение, уничтожение парольной информации в ИС.

1.2. Требования настоящей Инструкции распространяются на всех сотрудников администрации Апанасенковского муниципального округа Ставропольского края, являющихся пользователями ИС.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов проводятся организуемые администратором информационной безопасности (далее – АИБ) семинары и персональные инструктажи (при необходимости) пользователей ИС.

1.4. Доведение Инструкции до сотрудников администрации Апанасенковского муниципального округа Ставропольского края, в части их касающейся, осуществляется АИБ под роспись в журнале или самом документе. Лист ознакомления с Инструкцией представлен в Приложении 2.

1.5. Внесение изменений в настоящую Инструкцию осуществляется на периодической и внеплановой основе:

пересмотр положений настоящей Инструкции должно осуществляться не реже одного раза в 24 месяца;

внеплановое внесение изменений может проводиться в случае приобретения администрации Апанасенковского муниципального округа Ставропольского края новых средств защиты, существенно изменяющих порядок работы с ними, либо по результатам контрольных мероприятий.

1.6. Ответственным за внесение изменений в настоящую Инструкцию является руководитель Ответственного за обеспечение информационной безопасности подразделения.

1.7. Ответственность за выполнение положений настоящей Инструкции несут все пользователи ИС. Ответственность сотрудников администрации Апанасенковского муниципального округа Ставропольского края за несоблюдение требований настоящей Инструкции, повлекших за собой разглашение или утрату информации, обрабатываемую в ИС, определяется законодательством РФ, внутренними нормативными документами администрации Апанасенковского муниципального округа Ставропольского края, а также должностными инструкциями работников администрации Апанасенковского муниципального округа Ставропольского края.

1.8. Ответственность за общий контроль выполнения требований данной Инструкции возлагается на руководителя Ответственного за обеспечение информационной безопасности подразделения.

1.9. Ответственность за организацию контрольных и проверочных мероприятий по вопросам парольной защиты возлагается на АИБ.

2. Функции пользователей и АИБ по обеспечению парольной защиты

2.1. Функции пользователей ИС по обеспечению парольной защиты:

регулярная (с частотой, установленной настоящей Инструкцией) смена используемой в работе парольной информации;

выбор парольной информации с качеством, установленным настоящей Инструкцией.

2.2. Функции АИБ:

организационно-методическое обеспечение процессов генерации, смены и удаления паролей в ИС;

разработка всех необходимых инструкций по вопросам парольной защиты ИС;

организация доведения до пользователей ИС требований по парольной защите;

организация периодического и выборочного контроля исполнения сотрудниками администрации Апанасенковского муниципального округа Ставропольского края требований настоящей Инструкции;

согласование выдачи управляющих учетных записей к ИС;

текущий контроль действий персонала администрации Апанасенковского муниципального округа Ставропольского края по работе с паролями (автоматизированный контроль качества паролей – при наличии программно-технических средств);

техническое обеспечение (при наличии программно-технических средств) процессов генерации/выбора, смены и удаления паролей, соответствующая конфигурация ИС.

3. Качество и обращение парольной информации

3.1. Пароли доступа к аппаратно-программным вычислительным средствам, информационным ресурсам ИС формируются (выбираются) пользователями этих ресурсов с учетом следующих требований к качеству парольной информации:

№ п/п	Параметр качества пароля	Администратор	Пользователь
1.	Минимальная длина пароля в символах	10	8
2.	Максимальная длина пароля в символах	32	16
3.	Содержание в пароле букв верхнего и нижнего регистра	да	да
4.	Содержание в пароле специальных символов (@, #, $, &, * и т.п.) и цифр	обязательно	рекомендуется
5.	Содержание в пароле личных имен, фамилий, кличек домашних животных, № телефонов, дат рождения, географических названий, именований АРМ и т.п.	нет	нет

№ п/п	Параметр качества пароля	Администратор	Пользователь
6.	Содержание в пароле общепринятых сокращений (ПЭВМ, ЛВС, USER, SYSOP и т.д.)	нет	нет
7.	Минимальное отличие нового пароля от предыдущего (в позициях)	3	3
8.	Максимальный срок действия пароля	30 дней	60 дней
9.	Минимальный срок действия пароля	нет	нет
10.	Дополнительный (типа ТМ, eToken[1] или другие электронные ключи) идентификатор	рекомендуется	рекомендуется
11.	Пароль на заставку монитора	да	да

3.2. Хранение сотрудником (администратором, пользователем) личных паролей допускается только в личном сейфе (запираемом шкафу, ящике), либо в сейфе (запираемом шкафу, ящике) администратора. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

3.3. Личные пароли и/или дополнительные идентификаторы (электронные ключи) пользователи и администраторы никому не имеют права сообщать и (или) передавать

3.4. Внеплановая смена/удаление пароля (и при возможности учетной записи) пользователя или АИБ в случае прекращения его полномочий должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

3.5. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий АИБ, другими сотрудниками, которым по роду работы были предоставлены либо полномочия по управлению ИС, либо полномочия по управлению подсистемой защиты информации ИС.

