УПРАВЛЕНИЕ СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ АДМИНИСТРАЦИИ КАРАБАШСКОГО ГОРОДСКОГО ОКРУГА

ПРИКАЗ

«29» декабря 2018 г. № 73

Об организации работ по защите персональных данных, обрабатываемых в информационных системах персональных данных

С целью организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Управления социальной защиты населения администрации Карабашского городского округа в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить:

- Положение о персональных данных в Управлении социальной защиты населения администрации Карабашского городского округа (Приложение № 1).

- Инструкцию лица, ответственного за организацию работ по обработке персональных данных (Приложение № 2).

- Инструкцию администратора безопасности информационной системы персональных данных (Приложение № 3).

- Инструкцию по организации парольной защиты (Приложение № 4).

- Инструкцию по резервному копированию защищаемой информации (Приложение № 5).

- Инструкцию по физической охране специальных помещений (Приложение № 6).

2. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник УСЗН Ю.Б. Мещерякова

Приложение № 1

УТВЕРЖДЕНО
приказом начальника УСЗН
администрации Карабашского
городского округа

от 29.12.2018 № 73

Положение о персональных данных в Управлении социальной защиты населения администрации Карабашского городского округа

1. Общие положения

1.1. Настоящее «Положение о персональных данных в Управлении социальной защиты населения администрации Карабашского городского округа» (далее – Положение) разработано на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и других нормативных правовых актов Российской Федерации.

1.2. Настоящим Положением определяется порядок обработки персональных данных субъектов персональных данных как с использованием средств автоматизации, так и без использования таковых.

1.3. Целью настоящего Положения является обеспечение защиты прав и свобод сотрудников Управления социальной защиты населения администрации Карабашского городского округа (далее УСЗН) при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.4. Положение распространяется также на персональные данные любых иных лиц, содержащихся в документах, полученных УСЗН из других организаций, в обращениях граждан и иных источниках персональных данных.

1.5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, а также затруднения реализации прав и свобод граждан Российской Федерации.

1.6. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными положениями и инструкциями УСЗН.

1.7. Персональные данные относятся к категории конфиденциальной информации. Обработка персональных данных субъекта персональных данных без письменного его согласия не допускаются, если иное не определено законом. Режим конфиденциальности персональных данных снимается в

случаях обезличивания или по истечении сроков хранения, если иное не определено законом.

1.8. Должностные лица предприятия, в обязанности которых входит обработка персональных данных субъектов, обязаны обеспечить каждому субъекту возможность ознакомления в установленном порядке, со своими персональными данными, если иное не предусмотрено законом.

1.9. Настоящее Положение утверждается начальником УСЗН и является обязательным для исполнения всеми сотрудниками УСЗН, имеющими доступ к персональным данным субъектов персональных данных.

2. Основные понятия, применяемые в настоящем Положении:

2.1. **Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации, Перечнем ПДн, обрабатываемых в УСЗН, настоящим Положением и другими локальными правовыми актами.

2.2. **Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2.3. **Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) · или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.4. **Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

2.5. **Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

2.6. **Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в

информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2.7. **Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

2.8. **Информационная система персональных данных** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

2.9. **Конфиденциальность персональных данных** – обязательное для соблюдения любым сотрудником или иным получившим доступ к персональным данным лицом требование, не допускать их распространение, без согласия субъекта персональных данных или наличия иного законного основания.

2.10. **Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.11. **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

2.12. **К субъектам персональных данных** (далее – субъекты) относятся сотрудники УСЗН, включая совместителей и лиц, выполняющие работы по договорам гражданско-правового характера, персональные данные которых переданы (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для обработки, а также иные лица, предоставляющие персональные данные.

3. Правила обработки персональных данных

3.1. Обработка персональных данных осуществляется на основе следующих принципов:

3.1.1. Законности целей и способов обработки персональных данных и добросовестности;

3.1.2. Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям предприятия;

3.1.3. Соответствия объема, характера и способов обработки персональных данных целям обработки;

3.1.4. Достоверности и достаточности персональных данных для целей обработки;

3.1.5. Недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

3.1.6. Недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

3.2. Собственником своих персональных данных является субъект персональных данных, и он самостоятельно решает вопрос передачи своих персональных данных.

