

**Муниципальное учреждение
«Муниципальный архив Вольского муниципального района»**

РАСПОРЯЖЕНИЕ

От 11.10.2024

№ 7

Об утверждении Политики муниципального учреждения «Муниципальный архив Вольского муниципального района» Саратовской области в отношении обработки персональных данных

В целях осуществления мероприятий по защите информационных систем персональных данных в соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», и в соответствии с Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне», Указом Президента Российской Федерации от 17 марта 2008г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», постановлением Правительства Российской Федерации от 21 марта 2012г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», приказа ФСТЭК России от 11 февраля 2013г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», в соответствии с решением коллегии ФСТЭК России от 18.06.2018г. № 62 «Об организации и состоянии работ по технической защите информации в государственных информационных системах органов государственной власти Российской Федерации» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», и на основании ст.38 и ст.50 Устава Вольского муниципального района:

1. Утвердить Политику МУ «Муниципальный архив Вольского муниципального района» Саратовской области в отношении обработки персональных данных (приложение).
2. Ответственному за организацию обработки персональных данных в МУ «Муниципальный архив Вольского муниципального района» ознакомить работников учреждения, непосредственно осуществляющих обработку персональных данных, с положениями настоящего распоряжения.

3. Главному специалисту МУ «Муниципальный архив ВМР» организовать мероприятия по своевременному размещению документов, определяющих политику учреждения в отношении обработки персональных данных, на официальном сайте МУ «Муниципальный архив Вольского муниципального района» в информационно-телекоммуникационной сети «Интернет» в соответствующем разделе.

4. Контроль за исполнением настоящего распоряжения оставляю за собой.

Директор МУ
«Муниципальный архив ВМР»



О.Н. Саюшева

Приложение к распоряжению
Муниципального учреждения
«Муниципальный архив Вольского
муниципального района»
от 11.10.2024 № 7

ПОЛИТИКА

Муниципального учреждения «Муниципальный архив Вольского муниципального района»
Саратовской области в отношении обработки персональных данных

Термины и определения

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор - муниципальное учреждение «Муниципальный архив Вольского муниципального района» Саратовской области. Юридическое лицо - учреждение является некоммерческой организацией, имущество которой находится в собственности Вольского муниципального района и закреплено за Учреждением на праве оперативного управления.

Учреждение создано в целях обеспечения исполнения органами местного самоуправления Вольского муниципального района отдельных полномочий по решению вопросов местного значения, отдельных государственных полномочий, которыми органы местного самоуправления Вольского муниципального района наделены действующим законодательством, а также обеспечения участия органов местного самоуправления в осуществлении отдельных государственных полномочий, решение об участии в осуществлении которых принято в установленном порядке.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных - действия, направленные на раскрытие персональных данных определенному лицу.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1. Введение

Политика муниципального учреждения «Муниципальный архив Вольского муниципального района» в отношении обработки персональных данных (далее - Политика) определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется МУ «Муниципальный архив Вольского муниципального района» в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных МУ «Муниципальный архив Вольского муниципального района» позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

2. Общие положения

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение, реагирование на угрозы безопасности персональных данных, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

3. Правовая основа документа

Настоящая Политика разработана с учетом следующих документов:

- Федеральный закон от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 29 июля 2004г. №98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 27 июля 2006г. №152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации от 17 марта 2008г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- постановление Правительства Российской Федерации от 21 марта 2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- постановление Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ Федеральной службы по техническому и экспортному контролю от

18 февраля 2013г. №21 «Об утверждении состава и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденные приказом Гостехкомиссии от 30 августа 2002г. № 282.

4. Объекты защиты

Основными объектами системы безопасности персональных данных в МУ «Муниципальный архив Вольского муниципального района» являются:

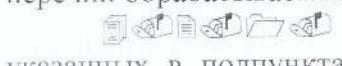
- информационные ресурсы с ограниченным доступом, содержащие персональные данные;
- процессы обработки персональных данных в информационных системах персональных данных МУ «Муниципальный архив Вольского муниципального района», информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

4.1. Субъекты персональных данных обрабатываемых в МУ «Муниципальный архив Вольского муниципального района».