3.6. В случае компрометации пароля доступа в ИС, АИБ должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля и обстоятельств компрометации.

3.7. АИБ, проводит ежеквартальный выборочный контроль выполнения сотрудниками администрации Апанасенковского муниципального округа Ставропольского края требований Инструкции.

3.8. У пользователя есть 5 попыток для корректного ввода учетных данных. В том случае если попытки ввода учетных данных исчерпаны система блокирует учетную запись пользователя. Разблокирование учетной записи пользователя осуществляется системой по истечении 15 минут либо АИБ.

4. Обращение дополнительных идентификаторов

4.1. В целях усиления процедур идентификации и аутентификации в ИС, пользователи ИС могут использовать дополнительные индивидуальные электронные идентификаторы (смарт-карты, eToken и т.д.) совместно с личным паролем доступа.

4.2. Дополнительные идентификаторы выдаются и учитываются:

сотрудники получают дополнительные идентификаторы под роспись;

АИБ, по обращению к нему сотрудников, регистрирует дополнительные идентификаторы в ИС и инструктирует сотрудников с учетом требований настоящей Инструкции и правил эксплуатации для дополнительных идентификаторов.

4.3. Сотрудники администрации Апанасенковского муниципального округа Ставропольского края, получившие в пользование дополнительные идентификаторы, лично обеспечивают надежное круглосуточное безопасное хранение и использование идентификаторов. Оставление идентификатора без присмотра запрещается.

4.4. В случае утери дополнительного идентификатора сотрудники немедленно ставят об этом в известность АИБ и своего непосредственного руководителя. АИБ организует немедленную блокировку утерянных ключей в автоматизированных системах.

Администратор ИБ _____ ФИО

_____

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений в инструкции

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

№ п/п	Фамилия, инициалы сотрудника	Должность	Дата ознакомления	Расписка сотрудника в ознакомлении

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ИНСТРУКЦИЯ

по допуску лиц в помещения администрации
Апанасенковского муниципального округа Ставропольского края,
в которых осуществляются обработка информации ограниченного доступа
и эксплуатация криптографических средств защиты информации

1. Общие положения

1.1. Настоящая инструкция разработана в целях обеспечения безопасности конфиденциальной информации и информации содержащей персональные данные (далее – информация ограниченного доступа), средств вычислительной техники информационных систем, обрабатывающих информацию ограниченного доступа, материальных носителей информации ограниченного доступа, а так же обеспечения внутриобъектного режима.

Объектами охраны администрации Апанасенковского муниципального округа Ставропольского края (далее - Администрация) являются:

помещения, в которых происходит обработка информации ограниченного доступа с использованием средств автоматизации;

помещения, в которых установлены компьютеры, серверы и коммутационное оборудование, защищенные средствами криптографической защиты (далее – СКЗИ), участвующие в обработке информации ограниченного доступа;

помещения, в которых хранятся ключевые документы СКЗИ;

1.2. Бесконтрольный доступ посторонних лиц в указанные помещения должен быть исключён.

1.3. Ответственность за соблюдение положений настоящей инструкции несут сотрудники структурных подразделений, обрабатывающих информацию ограниченного доступа, а так же руководители структурных подразделений.

1.4. Контроль соблюдения требований настоящей инструкции возлагается на ответственного пользователя СКЗИ.

1.5. Все объекты охраны администрации Апанасенковского муниципального округа Ставропольского края должны быть оборудованы охранной сигнализацией, либо предусматривать круглосуточное дежурство.

1.6. Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению.

2. Допуск в помещения, в которых ведётся обработка информации ограниченного доступа

2.1. Доступ посторонних лиц в помещения, в которых ведётся обработка информации ограниченного доступа, должен осуществляется только ввиду служебной необходимости. При этом на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с информацией ограниченного доступа.

2.2. Допуск сотрудников в помещения, в которых ведётся обработка информации ограниченного доступа, оформляется после подписания сотрудником обязательства о

неразглашении и проведении инструктажа ответственным пользователем СКЗИ, либо администратором информационной безопасности.