3.3. Необходимым условием обработки персональных данных субъекта персональных данных является его письменное согласие.

3.4. Субъект персональных данных обязан передать комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, иными законами Российской Федерации, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и др.

3.5. УСЗН имеет право проверять достоверность указанных сведений в порядке, не противоречащем законодательству России.

3.6. Субъект персональных данных имеет право на свободный и бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами, а также получать информацию, касающуюся обработки его персональных данных.

3.7. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, производится не дольше, чем этого требуют цели их обработки.

3.8. Уничтожение персональных данных производится при достижении целей обработки или в случае утраты необходимости в их обработке.

3.9. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в соответствии с положением статьи 6 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

3.10. В случае отзыва субъектом согласия на обработку своих персональных данных, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

3.11. Правила обработки персональных данных для целей кадрового и бухгалтерского учета, юридического оформления деятельности УСЗН приводятся в «Положение об организации работы с персональными данными работников УСЗН и ведении их личных дел».

3.12. В целях информационного обеспечения функционирования могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться фамилия, имя, отчество, адрес, абонентский номер, сведения о должности и иные персональные данные, предоставленные субъектом.

3.13. Перечень уполномоченных сотрудников, допущенных к обработке персональных данных, определяется приказом начальника УСЗН .

3.14. УСЗН обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа в установленные нормативно-правовыми актами Российской Федерации сроки.

3.15. Внутренний доступ (доступ внутри УСЗН) к персональным данным субъектов имеют сотрудники, которым эти данные необходимы для выполнения должностных обязанностей.

3.16. Внешний доступ к персональным данным субъектов имеют массовые потребители персональных данных и контрольно-надзорные органы.

3.17. Надзорно-контрольные органы имеют доступ к информации исключительно в сфере своей компетенции.

3.18. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе деятельности УСЗН.

3.19. При обработке персональных данных принимаются необходимые организационные и технические меры, в том числе используются криптографические средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования и распространения, а также от иных неправомерных действий.

3.20. Мероприятия по технической защите персональных данных проводятся в соответствии с требованиями приказа ФСТЭК от 5 февраля 2010г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» (зарегистрировано в Минюсте РФ 19 февраля 2010 г., регистрационный № 16456), постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и «Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные Руководством 8 Центра ФСБ России от 21 февраля 2008 г.

4. Ответственность за разглашение конфиденциальной информации

4.1. За разглашение информации лицом, получившим доступ к персональным данным в связи с исполнением служебных обязанностей, предусмотрена административная ответственность.

4.2. За неправомерный отказ в предоставлении субъекту персональных данных доступа к своим персональным данным или в получении информации,

касающейся обработки его персональных данных, предусмотрена административная ответственность.

4.3. Юридические и физические лица, в соответствии со своими полномочиями владеющие персональными данными субъектов, получающие и использующие их, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

4.4. Нарушение неприкосновенности частной жизни (в том числе незаконный сбор или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), совершенные лицом с использованием своего служебного положения, влечет наложение наказания в порядке, предусмотренном Уголовным кодексом Российской Федерации.

Приложение № 2

УТВЕРЖДЕНА
приказом начальника УСЗН
администрации Карабашского
городского округа
от 29.12.2018г № 73

Инструкция лица, ответственного
за организацию работ по обработке персональных данных

Ответственный за организацию работ по обработке персональных данных обязан:

1. Осуществлять руководство и координацию работ по защите информации, относящейся к категории персональных данных.
2. Организовывать выполнение требований по защите информации на объектах, осуществляющих обработку персональных данных.
3. Осуществлять внутренний контроль за соблюдением Управления социальной защиты населения администрации Карабашского городского округа и его сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.
4. Доводить до сведения сотрудников Управления социальной защиты населения администрации Карабашского городского округа положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.
5. Осуществлять контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.
6. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.
7. Уведомлять уполномоченный орган по защите прав субъектов персональных данных об обработке персональных данных.
8. Осуществлять контроль за публикацией на официальном сайте Управления социальной защиты населения администрации Карабашского городского округа документов, определяющих политику в отношении обработки персональных данных.