К субъектам персональных данных, персональные данные которых обрабатываются в МУ «Муниципальный архив Вольского муниципального района», в соответствии с настоящей Политикой относятся:

- 1) работники МУ «Муниципальный архив Вольского муниципального района», занимающие должности, на основании трудового договора и члены их семьи;
- 2) граждане, претендующие на замещение должностей в МУ «Муниципальный архив Вольского муниципального района»;
- 3) супруги (в том числе бывшие, супруги братьев и сестер, братья и сестры супругов), лица, состоящие в родстве (свойстве) с субъектами персональных данных, указанными в подпунктах 1, 2 настоящего пункта, в случаях, предусмотренных законодательством Российской Федерации;
- 4) уволенные работники МУ «Муниципальный архив Вольского муниципального района»;
1. лица, включенные в кадровый резерв МУ «Муниципальный архив Вольского муниципального района»;
- 5) лица, обработка персональных данных которых осуществляется в связи с исполнением муниципального контракта, заключаемого МУ «Муниципальный архив Вольского муниципального района»;
- 6) лица, обработка персональных данных которых осуществляется в связи с исполнением гражданско-правовых договоров, заключаемых МУ «Муниципальный архив Вольского муниципального района»;
- 7) лица, обработка персональных данных которых осуществляется в связи с выполнением возложенных нормативными правовыми документами на МУ «Муниципальный архив Вольского муниципального района» функций, полномочий и обязанностей;
- 8) граждане, обратившиеся в соответствии с Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- 9) пользователи официального сайта МУ «Муниципальный архив Вольского муниципального района» в информационно-телекоммуникационной сети «Интернет».

4.2. Цели, условия и порядок обработки персональных данных и соответствующие им перечни обрабатываемых персональных данных

 Персональные данные субъектов персональных данных, указанных в подпунктах 1-5 пункта 4.1 настоящей Политики, обрабатываются в целях обеспечения архивной службы, трудового законодательства, содействия в выполнении осуществляющей работы, организации и прохождения конкурса на замещение вакантных должностей, формирования кадрового резерва архивной службы, обучения и должностного роста, учета результатов исполнения работниками МУ»Муниципальный архив Вольского муниципального района» должностных обязанностей, обеспечения личной безопасности работников, обеспечения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, в том числе при рассмотрении вопроса о предоставлении единовременной субсидии на приобретение жилого помещения, сохранности принадлежащего им имущества, противодействия коррупции.

 В целях, указанных в пункте 4.2.1 настоящей Политики, обрабатываются следующие категории персональных данных субъектов персональных данных, указанных в подпунктах 1 – 5 пункта 4.1 настоящей Политики:

- 1) фамилия, имя, отчество (при наличии) (в том числе прежние фамилии, имена и (или) отчества (при наличии), в случае их изменения);
- 2) дата рождения;
- 3) место рождения;
- 4) сведения о гражданстве (в том числе о прежних гражданствах, иных гражданствах);
- 5) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи;
- 6) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации за пределами Российской Федерации, наименование органа, выдавшего его, дата выдачи;
- 7) адрес места жительства, дата регистрации по месту жительства (месту пребывания);
- 8) номер телефона или сведения о других способах связи;
- 9) сведения, содержащиеся в страховом свидетельстве обязательного пенсионного страхования или документе, подтверждающем регистрацию в системе индивидуального (персонифицированного) учета;
- 10) идентификационный номер налогоплательщика;
- 11) реквизиты страхового медицинского полиса обязательного медицинского страхования;
- 12) реквизиты свидетельства о государственной регистрации актов гражданского состояния;
- 13) сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших супругах);
- 14) сведения о трудовой деятельности, включая работу по совместительству, предпринимательскую и иную деятельность, военную службу;
- 15) отношение к воинской обязанности, сведения о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документов воинского учета, наименование органа, выдавшего его);
- 16) сведения об образовании с указанием наименования образовательной организации, года ее окончания, квалификации, специальности и (или) направления подготовки, наименования и реквизитов документа об образовании;
- 17) сведения об ученой степени, ученом звании;
- 18) сведения о владении иностранными языками и языками народов Российской Федерации;
- 19) сведения о наличии либо отсутствии заболевания, препятствующего поступлению на на работу;
- 20) фотография;

21) сведения о прохождении архивной службы, в том числе: дата и основание поступления на работу и назначения на должность архивной службы, дата и основание назначения, перевода, перемещения на иную должность архивной службы, наименование замещаемых должностей архивной службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности архивной службы, а также сведения о прежнем месте работы;

22) сведения, содержащиеся в служебном контракте (трудовом договоре), дополнительных соглашениях к служебному контракту (трудовому договору);

23) сведения о пребывании за границей;