2.3. В нерабочее время помещения, в которых осуществляется функционирования СКЗИ, должны ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, ключевые документы, должны быть убраны в запираемые шкафы (сейфы), средства вычислительной техники выключены либо заблокированы.

3. Допуск лиц в помещения, в которых эксплуатируются СКЗИ

3.1. Помещения, в которых эксплуатируются СКЗИ (далее – спецпомещения) выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное запирание помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц в спецпомещения, необходимо оборудовать металлическими решётками или ставнями, охранной сигнализацией и другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

3.2. Размещение, специальное оборудование, охрана и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

3.3. Для предотвращения просмотра извне спецпомещений их окна должны быть защищены жалюзями или плотными занавесками.

3.4. Спецпомещения, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по администрации Апанасенковского муниципального округа Ставропольского края. Исправность сигнализации необходимо периодически проверять ответственному пользователю СКЗИ совместно с представителем службы охраны или дежурным по администрации Апанасенковского муниципального округа Ставропольского края.

3.5. Для хранения ключевых документов, эксплуатационной и технической документации, установочных пакетов СКЗИ должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у ответственного пользователя СКЗИ, второй на посту охраны.

3.6. По окончании рабочего дня спецпомещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны.

3.7. Ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ спецпомещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по администрации Апанасенковского муниципального округа Ставропольского края одновременно с передачей под охрану самих спецпомещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей СКЗИ, ответственных за эти хранилища.

3.8. При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей. Факт изготовления новых ключей должен быть документально оформлен в виде акта в произвольной форме. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых документов и технической и эксплуатационной документации к СКЗИ в хранилище, от которого утрачен ключ, устанавливает ответственный пользователь СКЗИ.

3.9. В обычных условиях спецпомещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями СКЗИ или ответственным пользователем СКЗИ.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ. Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей.

3.10. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

3.11. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным пользователем СКЗИ необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

Администратор ИБ _____ ФИО

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений в инструкции

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

№ п/п	Фамилия, инициалы сотрудника	Должность	Дата ознакомления	Расписка сотрудника в ознакомлении

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ИНСТРУКЦИЯ

об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в администрации Апанасенковского муниципального округа Ставропольского края

1. Общие положения

1.1. Средства криптографической защиты информации (далее – СКЗИ) предназначены для обеспечения безопасности хранения, обработки и передачи по каналам связи информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну.

1.2. Обладатели конфиденциальной информации обязаны выполнять указания ответственного пользователя СКЗИ по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

1.3. Для работы с СКЗИ допускаются только уполномоченные должностные лица, имеющие необходимый уровень знаний работы с СКЗИ и назначенные Распоряжением администрации Апанасенковского муниципального округа Ставропольского края (далее - Администрация).

1.4. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения и ознакомления с настоящей инструкцией. Обучение пользователей правилам работы с СКЗИ осуществляет ответственный пользователь СКЗИ.

1.5. Изготовление ключевых документов осуществляется ответственным пользователем СКЗИ с применением штатных СКЗИ (если такая возможность предусмотрена эксплуатационной и технической документацией СКЗИ).

1.6. Ключевые документы, СКЗИ с введёнными криптографическими ключами относятся к материальным носителям, содержащие конфиденциальную информацию. При этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения с конфиденциальной информацией в администрации Апанасенковского муниципального округа Ставропольского края.

1.7. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учёту в «Журнале поэкземплярного учета средств криптографической защиты информации в администрации Апанасенковского муниципального округа Ставропольского края».

1.8. Все экземпляры СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы должны быть выданы под расписку в соответствующем журнале учета пользователей СКЗИ, несущих персональную ответственность за их сохранность.

1.9. Передача экземпляров СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под расписку в соответствующем журнале.

1.10. Пользователи СКЗИ хранят установочные пакеты СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в шкафах (ящиках, сейфах)

индивидуального пользования, в условиях, исключающих бесконтрольный доступ к ним, а также непреднамеренное уничтожение.

1.11. Для исключения утраты ключевой информации вследствие дефектов носителей (eToken) рекомендуется создать их резервные копии. Копии должны быть соответствующим образом маркированы и могут использоваться и храниться так же, как и оригиналы.

1.12. Криптографические ключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно изъять и при доказательстве компрометации надлежащим образом уничтожить.

1.13. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов и ключевых носителей.