Приложение № 3

УТВЕРЖДЕНА

Приказом начальника Управления
социальной защиты населения
администрации Карабашского
городского округа

от « 29 » 12 2018 г. № 73

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА БЕЗОПАСНОСТИ
ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Карабаш
2018

Содержание

1. Общие положения

1.1. Данная Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных (далее – ИСПДн) в Управлении социальной защиты населения администрации Карабашского городского округа (далее – Учреждении).

1.2. Администратор безопасности ИСПДн является штатным сотрудником Учреждения.

1.3. Администратор безопасности ИСПДн назначается приказом руководителя Учреждения.

1.4. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности администратора безопасности ИСПДн.

1.5. Администратор безопасности ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам ИСПДн.

1.6. Администратор безопасности должен иметь специальное рабочее место – рабочую станцию (PC), размещенную в отдельном помещении и функционирующую постоянно при включении сети.

2. Должностные обязанности

Администратор безопасности ИСПДн обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Знать перечень установленных в подразделениях Учреждения автоматизированных рабочих мест (далее АРМ) и перечень задач, решаемых с их использованием.

2.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

2.4. Обеспечивать функционирование и поддерживать работоспособность элементов ИСПДн, в том числе средств защиты информации, и локальной вычислительной сети.

2.5. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.6. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.7. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля.

2.8. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.9. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.10. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ (далее - ИСПДн).

2.11. Осуществлять оперативный контроль за работой пользователей защищенных АРМ, анализировать содержимое системных журналов всех АРМ и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов АРМ и надлежащий режим хранения данных архивов.

2.12. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых на АРМ ИСПДн специальных технических средств защиты от несанкционированного доступа (далее - НСД).

2.13. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов сторонними физическими лицами и организациями.

2.14. Периодически проверять состояние используемых средств защиты информации (далее - СЗИ) от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

2.15. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ.

2.16. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления НСД к информации и техническим средствам АРМ.

2.17. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению средствами защиты от НСД, установленных на АРМ ИСПДн.

2.18. Проводить занятия с сотрудниками и начальниками отделов по правилам работы на АРМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации.

2.19. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.

2.20. Участвовать в работе комиссий по пересмотру планов защиты.

3. Порядок работы с ресурсами ИСПДн

Перечень работ, производимых администратором безопасности ИСПДн.

3.1. Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн:

3.1.1. администратор безопасности ИСПДн разрабатывает правила парольной защиты и контролирует их соблюдение;

3.1.2. администратор безопасности ИСПДн сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, кодирует аппаратный идентификатор пользователя (при наличии);

3.1.3. администратор безопасности ИСПДн производит изменения учетных данных пользователя по требованию начальника отдела, при согласовании с ответственным за обеспечение безопасности персональных данных, а также периодически по утвержденному плану и в случае увольнения сотрудника;

3.1.4. администратор безопасности ИСПДн имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, в случае успешного взлома, администратор безопасности ИСПДн обязан потребовать у пользователя изменения пароля.

3.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации:

3.2.1. администратор безопасности ИСПДн обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – прекратить работы.

3.2.2. в случае сбоя программных СЗИ, таких, как неправильная идентификация и аутентификация пользователей, администратор безопасности ИСПДн обязан прекратить работы, в случае производственной необходимости продолжения работ – отключить программное обеспечение (далее - ПО) СЗИ и лично контролировать проведение работ пользователем.

3.3. Антивирусная защита ресурсов ИСПДн:

3.3.1. администратор безопасности ИСПДн в соответствии с инструкцией по организации антивирусной защиты разрабатывает и контролирует реализацию антивирусной политики, а именно:

– настраивает параметры антивирусной программы;

– контролирует работоспособность антивирусной программы;

– немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы;

– имеет право на проведение внеплановой проверки на присутствие вирусов;

– периодически обновляет антивирусные базы данных, а также исполняемые модули антивирусной программы.

