**ФИНАНСОВОЕ УПРАВЛЕНИЕ**

**АДМИНИСТРАЦИИ АРЗГИРСКОГО МУНИЦИПАЛЬНОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ**

П Р И К А З

03.02.2021 года с. Арзгир № 82

Об обработке и обеспечении безопасности персональных данных в информационных системах персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края

В соответствии с Федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края согласно приложению 1.

1.2. Инструкцию администратора информационной безопасности информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края согласно приложению 2.

1.3. Инструкцию пользователя информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края согласно приложению 3.

1.4. Порядок парольной защиты в информационных системах персональных данных финансового управлении администрации Арзгирского муниципального округа Ставропольского края согласно приложению 4.

1.5. Инструкцию по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края согласно приложению 5.

1.6. Инструкцию по наделению пользователей информационных систем персональных данных уникальными учетными записями и правами доступа к ресурсам информационных систем персональных данных в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края согласно приложению 6.

1.7. Инструкцию по организации антивирусной защиты информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края согласно приложению 7.

1.8. Инструкцию по резервному копированию защищаемой информации в информационных системах персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края согласно приложению 8.

1.9. Порядок доступа в помещения с компонентами информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края согласно приложению 9.

1.10. Инструкцию учета средств защиты, документации и электронных носителей персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края согласно приложению 10.

1.11. Перечень сведений конфиденциального характера финансового управления администрации Арзгирского муниципального округа Ставропольского края согласно приложению 11.

1.12. Положение по работе с инцидентами информационной безопасности финансового управления администрации Арзгирского муниципального округа Ставропольского края согласно приложению 12.

1.13. Порядок оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края согласно приложению 13.

1.14. Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края согласно приложению 14.

 2. Признать утратившим силу приказ финансового управления администрации Арзгирского муниципального района Ставропольского края от 16 ноября 2015 года №179 «Об обработке и обеспечении безопасности персональных данных в информационных системах персональных данных финансового управления администрации Арзгирского муниципального района Ставропольского края».

3. Контроль за выполнение приказа оставляю за собой.

4. Приказ вступает в силу со дня его подписания.

Начальник финансового управления

администрации Арзгирского муниципального округа

Ставропольского края Н.Ю. Овсянникова

 Приложение 1

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

Положение

об обеспечении безопасности персональных данных при их

обработке в информационных системах персональных данных в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края

1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах персональных данных.

Персональные данные (далее – ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, субъекту ПДн.

Оператор ПДн – финансовое управление администрации Арзгирского муниципального округа Ставропольского края Ставропольского края (далее – управление), обеспечивающее защиту ПДн, при их обработке в информационных системах персональных данных(далее – ИСПДн).

2. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн.

Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (далее – СЗПДн) (в том числе шифровальные (криптографические), средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПДн информационные технологии. Технические и программные средства должны удовлетворять требованиям действующего законодательства.

3. ИСПДн классифицируются в зависимости от объема обрабатываемых ПДн и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации ИСПДн устанавливается в соответствии с действующим законодательством.

4. Обмен ПДн при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

5. Размещение ИСПДн производится в специальном оборудованном помещении, в котором обеспечивается сохранность носителей ПДн и СЗПДн, а также исключена возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

6. При обработке ПДн в ИСПДн должно быть обеспечено:

проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн, и (или) передачи их лицам, не имеющим права доступа к такой информации;

своевременное обнаружение фактов несанкционированного доступа к ПДн;

недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

постоянный контроль за обеспечением уровня защищенности ПДн.

7. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн включают в себя:

определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

разработку на основе модели угроз СЗПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

проверку готовности СЗПДн к использованию с составлением заключений о возможности их эксплуатации;

установку и ввод в эксплуатацию СЗПДн в соответствии с эксплуатационной и технической документацией;

обучение лиц, использующих СЗПДн, применяемые в ИСПДн, правилам работы с ними;

учет применяемых СЗПДн, эксплуатационной и технической документации к ним, носителей ПДн;

учет лиц, допущенных к работе с ПДн в ИСПДн;

контроль за соблюдением условий использования СЗПДн, предусмотренных эксплуатационной и технической документацией;

описание СЗПДн.

8. При обнаружении нарушений порядка предоставления ПДн пользователи ИСПДн незамедлительно приостанавливают предоставление ПДн до выявления причин нарушений и устранения этих причин.

9. Реализация требований по обеспечению безопасности информации в СЗПДн возлагается на их разработчиков.

10. СЗПДн, предназначенные для обеспечения безопасности ПДн при их обработке в ИСПДн, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется действующим законодательством.

 Приложение 2

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ИНСТРУКЦИЯ

администратора информационной безопасности информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края

# 1. Общие положения

1.1. Инструкция администратора информационной безопасности информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – Инструкция) определяет основные обязанности, права и ответственность администратора информационной безопасности информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее соответственно – администратор, управление).

1.2. Администратор назначается приказом начальника управления.

1.3. Администратор руководствуется требованиями нормативных правовых актов Российской Федерации и Ставропольского края, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

1.4. Администратор в пределах своих функциональных обязанностей обеспечивает работоспособность информационных систем персональных данных (далее – ИСПДн), безопасность информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (далее – СВТ) в ИСПДн управления.

1.5. Должностные лица, задействованные в обеспечении функционирования ИСПДн управления, могут быть ознакомлены с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

1.6. Администратор обязан в случае своего увольнения все носители защищаемой информации управления (рукописи, черновики, чертежи, диски, дискеты, распечатки с принтеров, модели, материалы, изделия и пр.), которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы в управлении, передать ответственному за защиту информации и персональных данных управления.