24) сведения о классном чине федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатическом ранге, воинском и (или) специальном звании, классном чине правоохранительной службы, классном чине юстиции, а также сведения о том, кем и когда они присвоены;

25) сведения о наличии или отсутствии судимости;

26) сведения об оформленных допусках к государственной тайне;

27) сведения о государственных наградах, иных наградах и знаках отличия;

28) сведения о профессиональной переподготовке и (или) повышении квалификации;

29) сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

30) сведения о доходах, об имуществе и обязательствах имущественного характера работника МУ «Муниципальный архив Вольского муниципального района», гражданина, претендующего на замещение должности в МУ «Муниципальный архив Вольского муниципального района», сведения о доходах, об имуществе и обязательствах имущественного характера супруги (супруга) и (или) несовершеннолетних детей работников МУ «Муниципальный архив Вольского муниципального района», а также сведения о расходах работника;

31) сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет», на которых работники МУ «Муниципальный архив Вольского муниципального района», гражданином, претендующим на замещение должностей, размещалась общедоступная информация, а также данные, позволяющие его идентифицировать;

32) номер расчетного счета;

33) номер банковской карты;

34) иные сведения, которые субъект персональных данных пожелал сообщить о себе и которые отвечают целям обработки персональных данных, указанным в пункте 4.2.1 настоящей Политики.

Способы обработки персональных данных: смешанный, с передачей по внутренней сети юридического лица, с передачей по сети Интернет.

 Обработка персональных данных и биометрических персональных данных субъектов персональных данных, указанных в подпунктах 1-5 пункта 4.1 настоящей Политики, осуществляется без их согласия в целях, определенных пунктом 4.2.1 настоящей Политики, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных» и Федеральный закон от 02.03.2007 N 25-ФЗ "О муниципальной службе в Российской Федерации", Федерального закона от 25 декабря

 2008г. № 273-ФЗ «О противодействии коррупции»C:\Y\02\122\%D0%9F%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%BD%D0%8B5 1.docx - ftn5, Трудовым кодексом Российской ФедерацииC:\Y\02\122\%D0%9F%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%BD%D0%8B5 1.docx - ftn6.

 Обработка специальных категорий персональных данных субъектов персональных данных осуществляется без их согласия в целях, указанных в пункте 4.2.1 настоящей Политики, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона «О персональных данных»C:\Y:\02\122\%D0%9F%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5 1.docx - ftn7, за исключением случаев получения персональных данных у третьей стороны в соответствии с пунктом 3 статьи 86 Трудового кодекса Российской ФедерацииC:\Y:\02\122\%D0%9F%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5 1.docx - ftn8.

 Обработка персональных данных субъектов персональных данных, указанных в подпунктах 1 – 5 пункта 4.1 настоящей Политики, осуществляется с их согласия в следующих случаях:

1) при передаче персональных данных третьим лицам в случаях, не предусмотренных законодательством Российской Федерации о работнике, трудовым законодательством Российской Федерации и о противодействии коррупции;

2) при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных C:\Y:\02\122\%D0%9F%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5 1.docx - ftn9.

 В случаях, предусмотренных пунктом 4.2.5 настоящей Политики, согласие субъектов персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

 Обработка персональных данных субъектов персональных данных, указанных в подпунктах 1 – 5 пункта 4.1 настоящей Политики, осуществляется специалистом по персоналу МУ «Муниципальный архив Вольского муниципального района» и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

 Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных осуществляется путем:

1) получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые в кадровое подразделение) (далее – оригиналы документов);

2) копирования оригиналов документов;

3) внесения сведений в учетные формы (на бумажных и электронных носителях);

4) формирования персональных данных в ходе кадровой работы;

5) внесения персональных данных в информационные системы персональных данных, используемые кадровым подразделением.

 Запрещается получать, обрабатывать и приобщать к личному делу субъектов персональных данных, указанных в подпунктах 1 – 5 пункта 4.1 настоящей Политики, персональные данные, не предусмотренные пунктом 6 настоящей Политики, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

 Персональные данные лиц, указанных в подпунктах 6-8 пункта 4.1 настоящей Политики, обрабатываются в целях реализации полномочий МУ «Муниципальный архив Вольского муниципального района», установленных Уставом МУ «Муниципальный архив Вольского муниципального района» Саратовской области, а также

предусмотренных федеральными законами, актами Президента Российской Федерации, Правительства Российской Федерации.