3.4. Хранение дистрибутивов программного обеспечения СЗИ:

3.4.1. администратор безопасности ИСПДн должен хранить дистрибутивы ПО СЗИ, установленных на АРМ ИСПДн, в месте, исключающем доступ посторонних лиц.

3.5. Проверка целостности системного и прикладного ПО:

3.5.1. администратор безопасности ИСПДн должен периодически (не реже одного раза в квартал) производить проверку целостности системного и прикладного программного обеспечения с использованием специальных режимов работы СЗИ от НСД.

3.6. Резервное копирование и восстановление информации:

3.6.1. в соответствии с утвержденным регламентом, а также по требованию пользователей, администратор безопасности ИСПДн проводит резервное копирование и восстановление пользовательской информации. При этом необходимо выполнять следующие требования:

– иметь в наличии регламент резервного копирования и перечень резервируемой информации, утверждаемых руководителем Учреждения;

– вне графика производить обязательное резервное копирование в случае обнаружения неисправностей в работе АРМ или отчуждаемых носителей;

– допускается обоснованное внеплановое резервное копирование информации по инициативе администратора безопасности ИСПДн, если это не нарушает технологию обработки информации;

– резервные копии хранятся на отдельных носителях в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение (ответственным за хранение является администратор безопасности ИСПДн);

– при устранении неисправностей АРМ администратор безопасности ИСПДн производит восстановление важной информации с резервных копий.

3.7. Вывод ресурсов ИС из эксплуатации:

3.7.1. при невозможности ремонта технических средств ИСПДн администратор безопасности ИСПДн обязан:

– физически уничтожать любые носители, независимо от содержащейся на них информации, отразить факт уничтожения носителя в «Журнале учета машинных носителей персональных данных»;

– отразить факт выхода из строя и замены оборудования в «Техническом паспорте ИСПДн».

4. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят реализуемые в процессе сеанса работы операции;

4.1.2. действия третьего лица, пытающегося получить доступ (или получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

4.2. При выявлении факта НСД администратор безопасности ИСПДн обязан:

4.2.1. прекратить доступ к ИСПДн со стороны выявленного участка НСД;

4.2.2. доложить руководителю Учреждения служебной запиской о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить ответственного за обеспечение безопасности персональных данных и начальника отдела, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

4.2.4. проанализировать характер НСД, по результатам анализа составить письменный отчет и предоставить его руководителю Учреждения.

5. Права

5.1. Администратор безопасности ИСПДн имеет право:

5.1.1. требовать от пользователей информационных ресурсов выполнения инструкций пользователя ИСПДн;

5.1.2. проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

5.1.3. вносить свои предложения по совершенствованию мер защиты в ИСПДн.

6. Ответственность

6.1. Администратор безопасности ИСПДн несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации.

6.2. Администратор безопасности ИСПДн несет ответственность за программно-аппаратные, инженерно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и информационные системы обработки информации, закрепленные за ним приказом руководителя Учреждения и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

6.3. Администратор безопасности ИСПДн несет ответственность по действующему законодательству за разглашение информации, составляющей персональные данные, ставшие известными ему по роду работы.

6.4. Администратор безопасности ИСПДн несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

С должностной инструкцией ознакомлен(а) _____

Приложение № 4

УТВЕРЖДЕНА

Приказом начальника
Управления социальной защиты
населения администрации
Карабашского городского округа

от 29 12 2018 г. № 73

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

Карабаш
2018

Содержание

1. Общие положения

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее - ИСПДн) Управления социальной защиты населения администрации Карабашского городского округа, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПДн.

2. Правила формирования паролей

Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее 6 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях;

– личный пароль пользователь не имеет права сообщать никому.

В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности ИСПДн.