# 2. Должностные обязанности администратора

2.1. Администратор обязан:

знать перечень установленных в подразделениях управления СВТ и перечень задач, решаемых их использованием;

обеспечивать работоспособность СВТ ИСПДн управления, проводить организационно-технические мероприятия по их обслуживанию;

устанавливать и настраивать элементы ИСПДн и 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 ИСПДн управления;

выполнять своевременное обновление программного обеспечения элементов ИСПДн и системы защиты персональных данных (далее – СЗПДн) по мере появления таких обновлений;

выполнять резервное копирование и восстановление данных;

выявлять попытки несанкционированного доступа к защищаемым информационным ресурсам и техническим средствам ИСПДн управления;

настраивать СЗПДн, выполнять другие действия по изменению элементов ИСПДн;

периодически осуществлять тестирование всех функций СЗПДн с помощью тестовых программ, имитирующих попытки несанкционированного доступа, при изменении программной среды и персонала ИСПДн;

учитывать все защищаемые носители информации с помощью их любой маркировки и с занесением учетных данных в Журнал поэкземплярного учета средств защиты персональных данных, эксплуатационной и технической документации к ним, электронных носителей персональных данных, учтенные носители информации выдавать пользователям ИСПДн под роспись;

осуществлять текущий и периодический контроль работы СЗПДн;

осуществлять текущий контроль технологического процесса обработки ПДн;

в случае возникновения сбоев в работе технических средств немедленно докладывать начальнику управления;

участвовать в проведении служебных проверок фактов нарушения или угрозы нарушения безопасности ПДн;

проводить работы по восстановлению работоспособности СЗПДн;

проводить обучение пользователей ИСПДн правилам работы с СВТ и СЗПДн с отметкой в карточке проведения инструктажа по вопросам защиты информации по форме согласно приложению к настоящей Инструкции;

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

регулярно анализировать работу любых элементов ИСПДн, электронных системных журналов средств защиты для выявления и устранения неисправностей, а также для оптимизации ее функционирования.

# 3. Права администратора

3.1. Администратор имеет право:

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

в установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн;

требовать от пользователей ИСПДн соблюдения правил работы в ИСПДн, приведенных в Инструкции пользователя информационных систем персональных данных управления;

требовать от пользователей ИСПДн безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований внутренних документов управления, регламентирующих вопросы обеспечения безопасности и защиты информации;

обращаться к ответственному за защиту информации и ПДн управления с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования СЗПДн;

вносить предложения по совершенствованию функционирования ИСПДн управления;

осуществлять текущий контроль процесса обработки защищаемой информации на персональных электронных вычислительных машинах (далее – ПЭВМ) пользователей ИСПДн;

инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности в ИСПДн управления.

# 4. Ответственность администратора

4.1. Администратор несет ответственность:

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

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 управления в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

за бесперебойное и надлежащее функционирование ИСПДн и СЗПДн управления.

# 5. Ответственные за организацию и контроль

# выполнениЯ инструкции

5.1. Контроль за выполнением администратором настоящей Инструкции возлагается на начальника управления.

 Приложение 3

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ИНСТРУКЦИЯ

пользователя информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края

1. Общие положения

1.1. Инструкция пользователя информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – Инструкция) определяет основные обязанности, права и ответственность пользователя информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее соответственно – пользователь ИСПДн, управление).

1.2. Ознакомление пользователей ИСПДн с требованиями настоящей Инструкции проводит администратор информационной безопасности ИСПДн (далее – администратор) под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции, непосредственно для повседневного использования в работе.

2. Функции и обязанности пользователей

2.1. Каждый пользователь ИСПДн, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

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

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

исполнять требования Инструкции учета средств защиты, документации и электронных носителей персональных данных управления в части их касающейся, выполнять правила работы со средствами защиты информации, установленными в ИСПДн;

хранить в тайне свой пароль (пароли);

исполнять требования Порядка парольной защиты в информационных системах персональных данных управления, Инструкции по организации антивирусной защиты информационных систем персональных данных управления, а также других документов, регламентирующих вопросы работы в ИСПДн и обеспечение безопасности информации в части, его касающейся;

немедленно ставить в известность администратора и ответственного за защиту информации и персональных данных управления в случае утери личных реквизитов доступа или при подозрении на компрометацию личных паролей и на совершение попыток несанкционированного доступа к ПЭВМ, а также при обнаружении несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

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

присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним ПЭВМ в подразделении;

при обработке на ПЭВМ ПДн и необходимости использовать носители информации применять только учтенные носители, учет которых производится в соответствии с Порядком учета средств защиты, документации и электронных носителей персональных данных управления;

по окончании работы выключать ПЭВМ и извлекать носитель ключа средства защиты.

2.2. Пользователям ИСПДн запрещается:

использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

хранить и обрабатывать личную информацию на ПЭВМ и серверах ИСПДн;

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

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

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

использовать в работе неучтенные носители информации для обработки, ПДн;

передавать ПДн с ПЭВМ пользователя по электронной почте и размещать на сетевых ресурсах общего пользования;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты. Об обнаружении такого рода ошибок пользователь ИСПДн обязан ставить в известность администратора и ответственного за защиту информации и персональных данных управления.

# 3. Ответственные за организацию и контроль

# выполнениЯ инструкции

3.1. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех пользователей ИСПДн.

3.2. Ответственность за организацию контрольных и проверочных мероприятий возлагается на администратора.

3.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации и ПДн управления.

 Приложение 4

 к приказу финансового управления

 администрации Арзгирского

 муниципального района

 Ставропольского края

 № 82 от 03.02.2021 года

ПОРЯДОК

парольной защиты в информационных системах персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края

# 1. Общие положения

1.1. Порядок парольной защиты в информационных системах персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – Порядок) включает в себя взаимоувязанный комплекс организационно-технических мер, регламентирующих генерацию и/или выбор, использование, хранение, уничтожение парольной информации в информационных системах персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее соответственно – ИСПДн, управление).

1.2. Требования Порядка являются неотъемлемой частью комплекса мер безопасности и защиты информации в управлении.

1.3. Требования настоящего Порядка распространяются на всех должностных лиц и сотрудников управления, использующих в работе ИСПДн, а также всех видов программного обеспечения ИСПДн (далее – ПО), эксплуатируемого в управлении.

1.4. Ознакомление сотрудников управления, использующих в работе ИСПДн (далее – пользователи ИСПДн), с требованиями Порядка проводит администратор информационной безопасности ИСПДн (далее – администратор) под роспись в листе ознакомления с Порядком парольной защиты в информационных системах персональных данных управления по форме согласно приложению 1 к настоящему Порядку.

1.5. В целях закрепления знаний по вопросам практического исполнения требований Порядка, разъяснения возникающих вопросов администратор проводит (при необходимости) персональные инструктажи пользователей ИСПДн управления.

1.6. В случае невозможности исполнения требований Порядка в полном объеме при возникновении нештатных ситуаций, порядок парольной защиты в ИСПДн управления определяется администратором по согласованию с ответственным за защиту информации и персональных данных управления.

В целях настоящего Порядка под нештатными ситуациями, возникающими в процессе обработки ПДн следует понимать следующие: отказ, сбой, ошибка в работе технических средств, форс – мажорные обстоятельства.