В целях, указанных в пункте 4.2.10 настоящей Политики, обрабатываются следующие персональные данные лиц, указанных в подпунктах 6-8 пункта 4.1 настоящей Политики:

- 1) фамилия, имя, отчество (при наличии);
- 2) дата и место рождения;
- 3) адрес места жительства, дата регистрации по месту жительства (месту пребывания);
- 4) сведения, содержащиеся в страховом свидетельстве обязательного пенсионного страхования или документе, подтверждающем регистрацию в системе индивидуального (персонифицированного) учета;
- 5) идентификационный номер налогоплательщика;
- 6) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи;
- 7) номер телефона или сведения о других способах связи;
- 8) иные персональные данные, которые отвечают цели обработки персональных данных, указанной в пункте 4.2.10 настоящей Политики.

Способы обработки персональных данных: смешанный, с передачей по внутренней сети юридического лица, с передачей по сети Интернет.

Персональные данные лиц, указанных в подпункте 9 пункта 4.1 настоящей Политики, обрабатываются в целях обеспечения своевременного и в полном объеме рассмотрения устных и письменных обращений таких лиц в порядке, установленном Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

В целях, указанных в пункте 4.2.12 настоящей Политики, обрабатываются следующие персональные данные лиц, указанных в подпункте 9 пункта 4.1 настоящей Политики:

- 1) фамилия, имя, отчество (при наличии);
- 2) адрес места жительства;
- 3) адрес электронной почты (при наличии);
- 4) иные персональные данные, указанные в обращении, а также ставшие известными в ходе личного приема или в процессе рассмотрения обращения.

Способы обработки персональных данных: смешанный, с передачей по внутренней сети юридического лица, с передачей по сети Интернет.

Обработка персональных данных лиц, указанных в подпункте 10 пункта 4.1 настоящей Политики, осуществляется в целях организации доступа к информации о деятельности МУ «Муниципальный архив Вольского муниципального района», размещаемой в информационно-телекоммуникационной сети «Интернет».

В целях, указанных в пункте 4.2.14 настоящей Политики, обрабатываются следующие персональные данные лиц, указанных в подпункте 10 пункта 4.1 настоящей Политики:

- 1) фамилия, имя, отчество (при наличии);
- 2) адрес места жительства;
- 3) адрес электронной почты (при наличии);
- 4) иные сведения, которые представлены пользователем официального сайта администрации Вольского муниципального района в информационно-телекоммуникационной сети «Интернет».

Способы обработки персональных данных: смешанный, с передачей по внутренней сети юридического лица, с передачей по сети Интернет.

4.3. Сроки обработки и хранения персональных данных



Сроки обработки и хранения персональных данных определяются:

1) Приказом Росархива от 20.12.2019 N 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;

2) иными требованиями законодательства Российской Федерации и муниципальными правовыми актами администрации Вольского муниципального района.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Персональные данные при их обработке, осуществляющейся без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях.

4.4. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

Уничтожение по окончании обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

5. Цели и задачи обеспечения безопасности персональных данных

5.1. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности персональных данных МУ «Муниципальный архив Вольского муниципального района» являются:

- МУ «Муниципальный архив Вольского муниципального района», как собственник информационных ресурсов;
- руководство и сотрудники МУ «Муниципальный архив Вольского муниципального района», в соответствии с возложенными на них функциями;
- граждане, обращающиеся в МУ «Муниципальный архив Вольского муниципального района» по вопросам, относящимся к компетенции МУ «Муниципальный архив Вольского муниципального района».

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимым им персональным данным (их доступности);
- достоверности (полноты, точности, адекватности, целостности) персональных данных;

- конфиденциальности (сохранения в тайне) персональных данных;
- защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
- защиты персональных данных от незаконного распространения.

5.2. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений МУ «Муниципальный архив Вольского муниципального района» от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

- доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района», при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах персональных данных МУ «Муниципальный архив Вольского муниципального района» и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

5.3. Основные задачи системы обеспечения безопасности персональных данных

Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности МУ «Муниципальный архив Вольского муниципального района» должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района»;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района» посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам МУ «Муниципальный архив Вольского муниципального района» (возможный и иным)

можность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в информационных системах персональных данных МУ «Муниципальный архив Вольского муниципального района» программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