1.14. Средства вычислительной техники, на которых осуществляется штатное функционирование СКЗИ, должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

2. Обязанности пользователя СКЗИ

2.1. Пользователь СКЗИ обязан:

не разглашать конфиденциальную информацию, к которой они допущены, рубежи её защиты, в том числе сведения о криптоключах;

соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

сообщать ответственному пользователю СКЗИ о ставших им известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов к ним;

при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы;

немедленно уведомлять ответственного пользователя СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

2.2. Пользователям СКЗИ запрещается:

осуществлять несанкционированное копирование ключевых документов;

осуществлять несанкционированный вынос ключевых носителей за пределы контролируемой зоны;

хранить ключевые документы и ключевые носители вне специально выделенных хранилищ и помещений;

вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;

вносить какие-либо изменения в программное обеспечение СКЗИ;

изменять настройки, установленные программой установки СКЗИ или администратором информационной безопасности;

осуществлять несанкционированное вскрытие системных блоков ПЭВМ, подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в комплектации.

Ответственный пользователь СКЗИ _____
ФИО

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений в инструкции

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

№ п/п	Фамилия, инициалы сотрудника	Должность	Дата ознакомле-ния	Расписка сотруд-ника в ознакомле-нии

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ

ответственного пользователя средств криптографической защиты информации администрации Апанасенковского муниципального округа Ставропольского края

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность ответственного пользователя СКЗИ администрации Апанасенковского муниципального округа Ставропольского края (далее – Администрация).

1.2. Ответственный пользователь СКЗИ назначается распоряжением администрации Апанасенковского муниципального округа Ставропольского края приказом и функционально подчиняется начальнику отдела, в штате которого он состоит.

2. Квалификационные требования

Профессиональные знания и навыки:

2.1. Ответственный пользователь СКЗИ в своей работе руководствуется следующими нормативными документами Российской Федерации и организационно-распорядительной документацией администрации Апанасенковского муниципального округа Ставропольского края:

«Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в администрации Апанасенковского муниципального округа Ставропольского края»;

распоряжениями, инструкциями и иными организационно-распорядительными документами администрации Апанасенковского муниципального округа Ставропольского края.

3. Функциональные обязанности ответственного пользователя СКЗИ

3.1. В обязанности ответственного пользователя СКЗИ входит:

своевременное и качественное исполнение поручений руководства администрации Апанасенковского муниципального округа Ставропольского края, данные в пределах их полномочий, установленных законодательством Российской Федерации;

оказание консультационной помощи по вопросам соблюдения защиты информации при обращении со средствами криптографической защиты информации (далее – СКЗИ);

постоянное повышение профессиональных навыков и умений, необходимых для надлежащего исполнения функциональных обязанностей;

знание порядка эксплуатации используемых администрацией Апанасенковского муниципального округа Ставропольского края СКЗИ;

ведение установленного нормативными документами учета СКЗИ, ключевых документов, сертификатов электронных цифровых подписей;

соблюдение режима конфиденциальности при обращении со сведениями, полученными при исполнении функциональных обязанностей, в том числе со сведениями о функ-

ционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;

надежное хранение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

выявление попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним и своевременное оповещение об этом руководителя органа криптографической защиты информации;

немедленное принятие мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

3.2. Ответственный пользователь СКЗИ осуществляет следующие функции:

осуществляет профилактическую деятельность по соблюдению требований руководящих документов, технической, эксплуатационной документации с сотрудниками Управления, назначенными пользователями СКЗИ;

участвует в проведении служебных расследований по фактам нарушения требований по обращению с СКЗИ;

принимает меры к предотвращению разглашения и утечки информации ограниченного доступа при эксплуатации и хранении специальных технических средств, предназначенных для передачи, приема и обработки конфиденциальной информации, а также при использовании незащищенных каналов связи;

участвует в разработке методических и нормативных материалов и оказании необходимой методической помощи в проведении работ по защите информации при обращении с СКЗИ.

4. Права ответственного пользователя СКЗИ

4.1. Ответственный пользователь СКЗИ имеет право:

осуществлять плановые и внеплановые проверки функционирования СКЗИ, наличия ключевых документов и технической документации с СКЗИ;

осуществлять, в рамках своей компетенции, взаимодействие с организациями-производителями СКЗИ;

при изменении состава СКЗИ получить профессиональную переподготовку, повышение квалификации и стажировку в порядке, установленном законодательством Российской Федерации;

ходатайствовать о проведении служебной проверки.