При использовании имен и паролей сотрудников в их отсутствие, ввиду технологической необходимости (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), по возвращении сотрудники обязаны сменить свои пароли, а их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передать на хранение администратору безопасности ИСПДн. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать администратора безопасности ИСПДн.

3. Ввод пароля

При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4. Порядок смены личных паролей

4.1. Смена паролей должна проводиться регулярно, не реже одного раза в 6 месяцев.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов безопасности ИСПДн, ответственных за обеспечение безопасности персональных данных, администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п.2 настоящей инструкции, и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

4.5. Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

5. Хранение пароля

5.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

5.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

5.3. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора безопасности ИСПДн, или начальником отдела в опечатанном личной печатью пенале.

6. Действия в случае утери или компрометации пароля

В случае утери или компрометации пароля пользователя должны быть немедленно предприняты следующие меры:

– Владелец скомпрометированного пароля должен сообщить о факте утери или компрометации пароля администратору безопасности ИСПДн;

– Владелец скомпрометированного пароля должен немедленно произвести смену скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

7.2. Ответственность за организацию парольной защиты в организации возлагается на администратора безопасности ИСПДн.

Приложение: на 1 л. в 1.экз.

Приложение № 5

УТВЕРЖДЕНА
приказом начальника УСЗН
администрации Карабашского
городского округа
от 29 декабря 2018. № 73

Инструкция
по резервному копированию защищаемой информации

1. Общие положения

1.1. Настоящая «Инструкция по резервному копированию защищаемой информации» устанавливает основные требования к организации резервного копирования (восстановления) программ, данных, базах данных на серверах Управления социальной защиты населения администрации Карабашского городского округа.

1.2. Настоящая Инструкция разработана с целью:

- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления;
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

1.3. Под резервным копированием информации понимается создание избыточных копий персональных данных на электронном носителе для быстрого восстановления работоспособности информационных систем персональных данных (далее ИСПДн) в случаях возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.4. Сервера, содержащие резервные копии, подлежат защите в той же степени, что и копии персональных данных.

1.5. Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;
- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в

том числе систем управления базами данных (далее СУБД) общего пользования и справочно-информационных систем общего использования;

- рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн, СУБД, серверов и рабочих станций;

- информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн, локальной вычислительной сети;

- регистрационная информация системы информационной безопасности ИСПДн;

- другая информация ИСПДн, по мнению пользователей и администратора безопасности, являющаяся критичной для работоспособности ИСПДн.

1.6. Резервные копии хранятся в пределах серверного помещения, доступ к резервным копиям ограничен. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только сотрудники, имеющие доступ к резервируемым программным и аппаратным средствам ИСПДн.

2. Контроль результатов исполнения процедур резервного копирования и восстановления данных, а также ротация носителей резервных копий

2.1. Контроль результатов всех процедур резервного копирования и восстановления данных осуществляется в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

2.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

2.3. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

2.4. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится через доступ к сетевым ресурсам на серверах. При этом используется последняя копия данных.

2.5. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью данные восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

2.6. Система резервного копирования обеспечивает возможность периодической замены (выгрузки) резервных носителей без потери данных на них, а также обеспечивает восстановление текущей данных ИСПДн в случае отказа любого из устройств резервного копирования.

2.7. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются администратором информационной безопасности. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащихся данных истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

3. Общие требования к резервному копированию

3.1. В Регламенте резервного копирования описываются действия при выполнении следующих мероприятий:

- резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);
- контроль резервного копирования:
- хранение резервных копий;
- полное или частичное восстановление данных.

3.2. Требования к техническому обеспечению систем резервного копирования:

- это комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;
- имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации:
- обеспечивает выполнение функций, перечисленных в п. 2.1;
- средства вычислительной техники отвечают действующим на момент сертификации российским и международным стандартам и рекомендациям.

3.3. Требования к программному обеспечению систем резервного копирования:

- лицензионное системное программное обеспечение и программное обеспечение резервного копирования;
- программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

3.4. Сопровождение системы резервного копирования возлагается на администратора информационной безопасности, который обязан следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование, в соответствии с их инструкциями по эксплуатации.