5.4. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района» (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов МУ «Муниципальный архив Вольского муниципального района» по вопросам обеспечения безопасности персональных данных;
- назначением должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;
- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам МУ «Муниципальный архив Вольского муниципального района»;
- четким знанием и строгим соблюдением всеми пользователями информационных систем МУ «Муниципальный архив Вольского муниципального района» требований организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных;
- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам МУ «Муниципальный архив Вольского муниципального района»;
- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды МУ «Муниципальный архив Вольского муниципального района»;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов информационных систем персональных данных и непрерывной административной поддержкой их использования;
- эффективным контролем над соблюдением пользователями информационных ресурсов МУ «Муниципальный архив Вольского муниципального района» требований по обеспечению безопасности информации;
- юридической защитой интересов МУ «Муниципальный архив Вольского муниципального района» при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

6. Основные принципы построения системы безопасности персональных данных

Построение системы, обеспечение безопасности персональных данных МУ «Муниципальный архив Вольского муниципального района» и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность (экономическая целесообразность);
- персональная ответственность;
- минимизация полномочий;
- исключение конфликта интересов;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

6.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных МУ «Муниципальный архив Вольского муниципального района» в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации Российской Федерации, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района» должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

6.2. Системность

Системный подход к построению системы защиты информации в МУ «Муниципальный архив Вольского муниципального района» предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района», а также характер, возможные объекты и направления атак на них со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

6.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

6.4. Непрерывность защиты

Обеспечение безопасности персональных данных – процесс, осуществляемый руководством МУ «Муниципальный архив Вольского муниципального района», администра-

ром безопасности информационных систем персональных данных и сотрудниками всех уровней. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности МУ «Муниципальный архив Вольского муниципального района», и ее эффективность зависит от участия руководства МУ «Муниципальный архив Вольского муниципального района» в обеспечении информационной безопасности персональных данных.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления защиты.

6.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, включающий постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем в целом и их систем защиты в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самих защищаемых информационных систем. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счёте, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищённости.

6.6. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района» и системы ее защиты с учетом изменений в методах и средствах перехвата информации, а также нормативных требований по защите информации.

6.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района». Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока персональные данные находятся в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

6.8. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и систем их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится та-

ким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

6.9. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

6.10. Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сфера потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования персональными данными и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками МУ «Муниципальный архив Вольского муниципального района». Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

6.11. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе МУ «Муниципальный архив Вольского муниципального района». В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности администрации безопасности информационных систем персональных данных.

Важным элементом эффективной системы обеспечения безопасности персональных данных в МУ «Муниципальный архив Вольского муниципального района» является высокая культура работы с информацией. Все сотрудники МУ «Муниципальный архив Вольского муниципального района» должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

6.12. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления МУ «Муниципальный архив Вольского муниципального района» своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры МУ «Муниципальный архив Вольского муниципального района»;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

6.13. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алго-

ритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

6.14. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

6.15. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты персональных данных должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

6.16. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты персональных данных специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами МУ «Муниципальный архив Вольского муниципального района» (ответственным специалистом по технической защите информации).

6.17. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных, на основе используемых систем и средств защиты персональных данных, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками МУ «Муниципальный архив Вольского муниципального района» должны немедленно доводиться до сведения директора МУ «Муниципальный архив муниципального района» и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устраниены.

6.18. Меры, методы и средства обеспечения требуемого уровня защиты информационных ресурсов

6.19. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационной системы МУ «Муниципальный архив Вольского муниципального района» подразделяются на:

- правовые;

- морально-этические;
- технологические;
- организационные (административные);
- физические;
- технические (аппаратурные и программные).

7.1.1 Правовые меры защиты

К правовым мерам защиты относятся действующие законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района».

7.1.2 Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно установленные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или МУ «Муниципальный архив Вольского муниципального района» в целом. Морально-этические нормы бывают как неписаные, так и писанные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы.

7.1.3 Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

7.1.4 Организационные (административные) меры защиты

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования информационных систем обработки персональных данных, использование их ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системами таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

6.20. Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать политику в области обеспечения безопасности персональных данных, отражающую подходы к защите персональных данных, и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности персональных данных в МУ «Муниципальный архив Вольского муниципального района» целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность МУ «Муниципальный архив Вольского муниципального района» в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры и правила достижения целей и решения задач безопасности персональных данных и детализирует (регламентирует) эти правила:

- определение ролей и обязанностей должностных лиц, отвечающих за проведение политики безопасности персональных данных;
- разграничение прав доступа к персональным данным и т.д.