5. Ответственность ответственного пользователя СКЗИ

5.1. Ответственный пользователь СКЗИ несет персональную ответственность в соответствии с законодательством Российской Федерации за:

выполнение возложенных на него обязанностей и правильное использование предоставленных ему прав в соответствии с данными функциональными обязанностями;

несвоевременное или некачественное выполнение распоряжений администрации Апанасенковского муниципального округа Ставропольского края;

разглашение сведений, отнесенных к сведениям ограниченного доступа, ставших известными в ходе выполнения функциональных обязанностей или иным путем, утрату их носителей, передачу третьим лицам, публикацию без разрешения руководства, а также использование для занятия любой деятельностью, которая может нанести ущерб администрации Апанасенковского муниципального округа Ставропольского края.

Ответственный пользователь СКЗИ _____
ФИО

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ПРАВИЛА

осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных»,
принятыми в соответствии с ним правовыми актами
администрации Апанасенковского муниципального округа Ставропольского края

1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания и порядок проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом № 152-ФЗ, принятыми в соответствии с ним правовыми актами администрации Апанасенковского муниципального округа Ставропольского края (далее – внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных).

2. Условия осуществления внутреннего контроля

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Апанасенковского муниципального округа Ставропольского края (далее – Администрация) организовывается проведение периодических проверок условий обработки персональных данных (далее – проверки).

2.2. Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных в администрации Апанасенковского муниципального округа Ставропольского (далее – ответственный за организацию обработки персональных данных), либо комиссией, образуемой распоряжением администрации Апанасенковского муниципального округа Ставропольского края.

2.3. В проведении проверки не может участвовать сотрудник администрации Апанасенковского муниципального округа Ставропольского края прямо или косвенно заинтересованный в её результатах.

2.4. Проверки проводятся на основании утвержденного администрацией Апанасенковского муниципального округа Ставропольского края ежегодного Плана осуществления

внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных (плановые проверки) или на основании поступившего в администрацию Апанасенковского муниципального округа Ставропольского края письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

2.5. Плановые проверки проводятся не чаще чем один раз в полгода.

2.6. Проведение внеплановой проверки организуется в течение трех рабочих дней.

2.7. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

2.7.1. Порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

2.7.2. Порядок и условия применения средств защиты информации.

2.7.3. Эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы.

2.7.4. Состояние учета машинных носителей персональных данных.

2.7.5. Соблюдение правил доступа к персональным данным.

2.7.6. Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

2.7.7. Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.7.8. Осуществление мероприятий по обеспечению целостности персональных данных.

2.8. Ответственный за организацию обработки персональных данных в администрации Апанасенковского муниципального округа Ставропольского края или комиссия имеет право:

2.8.1. Запрашивать у сотрудников администрации Апанасенковского муниципального округа Ставропольского края информацию, необходимую для реализации полномочий.

2.8.2. Требовать от уполномоченных на обработку персональных данных должностных лиц администрации Апанасенковского муниципального округа Ставропольского края уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных.

2.8.3. Принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации.

2.8.4. Вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

2.8.5. Вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.9. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных, либо комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

2.10. По результатам проведения проверки оформляется акт проверки, который подписывается ответственным за организацию обработки персональных данных или членами комиссии.

2.11. Срок проведения проверки и оформления акта составляет 30 календарных дней со дня начала проверки, указанного в правовом акте о назначении проверки.

2.12. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

Ответственный за обработку ПДн _____
ФИО

_____

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ПРАВИЛА

рассмотрения запросов субъектов персональных данных

1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Федеральным законом от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами» и определяют порядок организации работы по приему, регистрации и рассмотрению поступивших в администрацию Апанасенковского муниципального округа Ставропольского края (далее – оператор) запросов субъектов персональных данных или их представителей (далее – запросы).

1.2. Целью настоящих Правил является упорядочение действий сотрудников оператора при обращении либо при получении запросов.

2. Прием, регистрация и рассмотрение запросов

2.1. Сведения, касающиеся обработки персональных данных субъекта персональных данных, предоставляются оператором субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

2.2. Запрос может быть подан одним из следующих способов:

лично;

письменно;

с использованием средств факсимильной связи или электронной связи, в том числе через официальный сайт оператора в информационно-телекоммуникационной сети «Интернет».

2.3. Информация об операторе, включая информацию о месте его нахождения, графике работы, контактных телефонах, а также о порядке обработки персональных данных размещается:

на стендах, расположенных в помещениях, занимаемых оператором;

на официальном сайте оператора в информационно-телекоммуникационной сети «Интернет».

2.4. Прием субъектов персональных данных или их представителей ведется сотрудниками оператора, ответственными за прием и регистрацию обращений в соответствии с графиком приема.