# 2. Функции Администратора ИСПДн

2.1. Администратор обязан проводить:

регулярную смену используемой в работе парольной информации;

выбор парольной информации с качеством, установленным Порядком;

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

организацию доведения до пользователей ИСПДн управления требований по парольной защите;

организацию периодического и выборочного контроля исполнения пользователями ИСПДн требований настоящего Порядка;

техническое обеспечение (при наличии программно-технических средств) процессов генерации/выбора, смены и удаления паролей, соответствующей конфигурации ИСПДн.

# 3. Качество и обращение парольной информации

3.1. Пароли доступа к аппаратно-программным вычислительным средствам, информационным ресурсам организации формируются администратором с учетом требований к качеству парольной информации согласно приложению 2.

3.2. Хранение сотрудником (администратором, пользователем ИСПДн) личных паролей допускается в надежном месте (в сейфе, запираемом шкафу, ящике), либо в сейфе (запираемом шкафу, ящике).

3.3. Пользователи ИСПДн и администратор самостоятельно никому не имеют права сообщать и (или) передавать свои личные пароли и (или) дополнительные идентификаторы (электронные ключи), за исключением своих непосредственных руководителей в случае производственной необходимости и (или) при проведении контрольно-проверочных мероприятий. По окончании производственных и (или) контрольно-проверочных работ администратор производит немедленную смену значений раскрытых паролей.

3.4. Внеплановая смена/удаление пароля (и при возможности учетной записи) пользователя ИСПДн или администратора 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 администратора.

3.6. Администратор по согласованию с ответственным за защиту информации и ПДн управления проводит ежеквартальный выборочный контроль выполнения сотрудниками управления требований Порядка с отметками в журнале контроля выполнения сотрудниками управления Порядка парольной защиты в информационных системах персональных данных управления по форме согласно приложению 3.

#

# 4. Обращение дополнительных идентификаторов

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

4.2. Дополнительные идентификаторы выдаются и учитываются в соответствии с Инструкцией по наделению пользователей информационных систем персональных данных уникальными учетными записями и правами доступа к ресурсам информационных систем персональных данных управления.

4.3. Пользователи ИСПДн, 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 пользователи ИСПДн немедленно ставят об этом в известность администратора и ответственного за защиту информации и персональных данных управления. Администратор организует немедленную блокировку утерянных ключей в ИСПДн.

# 5. Ответственные за организацию и контроль

# выполнениЯ порядка

5.1. Ответственность за соблюдение требований Порядка возлагается на пользователей ИСПДн и администратора.

5.2. Ответственность за организацию контрольных и проверочных мероприятий по соблюдению пользователями вопросов парольной защиты возлагается на администратора.

5.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации и ПДн управления.

 Приложение 5

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

Инструкция

по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края

# 1. Общие положения

1.1. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – Инструкция) включает в себя описание взаимоувязанного комплекса организационно-технических мер по проведению работ по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных (далее – ИСПДн).

1.2. Требования настоящей Инструкции распространяются на всех сотрудников финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – управление), использующих в работе ИСПДн (далее – пользователи ИСПДн).

1.3. Пользователи ИСПДн знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

1.4. Ознакомление с требованиями Инструкции пользователей ИСПДн осуществляет администратор информационной безопасности ИСПДн (далее – администратор) под роспись в листе ознакомления с инструкцией по установке, модификации и техническому обслуживанию программного и аппаратных средств систем персональных данных управления по форме согласно приложению 1 с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

1.5. В случае невозможности исполнения требований Инструкции в полном объеме при возникновении нештатных ситуаций, порядок установки, модификации и технического обслуживания программного обеспечения и аппаратных средств систем персональных данных управления определяется администратором по согласованию с начальником управления.

В целях настоящей Инструкции под нештатными ситуациями, возникающими в процессе установки, модификации и технического обслуживания программного обеспечения и аппаратных средств систем персональных данных следует понимать следующие: отказ, сбой, ошибка в работе технических средств, форс - мажорные обстоятельства.

# 2. Порядок проведения работ

2.1. Все изменения конфигурации технических и программных средств автоматизированных рабочих мест ИСПДн (далее – рабочих станций) управления должны производиться в соответствии с действующим законодательством.

2.2. Все изменения конфигурации технических и программных средств серверов, входящих в состав ИСПДн управления, должны производиться только по согласованию с начальником управления.

2.3. Все изменения конфигурации технических и программных средств рабочих станций и серверов (далее – объекты информатизации), входящих в состав ИСПДн управления, отражаются в Техническом паспорте объекта информатизации согласно приложению 2. Запрещается изменение состава, в том числе ввод новых программных средств, осуществляющих обработку персональных данных (далее – ПДн) на объектах информатизации, аттестованных по требованиям безопасности информации.

2.4. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций ИСПДн управления предоставляется администратору.

2.5. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме администратора, запрещено.

2.6. Установка и настройка программного средства осуществляется администратором согласно эксплуатационной документации.

2.7. Запрещается установка и использование на персональных электронных вычислительных машинах (далее – ПЭВМ) (серверах) программного обеспечения (далее – ПО), не связанного с выполнением должностных обязанностей.

2.8. Установка (обновление) ПО (системного, тестового и т.п.) на рабочих станциях и серверах производится с эталонных копий программных средств, хранящихся у администратора. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода в соответствии с Инструкцией по организации антивирусной защиты информационных систем персональных данных управления.

2.9. После установки (обновления) ПО администратор должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями разработчика ПО и совместно с пользователем ПЭВМ проверить правильность настройки средств защиты.

2.10. В случае обнаружения недекларированных (не описанных в документации) возможностей программного средства, пользователи ИСПДн немедленно докладывают ответственного за защиту информации и персональных данных управления и администратору. Использование программного средства до получения специальных указаний запрещается.

2.11. При изъятии ПЭВМ из состава рабочих станций, обрабатывающих ПДн, ее передача на склад, в ремонт или в другое подразделение для решения иных задач, осуществляется только после того, как администратор снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом затирания информации по форме согласно приложению 3 за подписью администратора.

2.12. Допуск новых пользователей к решению задач с использованием вновь развернутого ПО (либо изменение их полномочий доступа) осуществляется согласно Инструкции по наделению пользователей информационных систем персональных данных уникальными учетными записями и правами доступа к ресурсам информационных систем персональных данных управления.

2.13. Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств ПЭВМ с отметками о внесении изменений в состав аппаратно-программных средств, хранятся у администратора.