Политика нижнего уровня должна:

- предусматривать регламент информационных отношений, исключающих возможность произвольных или несанкционированных действий в отношении информационных ресурсов;
- определять принципы и методы разграничения доступа к персональным данным;
- выбирать программно-технические (аппаратные) средства противодействия несанкционированному доступу, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

6.21. Регламентация доступа в помещения

Компоненты информационных систем МУ «Муниципальный архив Вольского муниципального района» должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, автоматизированных рабочих мест и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем МУ «Муниципальный архив Вольского муниципального района», запираются на ключ.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

6.22. Регламентация допуска сотрудников к использованию информационных ресурсов

Допуск пользователей к работе с информационными системами персональных данных МУ «Муниципальный архив Вольского муниципального района» и доступ к их ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

- каждый сотрудник пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходимо работать в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационным ресурсам, в обязательном порядке, должно согласовываться с администратором безопасности информационных систем персональных данных.

Все сотрудники МУ «Муниципальный архив Вольского муниципального района» и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов информационных систем.

Обработка персональных данных в компонентах информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района» должна производиться в соответствии с утвержденными технологическими инструкциями.

6.23. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников МУ «Муниципальный архив Вольского муниципального района», с которых возможен доступ к ресурсам информацион-

ных систем персональных данных, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационных систем персональных данных и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

6.24. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационных систем, используемое для доступа и хранения персональных данных, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

6.25. Подбор и подготовка персонала, обучение пользователей

Пользователи информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района», а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющими требования и порядок обработки персональных данных в МУ «Муниципальный архив Вольского муниципального района».

Все пользователи информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района» должны быть ознакомлены с организационно-распорядительными документами по обеспечению безопасности персональных данных, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности персональных данных. Доведение требований, указанных документов до лиц, допущенных к обработке защищаемых персональных данных, должно осуществляться под распись.

6.26. Ответственность за нарушения установленного порядка пользования ресурсами информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района».

Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

Должностные лица МУ «Муниципальный архив Вольского муниципального района», в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.

Каждое должностное лицо получающее для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность полученной информации МУ «Муниципальный архив Вольского муниципального района».

6.27. Средства обеспечения безопасности персональных данных

Для обеспечения информационной безопасности МУ «Муниципальный архив Вольского муниципального района» используются следующие средства защиты:

- физические средства;
- технические средства;
- средства идентификации и аутентификации пользователей;
- средства разграничения доступа;
- средства обеспечения и контроля целостности;
- средства оперативного контроля и регистрации событий безопасности.

Средства защиты должны применяться ко всем ресурсам информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района», независимо от их вида и формы представления информации в них.

Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым персональным данным, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района» необходимо осуществлять ряд организационных и технических мероприятий, включающих проверку оборудования, предназначенного для обработки персональных данных, на введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки персональных данных, а также оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности персональных данных по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства разграничения доступа к данным;
- средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;
- средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств;
- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- защита данных системы защиты на файловом сервере от доступа пользователей, чьи должностные обязанности не входит работа с информацией, находящейся на нем.

Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационных систем персональных данных МУ «Муниципальный архив Вольского муниципального района» посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);
- путем проверки знания ими паролей;

- путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

- на контролируемую территорию;
- в отдельные помещения;
- к компонентам информационной среды МУ «Муниципальный архив Вольского муниципального района» и элементам системы защиты персональных данных (физический доступ);
- к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);
- к активным ресурсам (прикладным программам, задачам и т.п.);
- к операционной системе, системным программам и программам защиты.

Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов систем персональных данных МУ «Муниципальный архив Вольского муниципального района» предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации персональных данных должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);
- средствами электронной подписи;
- средствами подсчета контрольных сумм (для используемого программного обеспечения).

Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток несанкционированного доступа и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);
- получения твердой копии (печати) журнала регистрации событий безопасности;
- упорядочения журналов, а также установления ограничений на срок их хранения;
- оперативного оповещения администратора информационной безопасности о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

- дата и время события;

- идентификатор субъекта, осуществляющего регистрируемое действие;
- действие (тип доступа).

7.10. Контроль эффективности системы защиты

Контроль эффективности системы защиты персональных данных осуществляется с целью своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных действий, направленных на уничтожение персональных данных, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Директор МУ «Муниципальный архив ВМР»

О.Н. Саюшева