2.5. При приеме субъект персональных данных или его представитель предъявляет документ, удостоверяющий его личность, а также документ, подтверждающий полномочия представителя (в случае обращения представителя субъекта персональных данных).

2.6. Краткое содержание обращения заносится в «Журнал учета обращений граждан-субъектов персональных данных о выполнении их законных прав». В случае если изложенные в устном обращении факты и обстоятельства являются очевидными и не требуют дополнительной проверки, ответ с согласия субъекта персональных данных или его представителя может быть дан устно в ходе личного приема. В остальных случаях дается письменный ответ по существу поставленных в обращении вопросов. В «Журнале учета обращений граждан-субъектов персональных данных о выполнении их законных прав» производится соответствующая запись.

2.7. В том случае, когда при личном приеме субъект персональных данных или его представитель изъявил желание получить ответ в письменной форме, сотрудник оператора, ответственный за прием и регистрацию обращений, предлагает оформить письменный запрос и сообщает ему о сроках, в течение которых оператор обязан дать ответ на такой запрос в соответствии с федеральным законом.

2.8. В случае если в обращении содержатся вопросы, решение которых не входит в компетенцию оператора, субъекту персональных данных или его представителю дается разъяснение, куда и в каком порядке ему следует обратиться.

2.9. Запросы регистрируются в день их поступления к оператору в «Журнале учета обращений граждан-субъектов персональных данных о выполнении их законных прав». Днем обращения считается дата регистрации запроса субъекта персональных данных или его представителя.

2.10. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

2.11. Рассмотрение запросов субъектов персональных данных или их представителей осуществляется сотрудниками оператора, ответственными за их рассмотрение и подготовку ответов (далее – уполномоченные сотрудники оператора).

2.12. При рассмотрении запросов обеспечивается:

объективное, всестороннее и своевременное рассмотрения запроса;

принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

направление письменных ответов по существу запроса.

2.13. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской.

2.14. Оператор отказывает субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным.

2.15. Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение десяти календарных дней с даты обращения субъекта персональных данных или его представителя.

2.16. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя сотрудники оператора обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являю-

щееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его представителя.

2.17. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

2.18. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы.

3. Контроль за соблюдением порядка рассмотрения запросов субъектов персональных данных или их представителей

3.1. Оператор осуществляет контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов.

3.2. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных сотрудников оператора ответственность в соответствии с законодательством Российской Федерации.

Ответственный за обработку ПДн _____
ФИО

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ПРАВИЛА

обработки персональных данных в администрации
Апанасенковского муниципального округа
Ставропольского края

1. Общие положения

1.1. Обработка персональных данных может осуществляться исключительно в целях принятия решения о трудоустройстве, кадрового планирования, осуществления трудовых отношений, и в случаях, установленных законодательством Российской Федерации.

1.2. При определении объема и содержания обрабатываемых персональных данных в администрации Апанасенковского муниципального округа Ставропольского края (далее – администрация АМО СК) необходимо руководствоваться Конституцией Российской Федерации от 25.12.1993 года, Трудовым кодексом Российской Федерации от 30.12.2001 года № 197-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 года № 152-ФЗ и иными нормативно-правовыми актами Российской Федерации.

2. Порядок хранения персональных данных

2.1. Хранение электронных носителей (дискет, дисков и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

2.2. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

2.3. Обработка персональных данных в администрации Апанасенковского муниципального округа Ставропольского края осуществляется до утраты правовых оснований обработки персональных данных. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в администрации Апанасенковского муниципального округа Ставропольского края определяются «Перечнем персональных данных в администрации Апанасенковского муниципального округа Ставропольского края».

2.4. По истечении срока хранения документы, либо иные материальные носители персональных данных должны быть уничтожены без возможности восстановления (например, в бумагорезательных машинах) с составлением акта. Для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ без уничтожения материального носителя.

2.5. Обезличивания персональных данных в администрации Апанасенковского муниципального округа Ставропольского края не предполагается.

3. Порядок работы со сведениями, содержащими персональные данные

3.1. При обработке персональных данных на бумажных документах, съёмных носителях (дискетах, дисках, флеш-носителях и т.п.), компьютерах и других технических сред-

ствах, сотрудники администрации Апанасенковского муниципального округа Ставропольского края обязаны следить как за сохранностью самих бумажных документов, съёмных носителей и компьютеров, и других технических средств, так и за сохранностью содержащейся в них информации, а именно не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

3.2. Допуск к персональным данным субъекта могут иметь только те сотрудники администрации Апанасенковского муниципального округа Ставропольского края, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких сотрудников отражен в «Приказе об утверждении списка должностных лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей».