#  3. Ответственные за организацию и контроль

# выполнениЯ инструкции

 3.1. Ответственность за соблюдение требований Инструкции возлагается на пользователей ИСПДн и администратора управления.

 3.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на администратора.

 3.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации и персональных данных управления.

 Приложение 6

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 179 от 16.11.2015 года

ИНСТРУКЦИЯ

 по наделению пользователей информационных систем персональных данных

уникальными учетными записями и правами доступа к ресурсам информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края

# 1. Общие положения

1.1. Инструкция по наделению пользователей информационных систем персональных данных уникальными учетными записями и правами доступа к ресурсам информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее соответственно – Инструкция, управление) устанавливает порядок использования учетных записей пользователей информационной системы персональных данных (далее – ИСПДн) и порядок предоставления пользователям прав доступа к ИСПДн.

1.2. Сотрудники управления, допущенные к работе в ИСПДн (далее – пользователи ИСПДн), назначенные приказом начальника управления, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

1.3. Ознакомление с требованиями Инструкции пользователей ИСПДн осуществляет администратор информационной безопасности ИСПДн (далее – администратор) под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

1.4. В случае невозможности исполнения требований Инструкции в полном объеме при возникновении нештатных ситуаций, порядок наделения пользователей ИСПДн уникальными учетными записями и правами доступа к ресурсам ИСПДн управления определяется администратором по согласованию с ответственным за защиту информации и ПДн управления.

В целях настоящей Инструкции под нештатными ситуациями следует понимать следующие: отказ, сбой, ошибка в работе технических средств, форс – мажорные обстоятельства.

# 2. Порядок использования учетных записей

# пользователей ИСПДн

2.1. С целью соблюдения принципа персональной ответственности за свои действия, каждому пользователю ИСПДн, допущенному к работе с ИСПДн, назначается персональное уникальное имя (учетная запись пользователя), под которым он регистрируется и работает в системе.

2.2. В случае производственной необходимости пользователям ИСПДн назначается несколько уникальных имен (учетных записей).

2.3. Использование несколькими пользователями ИСПДн при самостоятельной работе в ИСПДн одного и того же имени пользователя ("группового имени") запрещено.

2.4. Использование пользователем ИСПДн имени пользователя, сопоставленного с другим пользователем ИСПДн (учетной записи другого сотрудника), при работе в ИСПДн запрещено.

# 3. Порядок предоставления пользователям прав

# доступа к ИСПДН

3.1. Процедура регистрации (создания учетной записи) пользователя ИСПДн и предоставления (изменения) ему прав доступа к ресурсам ИСПДн инициируется приказом управления.

 3.2. На основании приказа управления, администратор:

создает учетную запись;

производит изменение прав доступа учетной записи;

осуществляет блокирование учетной записи.

3.3. При предоставлении пользователю ИСПДн прав доступа к ресурсам необходимо руководствоваться принципом предоставления минимальных прав для решения требуемых задач.

3.4. Начальники отделов управления несут ответственность за минимальную достаточность прав доступа, имеющихся у пользователей ИСПДн отделов. В случае наличия у пользователей ИСПДн избыточных для работы прав доступа начальники отделов ставят об этом в известность администратора, который вносит необходимые изменения в соответствии с настоящей Инструкцией.

3.5. Документирование прав доступа производится в электронном виде, для чего создается специальная база данных прав пользователей ИСПДн, в которой указываются следующие данные:

ФИО пользователя;

отдел;

учетная запись;

контролируемый ресурс;

права доступа;

отметка об удалении учетной записи при увольнении.

3.7. Изменения в конфигурации механизмов защиты информации производятся только администратором и только в соответствии с документацией на средства защиты персональных данных.

# 4. Ответственные за организацию и контроль

# выполнениЯ ИНСТРУКЦИИ

4.1. Ответственность за соблюдение требований Инструкции возлагается на пользователей ИСПДн, назначаемых приказом управления.

4.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам управления правами пользователей ИСПДн возлагается на администратора, назначаемого приказом управления.

4.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации и персональных данных управления.

 Приложение 7

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ИНСТРУКЦИЯ

по организации антивирусной защиты информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края

# 1. Общие положения

1.1. Инструкция по организации антивирусной защиты информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – Инструкция) определяет требования к организации защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО) и устанавливает ответственность сотрудников финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – управление), эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. Требования настоящей Инструкции распространяются на всех сотрудников управления, использующих в работе ИСПДн (далее – пользователи ИСПДн) управления.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, а также для разъяснения возникающих вопросов администратором информационной безопасности ИСПДн (далее – администратор) проводятся инструктажи (при необходимости) пользователей ИСПДн.

1.4. Доведение Инструкции до пользователей ИСПДн, в части их касающейся, осуществляется администратором под роспись в листе ознакомления с Инструкцией по организации антивирусной защиты информационных систем персональных данных управления по форме согласно приложению 1.

1.5. В случае невозможности исполнения требований Инструкции в полном объеме при возникновении нештатных ситуаций, порядок организации антивирусной защиты информационных систем персональных данных управления определяется администратором по согласованию с ответственным за защиту информации и ПДн управления.

В целях настоящей Инструкции под нештатными ситуациями следует понимать следующие: отказ, сбой, ошибка в работе технических средств, форс - мажорные обстоятельства.

# 2. Применение средств антивирусной защиты

2.1. Антивирусный контроль дисков и файлов ИСПДн после загрузки персональных электронных вычислительных машин (далее – ПЭВМ) должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.2. Полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование) должен проводиться не реже одного раза в неделю.

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, 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. Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств управления.

2.5. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем один раз в неделю.

# 3. Функции Администратора по обеспечению антивирусной безопасности

3.1. Администратор обязан:

проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты;

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

предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов;

производить обновление антивирусных баз;

проводить работы по обнаружению и обезвреживанию вредоносного ПО в ИСПДн управления;

контролировать наличие вредоносного ПО на ПЭВМ пользователей ИСПДн, путём просмотра логов работы сервера антивирусной защиты;

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

осуществлять периодический контроль за соблюдением пользователями ИСПДн требований Инструкции.

# 4. Функции пользователей

Пользователи ИСПДн:

4.1. При возникновении подозрения на наличие вредоносного ПО (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИСПДн должен провести внеочередной антивирусный контроль ПЭВМ. При необходимости он должен привлечь администратора для определения факта наличия или отсутствия вредоносного ПО.