3.6. Хранение отдельных магнитных носителей архивных копий организуется в отдельном от используемых данных помещении. Физический доступ к архивным копиям строго ограничен. Контроль за физическим доступом возлагается на администратора информационной безопасности.

3.7. Доступ к носителям архивных копий имеет администратор информационной безопасности, который несет персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

Приложение № 6

УТВЕРЖДЕНА
приказом Начальником Управления
социальной защиты населения
администрации Карабашского городского
округа

от 29.12.2018г. № 73

Инструкция по физической охране специальных помещений

1. Общие положения

1.1. Данная Инструкция регламентирует условия и порядок осуществления доступа в помещения со средствами криптографической защиты информации (далее - СКЗИ).

1.2. Обеспечение доступа в помещения с СКЗИ (далее – специальные помещения) предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного пропускного режима и определяет порядок пропуска работников Управления социальной защиты населения администрации Карабашского городского округа (далее – УСЗН), сотрудников иных организации и учреждений и граждан.

1.3. Контроль за порядком обеспечения доступа работников УСЗН и посторонних лиц в специальные помещения возлагается на начальника отдела программно-технического обеспечения.

1.4. Специальные помещения и установленное в них оборудование размещены таким образом, чтобы исключить возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц.

1.5. Для исключения возможности бесконтрольного проникновения в специальные помещения и к установленному в них оборудованию посторонних лиц, включая сотрудников других отделов УСЗН, используются следующие инженерные средства: усиленные двери, охранная сигнализация, металлические шкафы и сейфы, опечатывающее устройство дверей и сейфов.

2. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним

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

2.2. При оборудовании специальных помещений (далее - спецпомещения) должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

2.3. Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Спецпомещения должны иметь охранную сигнализацию, усиленные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. 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.

2.4. Режим охраны спецпомещений, в том числе правила допуска сотрудников УСЗН и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации. Установленный режим охраны должен предусматривать периодический контроль состояния технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции.

2.5. Двери спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруются, учитываются и выдаются сотрудникам, имеющим право доступа в режимное помещение под расписку в журнале учета (Приложение № 1). Дубликаты ключей от входных дверей спецпомещений должны храниться в сейфе начальника отдела программно-технического обеспечения. Хранение дубликатов ключей вне данного помещения не допускается.

2.6. Для предотвращения просмотра извне окна спецпомещений должны быть защищены непрозрачными жалюзи.

2.7. Спецпомещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Исправность сигнализации периодически необходимо проверять администратору информационной безопасности совместно с представителем службы охраны с отметкой в соответствующих журналах (Приложение № 2)

2.8. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь металлические хранилища, оборудованные внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе начальника отдела программно-технического обеспечения.

2.9. Дубликат ключа от хранилища начальника отдела программно-технического обеспечения в опечатанной упаковке должен быть передан на хранение должностному лицу, назначаемому начальником отдела программно-технического обеспечения, под расписку в соответствующем журнале.

2.10. По окончании рабочего дня спецпомещения и установленные в них хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале начальнику отдела программно-технического обеспечения.

2.11. Ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службе охраны с передачей под охрану самих спецпомещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников, ответственных за эти хранилища.

2.12. При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

2.13. В обычных условиях спецпомещения и находящиеся в них опечатанные хранилища могут быть вскрыты только администратором информационной безопасности или администратором информационной безопасности персональных данных.

2.14. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководителю отдела программно-технического обеспечения. Администратор информационной безопасности должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных криптоключей.

2.15. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей СКЗИ 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.

2.16. 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 пользователи СКЗИ по согласованию с администратором информационной безопасности обязаны предусмотреть организационно - технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

2.17. В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

2.18. При утрате ключа от хранилища или от входной двери в спецпомещение пользователя СКЗИ замок необходимо заменить.

2.19. В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями.

2.20. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещения пользователей СКЗИ или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено администратору информационной безопасности.