3.3. Процедура оформления допуска к персональным данным представляет собой истребование с сотрудника «Обязательство о неразглашении конфиденциальной информации».

3.4. Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

3.5. Сотрудникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

3.6. Запрещается хранение или оставление бумажных документов и съёмных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съёмных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах, сейфах и помещениях, к которым исключён доступ лиц, не допущенных к обработке соответствующих персональных данных.

3.7. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съёмные носители.

3.8. Запрещается использовать для передачи персональных данных съёмные носители, не учтённые в «Журнале учета носителей персональных данных в администрации Апанасенковского муниципального округа Ставропольского края».

3.9. Запрещается выносить документы, съёмные носители или переносные компьютеры, содержащие персональные данные, за пределы служебных помещений администрации Апанасенковского муниципального округа Ставропольского края, если это не требуется для выполнения служебных (трудовых) обязанностей и если на это не дано разрешение руководителя администрации Апанасенковского муниципального округа Ставропольского края или ответственного за организацию обработки персональных данных.

3.10. Бумажные документы с персональными данными, у которых истёк срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления (например, в шредерах).

3.11. Большие объёмы бумажных документов с персональными данными, съёмные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных, способом, исключающим дальнейшее восстановление информации.

3.12. Мониторы компьютеров, использующихся для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуск к обработке персональных данных.

3.13. Категорически запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.

3.14. Запрещается в нерабочее время или за пределами служебных помещений упоминать в разговоре с кем-либо, включая любых сотрудников администрации Апанасенковского муниципального округа Ставропольского края, сведения, содержащие персональные данные.

3.15. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, администратора безопасности информации, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

3.16. Передавать персональные данные субъектов допускается только тем сотрудникам, которые имеют допуск к обработке персональных данных.

3.17. Предоставление персональных данных допускается в случаях передачи Федеральной налоговой службе, Пенсионному фонду России, «Банку» с целью начисления заработной платы, а также в иных случаях, установленных законодательством РФ.

3.18. Не допускается распространение персональных данных субъекта.

4. Уничтожение документов, содержащих персональные данные

4.1. Уничтожение документов, содержащих персональные данные, в том числе черновиков, бракованных листов и испорченных копий, производиться назначенной комиссией с обязательной простановкой отметок об уничтожении в соответствующих учетных документах.

4.2. Порядок уничтожения черновиков, испорченных листов, неподписанных проектов документов, содержащих персональные данные:

а) черновики документов, испорченные листы, варианты и неподписанные проекты документов надрываются (возможно использование автоматических уничтожителей бумаги) и помещаются в урну (мешок).

б) по мере накопления содержимое урны (мешка) изымается работниками и уничтожается;

в) уничтожение документов, содержащих персональные данные, производится в строгом соответствии со сроками хранения;

г) разрешение на уничтожение дает комиссия;

д) при проведении экспертизы ценности документов перед их передачей на архивное состояние, отбор документов на уничтожение производит комиссия;

е) отобранные для уничтожения документы, содержащие персональные данные, вносятся в акт установленной формы, сверяются перед уничтожением работниками с учетными данными и уничтожаются;

ж) после уничтожения в учетных данных производятся отметки с указанием номера акта, даты уничтожения и подписи сотрудников, производивших уничтожение;

з) уничтожение документов, содержащих персональные данные, производиться путем их сожжения или измельчения или другим путем исключающим восстановление текста документов.

5. Организация защиты персональных данных

5.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается в администрации Апанасенковского муниципального округа Ставропольского края за счет своих средств.

5.2. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

5.2.1. Проведение организационных мероприятий:

разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

организация учёта носителей персональных данных;

проведение обучения сотрудников вопросам защиты персональных данных.

5.2.2. Программно-аппаратная защита:

внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании» оценку соответствия.

5.2.3. Инженерно-техническая защита:

установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

5.3. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами администрации Апанасенковского муниципального округа Ставропольского края.

5.4. Организацию и контроль защиты персональных данных в структурных подразделениях администрации Апанасенковского муниципального округа Ставропольского края осуществляют их непосредственные руководители.

6. Заключительные положения

6.1. Настоящее Правило утверждается руководителем и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

6.2. Все сотрудники администрации Апанасенковского муниципального округа Ставропольского края участвующие в обработке персональных данных с использованием средств автоматизации, должны быть ознакомлены с настоящим Правилом под подпись.