4.2. В случае обнаружения при проведении антивирусной проверки зараженных вредоносным ПО файлов сотрудники подразделений обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за защиту информации и персональных данных управления и администратора;

привлечь администратора для проведения лечения или уничтожения зараженных файлов;

по факту обнаружения зараженных вирусом файлов составить служебную записку администратору, в которой необходимо указать предположительный источник (отправителя, владельца) зараженного файла.

# 5. Ответственные за организацию и контроль

# выполнениЯ инструкции

5.1. Ответственность за соблюдение требований Инструкции возлагается на пользователей ИСПДн и администратора, в части их касающейся.

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

5.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации и персональных данных управления.

 Приложение 8

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ИНСТРУКЦИЯ

по резервному копированию защищаемой информации в информационных системах персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края

# 1. Общие положения

1.1. Инструкция по резервному копированию защищаемой информации в информационных системах персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – Инструкция) определяет порядок резервного копирования информационных ресурсов информационных систем персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее соответственно – ИСПДн, управление).

1.2. Процесс резервного копирования обеспечивает сохранение на резервных носителях информации с целью ее восстановления при потере или порче на основном носителе и является ключевым элементом защиты от умышленной и неумышленной потери данных.

1.3. Конкретные информационные ресурсы, подлежащие резервному копированию, определяются администратором информационной безопасности ИСПДн управления (далее – администратор).

1.4. Резервное копирование осуществляется администратором и контролируется ответственным за защиту информации и персональных данных управления.

1.5. Сотрудники управления, задействованные в осуществлении резервного копирования информационных ресурсов ИСПДн управления, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

# 2. Периодичность и схема резервного копирования

2.1. При осуществлении резервного копирования используются два типа копирования: полное резервное копирование и инкрементальное резервное копирование.

2.2. Резервное копирование информационных ресурсов ИСПДн управления осуществляется по трехуровневой схеме ротации.

2.3. В соответствии с трехуровневой схемой ротации:

полное резервное копирование информационных ресурсов выполняется 15-16 числа каждого месяца, архив хранится в течение года и является архивом Уровня 1;

полное резервное копирование информационных ресурсов выполняется в конце каждой недели (в пятницу), архив хранится в течение календарного месяца и является архивом Уровня 2;

полное резервное копирование информационных ресурсов выполняется в начале каждой недели (утром в понедельник), затем ежедневно на эту копию выполняется инкрементальное копирование, архив хранится в течение недели и является архивом Уровня 3.

# 3. Порядок резервного копирования

3.1. Администратор настраивает задания для программного обеспечения, осуществляющего резервное копирование, на автоматическое выполнение в соответствии с перечнем информационных ресурсов, подлежащих резервному копированию, и графиком резервного копирования.

3.2. Перед выполнением задания резервного копирования администратор проверяет доступность резервного носителя, а также наличие на нем свободного места для записи данных.

3.3. После завершения выполнения задачи резервного копирования администратор должен извлечь резервный носитель и поместить в сейф.

# 4. Хранение резервных копий

4.1. Хранение резервных копий должно быть организовано в отдельном от копируемых информационных ресурсов помещении, оснащенном соответствующими системами вентиляции, кондиционирования и отопления для поддержки требуемых параметров температуры, влажности и т.п.

4.2. Резервные носители должны храниться в кассетах или закрытых коробках на безопасном расстоянии от источников магнитных полей: блоков питания, телефонов, мониторов и т.п.

4.3. Доступ к хранилищу резервных копий должны иметь только администратор и ответственный за защиту информации и персональных данных, назначенные приказом управления.

5. Восстановление ИСПДН после сбоя

5.1. В случае потери данных на основном носителе из хранилища извлекается накопитель с резервной копией информационных ресурсов, нуждающихся в восстановлении, последнего произведенного резервного копирования.

5.2. В зависимости от характера и уровня повреждения информационных ресурсов, администратор восстанавливает либо весь массив резервных данных, либо отдельные поврежденные или уничтоженные файлы и папки.

# 6. Ответственные за организацию и контроль

# выполнениЯ инструкции

6.1. Ответственность за выполнение резервного копирования и восстановление данных из резервных копий, а также за соблюдение периодичности и порядка выполнения резервного копирования и сохранность резервных копий, возлагается на администратора.

6.2. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации и персональных данных управления.

 Приложение 9

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ИНСТРУКЦИЯ

доступа в помещения с компонентами информационных систем персональных данных в здании финансового управления администрации Арзгирского муниципального округа Ставропольского края

# 1. Общие положения

1.1. Инструкция доступа в помещения с компонентами информационных систем персональных данных в здании финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – Инструкция) определяет порядок доступа в помещения, в которых располагаются автоматизированные рабочие места, серверы, сетевое оборудование (далее – компоненты) информационных систем персональных данных (далее – ИСПДн), находящиеся в здании финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – управление), расположенном по адресу: ул. П.Базалеева, зд. 7, с.Арзгир, 356570.

1.2. Выполнение требований Инструкции обязательно для всех сотрудников управления, использующих в работе ИСПДн (далее – пользователи ИСПДн).

1.3. Ознакомление сотрудников, использующих в работе ИСПДн управления, с требованиями Инструкции проводит администратор информационной безопасности ИСПДн (далее – администратор).

#

# 2. Техническое обеспечение защиты помещений

2.1. Помещения, в которых располагаются компоненты ИСПДн (далее – Помещения), должны быть оборудованы:

 надежными механическими замками;

 списками пользователей ИСПДн, имеющих право самостоятельно находиться в помещении (далее – Списки).

2.2. Помещения, в которых располагается серверное, сетевое оборудование, должны быть дополнительно снабжены оборудованием подсистемы межсетевого экранирования и кодовыми замками. Список Помещений составляется администратором, по форме согласно приложению 1 к настоящей Инструкции.

2.3. Администратор обеспечивает каждого пользователя ИСПДн ключом от Помещения. Учет ключей от Помещения производится в Журнале учета ключей помещения с автоматизированными рабочими местами ИСПДн согласно приложению 2. Ключ выдается под роспись в Журнале учета ключей помещения с автоматизированными рабочими местами ИСПДн.

2.4. Запасной комплект ключей находится у ответственного за защиту информации и персональных данных управления.

2.5. Списки составляются администратором и утверждаются начальником управления по форме согласно приложению 3 к настоящей Инструкции. В Списки вносятся только те сотрудники управления, право самостоятельного нахождения в Помещении которых обусловлено производственной необходимостью.

2.12. Списки вывешиваются в Помещении.

#

# 3. Режим доступа в помещения

3.1. Пользователи ИСПДн имеют право самостоятельно открывать и закрывать Помещения.