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

ПОРЯДОК

доступа сотрудников администрации Апанасенковского муниципального округа Ставропольского края в помещения, в которых ведется обработка персональных данных

1. Общие положения

1.1. Настоящий документ администрации Апанасенковского муниципального округа Ставропольского края (далее – Оператор) разработан в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и устанавливает единые требования к доступу сотрудников оператора в помещения в целях предотвращения нарушения прав субъектов персональных данных, персональные данные которых обрабатываются оператором, и обеспечения соблюдения требований законодательства о персональных данных.

2. Доступ сотрудников оператора в помещения, в которых ведется обработка персональных данных

2.1. Размещение информационных систем, специального оборудования осуществляется в охраняемых помещениях. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

2.2. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только уполномоченные на обработку персональных данных сотрудники оператора («Список лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей»).

2.3. Ответственными за организацию доступа в помещения, в которых ведется обработка персональных данных, являются руководители структурных подразделений оператора.

2.4. Нахождение лиц в помещениях, не являющихся уполномоченными на обработку персональных данных, возможно только в сопровождении уполномоченного за обработку персональных данных сотрудника оператора.

2.5. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, проводится лицом ответственным за организацию обработки персональных данных.

Администратор ИБ _____
ФИО

УТВЕРЖДЕНА

распоряжением администрации
Апанасенковского
муниципального округа
Ставропольского края

от 01 декабря 2021 г. № 358-р

РЕГЛАМЕНТ

резервного копирования и восстановления данных

1. Общие положения

1.1. Настоящий Регламент резервного копирования и восстановления данных, хранящихся на серверах и рабочих станциях администрации Апанасенковского муниципального округа Ставропольского края (далее – Администрация) разработан в соответствии с требованиями Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящий Регламент разработан с целью:

1.2.1. Определения порядка резервирования данных для последующего восстановления работоспособности информационных систем (далее – ИС) администрации Апанасенковского муниципального округа Ставропольского края при полной или частичной потере информации, вызванной попытками несанкционированного доступа, сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.).

1.2.2. Определения порядка восстановления информации в случае возникновения такой необходимости.

1.2.3. Упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации.

1.3. В настоящем документе регламентируются действия при выполнении следующих мероприятий:

резервное копирование;

контроль резервного копирования;

хранение резервных копий;

полное или частичное восстановление данных и приложений.

1.4. Если резервирование предполагает выгрузку на съемные машинные носители информации, то такие носители должны учитываться в порядке, установленном «Инструкцией администратора информационной безопасности администрации Апанасенковского муниципального округа Ставропольского края».

2. Термины и определения

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (статья 3 ФЗ РФ от 27.07.2006 года № 152-ФЗ «О персональных данных»).

2.2. Резервное копирование – процесс создания копии данных на носителе (дисковом массиве, магнитной ленте и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

2.3. Система резервного копирования – совокупность программного и аппаратного обеспечения, выполняющая задачу резервного копирования информации.

3. Порядок резервного копирования

3.1. Резервному копированию подлежит информация следующих основных категорий:

3.1.1. Базы данных, содержащие персональные данные субъектов.

3.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью.

3.3. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, должно быть немедленно сообщено администратору информационной безопасности (далее – Администратор ИБ), либо ответственному за обеспечение безопасности персональных данных администрации Апанасенковского муниципального округа Ставропольского края.

3.4. Существуют следующие наборы резервных копий:

3.4.1. Месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – 1 (Один) месяц.

3.5. Копии хранятся на внешнем носителе.

3.6. Для резервирования информации, хранимой в базах данных ИС, в качестве промежуточного звена автоматизации используются архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных ИС.

3.7. При резервировании информации следует руководствоваться инструкциями, описанными в документации, прилагающейся к системе резервного копирования ПО.

4. Контроль результатов резервного копирования

4.1. Контроль результатов всех процедур резервного копирования осуществляется Администратором ИБ.

5.2. 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 её хранения.

5. Ротация носителей резервной копии

5.1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации ИС в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение, осуществляются Администратором ИБ. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

5.2. Носители с персональными данными, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения, реализующим полное физическое уничтожение данных.

6. Восстановление информации из резервной копии

6.1. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя ИС. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более 1 (Одного) рабочего дня.

6.2. Любое восстановление информации выполняется на основании заявки пользователя Администратору ИБ или в случае необходимости восстановления утерянной или повреждённой информации, подлежащей резервированию. В процессе восстановления ре-

зервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к системе резервного копирования ПО.

Администратор ИБ _____ ФИО

_____