3.2. Пользователи ИСПДн имеют право самостоятельно открывать, закрывать Помещения, в которых располагается серверное, сетевое оборудование.

3.3. Лица, не имеющие доступа, могут находиться в Помещениях только в присутствии пользователей ИСПДн.

3.4. В течение рабочего дня пользователи ИСПДн обязаны:

 при покидании последними Помещений, закрывать двери Помещения на замок;

 не покидать Помещение, если в нем находятся посторонние лица;

 при обнаружении фактов нарушения режима доступа в Помещение ставить в известность администратора и ответственного за защиту информации и персональных данных управления;

при утере ключа от Помещения ставить в известность администратора и ответственного за защиту информации и персональных данных управления;

 при посещении Помещений посторонними лицами с целями проведения контрольных, проверочных мероприятий, а также работ по обслуживанию Помещений и инженерно-технических средств, находящихся в них, ставить в известность об этом администратора и ответственного за защиту информации и персональных данных управления.

3.5. Запрещается вынос из здания управления документов, электронных или иных носителей персональных данных, а также их передача лицам, не допущенным к обработке персональных данных, без согласования с начальником управления.

# 4. Смена кодов и ключей

4.1. При утере одного из комплектов ключей от Помещений, начальник управления инициирует служебное расследование, по результатам которого принимается решение об изготовлении дополнительного комплекта ключей или замене всех комплектов ключей на новые.

4.2. Смена кодов доступа и секретов замков в Помещениях организуется начальником управления в следующих случаях:

 увольнение или перемещение из состава отдела сотрудника, знавшего код доступа в Помещение или имеющего доступ к ключам от Помещения;

 преднамеренное или непреднамеренное разглашение кода доступа в Помещения посторонним лицам;

 установленный факт бесконтрольного нахождения в Помещении посторонних лиц;

 истечение одного календарного года с момента первичного ввода или последней смены значения кода доступа.

# 5. Ответственные за организацию и контроль

# выполнениЯ инструкции

5.1. Ответственность за своевременное доведение Инструкции до сотрудников управления в части их компетенции и обеспечение условий для выполнения требований данной Инструкции возлагается на администратора.

5.3. Ответственность за организацию технического обеспечения защиты Помещений несет начальник управления.

5.4. Администратор проводит текущий контроль выполнения сотрудниками управления требований Инструкции.

5.5. Ответственность за организацию контрольных и проверочных мероприятий по вопросам доступа в Помещения возлагается на ответственного за защиту информации и персональных данных управления.

 Приложение 10

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ИНСТРУКЦИЯ

учета средств защиты, документации и электронных носителей персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция учета средств защиты, документации и электронных носителей персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – Инструкция) устанавливает:

порядок учета и хранения средств защиты персональных данных (далее – СЗПДн);

порядок учета носителей персональных данных (далее – ПДн);

порядок хранения носителей ПДн.

1.2. Требования Инструкции распространяются на всех сотрудников финансового управления администрации Арзгирского муниципального округа Ставропольского края (далее – управление), использующих в работе информационные системы персональных данных (далее – ИСПДн, пользователи ИСПДн).

1.3. Администратор информационной безопасности ИСПДн управления (далее – администратор) осуществляет ознакомление пользователей ИСПДн с требованиями настоящей Инструкции под роспись в листе ознакомления с Инструкцией учета средств защиты, документации и электронных носителей персональных данных финансового управления администрации Арзгирского муниципального округа Ставропольского края по форме согласно приложению 1 к Инструкции.

#

# 2. Порядок учета и хранения средств защиты персональных данных

2.1. Используемые или хранимые СЗПДн, эксплуатационная и техническая документация к ним подлежат поэкземплярному учету. При этом программные СЗПДн должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СЗПДн подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СЗПДн учитываются также совместно с соответствующими аппаратными средствами.

2.2. Все полученные экземпляры СЗПДн, эксплуатационной и технической документации к ним должны быть выданы под расписку в Журнале поэкземплярного учета средств защиты персональных данных, эксплуатационной и технической документации к ним, электронных носителей персональных данных (далее – Журнал) согласно приложению 2 пользователям ИСПДн.

2.3. Эксплуатационная и техническая документация, а также электронные носители с инсталляционными файлами СЗПДн должны содержаться в хранилищах (шкафах, ящиках, сейфах и др.), исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.4. Аппаратные средства, с которыми осуществляется штатное функционирование СЗПДн, должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) должно быть таким, чтобы его можно было визуально контролировать.

2.5. СЗПДн изымаются из пользования администратором по согласованию с ответственным за защиту информации и ПДн управления. При этом вносятся необходимые изменения в Журнал, Технический паспорт ИСПДн, в составе которой эксплуатировались изъятые из употребления СЗПДн. Если эксплуатация СЗПДн, намеченных к изъятию из употребления, происходит в составе аттестованной ИСПДн, о прекращении эксплуатации СЗПДн необходимо уведомить организацию, производившую аттестацию данной ИСПДн. При этом СЗПДн считаются изъятыми из употребления, если исполнена предусмотренная эксплуатационной и технической документацией процедура удаления программного обеспечения СЗПДн и они полностью отсоединены от аппаратных средств.

# 3. Порядок учета Электронных носителей с ПДН

3.1. В отделах управления, работающих с ИСПДн, учет носителей для записи ПДн осуществляется администратором.

3.2. Ответственным за учет носителя информации с ПДн является администратор.

3.3. Учет и движение (выдача и возврат) носителей ПДн производится в Журнале.

3.4. Выдача носителей пользователю ИСПДн производится под его личную роспись в Журнале.

3.5. Носители для записи ПДн выдаются только пользователям ИСПДн, назначенным приказом управления.

3.6. После окончания работы с носителем ПДн пользователи ИСПДн обязаны удалить информацию с носителя и вернуть его администратору.

4. Порядок хранения электронных носителей ПДН

4.1. Носители с ПДн должны храниться в служебных помещениях в запираемых шкафах. При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

4.2. Запрещается выносить носители с ПДн из служебных помещений для работы с ними на дому, в гостиницах и т.д. В необходимых случаях начальник управления может разрешить исполнителям вынос из управления носителей с ПДн для их согласования, подписания и т.п.

4.3. Пользователь ИСПДн, получивший носитель с ПДн у администратора, несет ответственность за сохранность ПДн, находящихся на носителе ПДн.

#

# 5. Ответственные за организацию и контроль

# выполнениЯ инструкции

5.1. Ответственность за соблюдение требований настоящей Инструкции возлагается на пользователей ИСПДн и администратора.

5.2. Ответственность за организацию контрольных и проверочных мероприятий возлагается на администратора.

5.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации и ПДн управления.

 Приложение 11

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ПЕРЕЧЕНЬ

сведений конфиденциально характера финансового управления администрации Арзгирского муниципального округа Ставропольского края

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях:

1.1. Сведения о фактах, событиях и обстоятельствах жизни муниципальных служащих (работников) финансового управления администрации Арзгирского муниципального округа Ставропольского края, позволяющие идентифицировать их личность и содержащиеся в личном деле муниципального служащего (работника) либо подлежащие включению в личное дело, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

1.2. Сведения, содержащие персональные данные, обрабатываемые в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края, в рамках реализации его функций и полномочий.

2. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

2.1. Сведения, содержащиеся в служебных документах в части, не содержащей сведения, составляющих государственную тайну, в том числе полученных из сторонних организаций, государственных органов и органов местного самоуправления, а также сведения, образующиеся в деятельности финансового управления администрации Арзгирского муниципального округа Ставропольского края, ограничение на распространение которых диктуется служебной необходимостью, за исключением сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.

2.2. Сведения о платежах в соответствующие бюджеты бюджетной системы Российской Федерации и об их плательщиках, являющиеся информацией ограниченного доступа.

2.3. Сведения, содержащиеся в заявках, поданных в форме электронных документов на участие в открытом конкурсе.

2.4. Сведения об организации разграничения доступа к информационным ресурсам финансового управления администрации Арзгирского муниципального округа Ставропольского края, паролях, закрытых ключах электронной подписи, ключах шифрования информации, за исключением сведений, составляющих государственную тайну.

 Приложение 12

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ПОЛОЖЕНИЕ

по работе с инцидентами информационной безопасности

финансового управления администрации Арзгирского муниципального округа Ставропольского края

1. Общие положения

Положение о работе с инцидентами информационной безопасности (далее - Положение) разработано в соответствии с:

1. Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ).

2. Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119.

4. Требованиями по реализации мер, предусмотренных составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждёнными приказом ФСТЭК России от 18 февраля 2013 года № 21;

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов и информационных систем.

Работа с инцидентами включает в себя следующие направления:

1. определение лиц, ответственных за выявление инцидентов и реагирование на них;

2. обнаружение, идентификация и регистрация инцидентов;

3. своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

4. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценка их последствий;

5. принятие мер по устранению последствий инцидентов;

6. планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий, планирования и принятия мер по предотвращению повторного возникновения инцидентов, назначается постоянно действующая комиссия по работе с инцидентами в соответствии с приказом начальника финансового управления администрации Арзгирского муниципального округа Ставропольского края.

 2. Ответственные за выявление инцидентов и реагирование на них

 2.1. В информационных системах.

 Ответственными за выявление инцидентов в ИС являются:

 1.лица, имеющие право доступа к ИС;

 2. администратор информационной безопасности ИС.

Ответственными за реагирование на инциденты в ИС являются:

 1. лица, имеющих право доступа к ИС;

 2. руководитель отдела управления, в котором выявлен инцидент;

 3. администратор информационной безопасности ИС;

 4. ответственный за защиту информации и персональных данных;

 5. ответственный за организацию обработки персональных данных управления, в случае, если ИС является информационной системой персональных данных (далее - ИСПДн);

1. председатель комиссии по работе с инцидентами.

 Вне информационных систем.

Ответственными за выявление инцидентов вне ИС являются все сотрудники финансового управления.

Ответственными за реагирование на инциденты вне ИС являются:

1. сотрудник управления, обнаруживший инцидент;

2. руководитель отдела управления, в котором выявлен инцидент;

3. ответственный за организацию обработки персональных данных управления, в случае, если существует угроза безопасности персональных данных;

4. ответственный за защиту информации и персональных данных;

1. председатель комиссии по работе с инцидентами.

3. Обнаружение, идентификация и регистрация инцидентов

* 1. Работа по обнаружению инцидентов в области информационной

безопасности включает в себя мероприятия, направленные на:

1. выявление инцидентов в области информационной безопасности с помощью технических средств;

2. выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

3. выявление инцидентов с помощью сотрудников управления.

3.2. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до сотрудников управления информации, позволяющей идентифицировать инциденты.

3.3. Регистрацию инцидентов осуществляет Председатель комиссии по работе с инцидентами в журнале регистрации инцидентов информационной безопасности. Форма журнала утверждается приказом начальника управления.

Хранение журнала осуществляется в местах, исключающих доступ к журналу посторонних лиц. Ответственный за хранение ведение и хранение журнала - Председатель комиссии по работе с инцидентами.

4. Информирование о возникновении инцидентов

Сотрудник управления (пользователь ИС), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, администратору информационной безопасности ИС, ответственному за защиту информации и персональных данных, ответственному за организацию обработки персональных данных управления (в случае если ИС является ИСПДн), председателю комиссии по работе с инцидентами.

Администратор информационной безопасности ИС, в случае необходимости, информирует пользователей ИС о возникновении инцидента и дает указания по дальнейшим действиям.

5. Анализ инцидентов, а также оценка их последствий

Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий осуществляет комиссия по работе с инцидентами информационной безопасности.

* 1. Источниками и причинами возникновения инцидентов в области

информационной безопасности являются:

1. действия организаций и отдельных лиц враждебные интересам управления;

 2. отсутствие персональной ответственности сотрудников управления и его руководителя за обеспечение информационной безопасности, в том числе персональных данных;

3. недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе персональных данных;

4. отсутствие дисциплинарной мотивации соблюдения правил и требований информационной безопасности;

5. недостаточная техническая оснащённость работников, ответственных за обеспечение информационной безопасности;

 6. совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;

7. наличие привилегированных бесконтрольных пользователей в информационной системе;

 8. пренебрежение правилами и требованиями информационной безопасности сотрудниками управления;

 9. и другие причины.

5.2. Оценка последствий инцидента производится на основании потенциально возможного или фактического ущерба.

6. Принятие мер по устранению последствий инцидентов

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

1. определение границ инцидента и ущерба от реализации угроз информационной безопасности;

1. ликвидацию последствий инцидента и полное либо частичное

возмещение ущерба.

7. Планирование и принятие мер по предотвращению инцидентов

 7.1. Планирование и принятие мер по предотвращению возникновения инцидентов осуществляет комиссия по работе с инцидентами информационной безопасности и основывается на:

 1. Планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками управления;

 2. проведении мероприятий по обучению сотрудников управления правилам и способам работы со средствами защиты информационных систем;

 3. доведении до сотрудников норм законодательства, внутренних документов управления, устанавливающих ответственность за нарушение требований информационной безопасности;

 4. разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимаемыми на работу;

 5. своевременной модернизации системы обеспечения информационной безопасности, с учетом возникновения новых угроз информационной безопасности, либо в случае изменения требований руководящих документов по организации обеспечения информационной безопасности;

 6. своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом.

Как правило, самым слабым звеном в любой системе безопасности является человек. Поэтому работа с персоналом является основным направлением деятельности по обеспечению требований информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

 Приложение 13

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ПОРЯДОК

оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края

1.ОБЩИЕ ПОЛОЖЕНИЯ

В соответствии с пп.4 п. 2 статьи 19 Федерального закона «О персональных данных» обеспечение безопасности персональных данных (ПДн) достигается, в том числе, проведением «оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных (ИСПДн)».

Оценка эффективности может проводиться в формах добровольной аттестации по требованиям безопасности информации в системе сертификации ФСТЭК России, а также в других формах, выбираемых оператором ПДн (приемо-сдаточных испытаний СЗПДн, совместной оценки комиссией, состоящей из представителей Разработчика и Заказчика СЗПДн, и т. д.).

При проведении оценки эффективности принимаемых мер по обеспечению безопасности ПДн необходимо осуществить оценку соответствия ИСПДн организационно-техническим требованиям по безопасности информации и провести испытания средств и систем защиты ИСПДн на соответствие требованиям по защищенности ПДн от угроз безопасности ПДн.

2. РАЗРАБОТКА ПРОГРАММЫ ОЦЕНКИ

2.1. Процесс проведения оценки эффективности осуществляется на основании программы оценки, в которой отражается:

 - описание объекта оценки;

 - порядок проведения оценки;

 - перечень процедур оценки;

 - требования к содержанию проверок и испытаний;

 - критерии оценки, характеризующей успешное прохождение проверок и испытаний.

3. ПРОЦЕДУРА ОЦЕНКИ

3.1. Оценка соответствия ИСПДн организационно-техническим требованиям по защите ПДн может включать в себя:

 - анализ структуры ИСПДн и технологического процесса обработки информации;

 - оценку достаточности разработанных внутренних нормативных актов и соответствия их содержания требованиям по безопасности информации;

 - оценку правильности выбора уровней защищенности ПДн и мер защиты;

 - оценку соответствия состава и структуры программно-технических средств ИСПДн представленной документации;

 - оценку состояния организации работ и выполнения организационно-технических требований по защите информации;

 - оценку достаточности мер физической охраны технических средств информационной системы;

 - оценку уровня подготовки кадров и распределения ответственности персонала.

 3.2. Испытания ИСПДн на соответствие требованиям по защищенности ПДн от угроз безопасности ПДн могут проводиться в следующей последовательности (в зависимости от состава подсистем и средств защиты):

 - наличие необходимой проектной, рабочей и эксплуатационной документации;

 - оценка соответствия проектной документации состава и структуры программно­технических средств СЗПДн;

 - оценка выполнения требований формуляров СЗИ и СКЗИ, правил эксплуатации СЗИ и СКЗИ и условий действия сертификатов;

 - испытания подсистемы управления доступом;

 - испытания подсистемы регистрации и учета;

 - испытания подсистемы обеспечения целостности;

 - испытания подсистемы антивирусной защиты;

 - испытания подсистемы анализа защищенности;

 - испытания подсистемы обнаружения вторжений;

 - испытания подсистемы межсетевого экранирования;

 - испытания подсистемы защиты каналов связи (в том числе криптографическими средствами);

 - испытания защищенности комплекса программно-технических средств ИСПДн в целом, в том числе с использованием сканеров безопасности.

 3.3. Принятие мер в случае выявления несоответствия ИСПДн установленным требованиям по защите информации в себя включает:

 - доработку организационно-распорядительной документации;

 - исключение отдельных средств из состава ИСПДн;

 - внесение дополнительных настроек в СЗПДн и изменение рабочей и эксплуатационной документации;

 - применение дополнительных организационно-технических мер защиты;

 - применение дополнительных сертифицированных средств защиты информации.

 3.4. Оформление заключения по результатам оценки.

По результатам оценки оформляется заключение. К заключению прилагаются протоколы оценки, подтверждающие полученные при оценке результаты и обосновывающие приведенный в заключении вывод. Протоколы испытаний подписываются экспертами - членами комиссии по оценке, проводившими испытания.

 Приложение 14

 к приказу финансового управления

 администрации Арзгирского

 муниципального округа

 Ставропольского края

 № 82 от 03.02.2021 года

ПРАВИЛА

оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края

1. ОБЩИЕ ПОЛОЖЕНИЯ
	1. Настоящие Правила оценки возможного вреда субъектам персональных данных и принятия мер по его предотвращению (далее - Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ «О персональных данных» (далее - № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных № 152-ФЗ.
	2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.
2. ОСНОВНЫЕ ПОНЯТИЯ
	1. В настоящих Правилах используются основные понятия:
		1. Информация - сведения (сообщения, данные) независимо от формы их представления.
		2. Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.
		3. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
		4. Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.
		5. Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.
		6. Убытки - расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.
		7. Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.
		8. Оценка возможного вреда - определение уровня вреда на основании учёта причинённых убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.
3. МЕТОДИКА ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ
	1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
	2. Перечисленные неправомерные действия определяются как, следующие нарушения безопасности информации:
		1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных.
		2. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных.
		3. Неправомерное изменение персональных данных является нарушением целостности персональных данных.
		4. Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации.
		5. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных.
		6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных.
		7. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных.
		8. Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.
	3. Субъекту персональных данных может быть причинён вред в форме:
		1. Убытков - расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.
		2. Морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.
	4. При оценке возможного вреда финансовое управление администрации Арзгирского муниципального района Ставропольского края исходит из следующего способа учёта последствий допущенного нарушения принципов обработки персональных данных:
		1. Низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;
		2. Средний уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;
		3. Высокий уровень возможного вреда - во всех остальных случаях.

4.ПОРЯДОК ПРОВЕДЕНИЯ ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА

 4.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края за организацию обработки персональных данных, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведённых в Приложении.

 4.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», определяется лицом, ответственным в финансовом управлении администрации Арзгирского муниципального округа Ставропольского края за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.