АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ - ЕРШИЧСКИЙ РАЙОН СМОЛЕНСКОЙ ОБЛАСТИ

Р А С П О Р Я Ж Е Н И Е

от 04.08.2014 № 165-р
с. Ершичи
Ершичского района
Смоленской области

Об утверждении Положения об обработке и защите персональных данных работников Администрации муниципального образования – Ершичский район Смоленской области

В соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15.09.2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Уставом муниципального образования – Ершичский район Смоленской области:

1. Утвердить Положение об обработке и защите персональных данных работников Администрации муниципального образования – Ершичский район смоленской области (прилагается).
2. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава Администрации
муниципального образования –
Ершичский район Смоленской области **В. В. Евтихов**

Отп. 1экз. - в дело
Исп. М.В. Капцевич
Тел. 2-19-07
«___»_____ _____

Разослать: управляющему делами; бухгалтерии; кадрам; отделу экономики имущественных и земельных отношений.

Разработчик:
М.В. Капцевич
Тел. 2-19-07
«___»_____ _____

Визы:

М.М. Бугаев «___»_____ _____

М.М. Пахоменков «___»_____ _____

Приложение
к распоряжению Администрации муниципального образования – Ершичский район Смоленской области
от 04.08.2014 № 165-р

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ – ЕРШИЧСКИЙ РАЙОН СМОЛЕНСКОЙ ОБЛАСТИ

1. ОБЩЕЕ ПОЛОЖЕНИЕ

1.1.Настоящее Положение об обработке и защите персональных данных (далее – Положение) Администрации муниципального образования – Ершичский район Смоленской области (далее Оператор) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15.09.2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Уставом Администрации муниципального образования – Ершичский район Смоленской области.

1.2. Цель разработки Положения – определение порядка обработки персональных данных работников Оператора; обеспечение защиты прав и свобод работников Оператора при обработке их персональных данных, хранение персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников Оператора, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения

1.3.1. Настоящее Положение вступает в силу с момента его утверждения Администрацией муниципального образования – Ершичский район Смоленской области и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся распоряжением Администрации муниципального образования – Ершичский район Смоленской области.

1.4. Все работники должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока хранения или продлевается на основании заключения экспертной комиссии Оператора, если иное не определено законом.

2. ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И ОБУЧАЮЩИХСЯ

2.1. Для целей настоящего Положения используются следующие основные понятия:

- персональные данные работника – любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями, с ведением учебного процесса;

- обработка персональных данных - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников Оператора;

- конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;

- использование персональных данных – действия (операции) с персональными данными, совершаемые должностным лицом Оператора в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использование, распространения персональных данных работника , в том числе их передача;

- уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной

системе персональных данных работников и обучающихся или в результате которых уничтожаются материальные носители персональных данных работников;

- обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;

- документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. Получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, нормативными и распорядительными документами, Положением об обработке и защите персональных данных на основе согласия субъектов на обработку их персональных данных. Оператор не вправе требовать от субъекта персональных данных, предоставляющих информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и о его частной жизни. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка персональных данных для исполнения трудовых договоров или без использования средств автоматизации, и в иных случаях, предусмотренных законодательством Российской Федерации.

2.3. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации. Не допускается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы. В случае увольнения субъекта персональных данных и иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней, если иное не предусмотрено федеральными законами. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями Оператора.

2.4. Персональные данные могут храниться в бумажном и (или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных правил. Право на обработку персональных данных предоставляется работникам структурных подразделений и (или) должностным лицам, определенным настоящим Положением об обработке и защите персональных данных, распорядительными документами и иными письменными указаниями Оператора.

2.5. 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 нормативно-правовыми актами и инструкциями Оператора.

3. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Права субъекта персональных данных в целях обеспечения защиты своих персональных данных:

- в целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Федеральным законом Российской Федерации от27.06.2006г. № 152-ФЗ «О персональных данных», за исключением случаев, предусмотренных данным Федеральным законом, имеет право на получение сведений об Операторе;

- требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если по вине Оператора персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

- на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;

- на обжалование действий или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

3.2. Обязанности Оператора при сборе персональных данных

Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными

данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по представлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

3.3. В случае выявления неправомерных действий с персональными данными Оператор обязан сообщить непосредственному руководителю и проректору по безопасности о выявленных нарушениях, в срок не превышающий трех рабочих дней с даты такого выявления, устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

3.4. В случае отзыва субъекта персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено Федеральными законами и (или) соглашением между Оператором и субъектом персональных данных. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных.

4. ПРАВА ОПЕРАТОРА НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ

4.1. Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации.

5. ОТВЕТСТВЕННОСТЬ ОПЕРАТОРА ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Оператор, а также должностные лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную,

административную, дисциплинарную и иную ответственность предусмотренную законодательством Российской Федерации.

Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Оператора, обрабатывающих персональные данные.

ИНСТРУКЦИЯ О ПОРЯДКЕ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБРАЩЕНИИ С ИНФОРМАЦИЕЙ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Обязательные для всех структурных подразделений Администрации муниципального образования – Ершичский район Смоленской области требования по обеспечению конфиденциальности документов, содержащих персональные данные:

- 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.

1.2. Когда обеспечение конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

1.3. Необходимость согласия субъекта персональных данных или наличие иного законного основания на их обработку:

- конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку;

1.4. Согласие субъекта персональных данных не требуется на обработку данных:

- в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;

- адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;

- данных, включающих в себя только фамилии, имена и отчества;

- персональных данных, обрабатываемых без использования средств автоматизации.

1.5. Порядок ведения перечней персональных данных:

- в Администрации муниципального образования – Ершичский район Смоленской области сформирован и ведется перечень конфиденциальных данных, утвержденный постановлением от 04.04.2014 № 81 «Об утверждении Перечня сведений конфиденциального характера в Администрации муниципального образования – Ершичский район Смоленской области».

- осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

2. НОРМАТИВНЫЕ ДОКУМЕНТЫ, ОПРЕДЕЛЯЮЩИЕ ОСНОВНЫЕ ТРЕБОВАНИЯ И МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

- основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлением Правительства Российской Федерации от 17 ноября 2007г. № 781 « Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных данных» и от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные

данные содержатся в информационной системе персональных данных либо были извлечены из нее.

3. ОБЩИЕ ПРАВИЛА ХРАНЕНИЯ И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ:

- запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении;

- все сотрудники ответственные за обработку персональных данных, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе соответствующими видами персональных данных;

- сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, письменным запросам установленного образца;

- после подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных;

- без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

- передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», « О порядке рассмотрения обращений граждан Российской Федерации», настоящей инструкцией, а также по письменному поручению (резолюции) вышестоящих должностных лиц;

- запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и настоящей инструкцией;

- ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

4. ОТВЕТСТВЕННОСТЬ ЗА ЗАЩИТУ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

- сотрудники подразделений Администрации муниципального образования – Ершичский район Смоленской области, сотрудники организаций – Операторов или лица, осуществляющие такую обработку по договору с Оператором, а также иные лица, осуществляющие обработку или хранение конфиденциальных данных в КЧГУ, несут ответственность в соответствии с пунктом 5 настоящего положения за обеспечение их информационной безопасности;

- лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и нормативно – правовыми актами.

5. ПОРЯДОК ОЗНАКОМЛЕНИЯ С ИНСТРУКЦИЕЙ

- сотрудники подразделений Администрации муниципального образования – Ершичский район Смоленской области и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под распись с настоящей Инструкцией.

6. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ, В ТОМ ЧИСЛЕ УСЛОВИЯ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

- обработка персональных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных;

- при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

- необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- при фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;

- для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель;

-при несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

7. ИСПОЛЬЗОВАНИЕ ТИПОВЫХ ФОРМ ДОКУМЕНТОВ И ЖУРНАЛОВ УЧЕТА

- при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилия, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8. ПОРЯДОК УНИЧТОЖЕНИЯ ИЛИ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

- уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

9. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ, В ТОМ ЧИСЛЕ ПРАВИЛА ДОСТУПА, ХРАНЕНИЯ И ПЕРЕСЫЛКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены

индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа или под чужим, или общими (одинаковыми) паролями, запрещается.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернета, запрещается.

10. ОБЩИЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

- технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

б) учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание систем защиты персональных данных.

Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

11. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ТВЕРДЫМИ КОПИЯМИ И ИХ УТИЛИЗАЦИИ, В ТОМ ЧИСЛЕ ОРГАНИЗАЦИЯ УЧЕТА НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

- все находящиеся на хранении и обращении съемные носители с персональными данными подлежат учету;

- каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер;

- учет и выдача съемных носителей персональных данных **(Приложение № 1)** осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных;

- сотрудники КЧГУ получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок;

- при получении делаются соответствующие записи в журнале учета;

- по окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

12. ПРАВИЛА ИСПОЛЬЗОВАНИЯ СЪЕМНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

-нельзя хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- нельзя выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов с ограниченным правом пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

13. ПОРЯДОК ДЕЙСТВИЙ ПРИ УТРАТЕ ИЛИ УНИЧТОЖЕНИИ СЪЕМНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

- о фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения, администратор безопасности;

-по факту и (или) разглашения персональных данных, по распоряжению Администрации муниципального образования – Ершичский район Смоленской области, создается комиссия, которая проводит служебное разбирательство, по результатам которого принимается решение о привлечении к ответственности виновных лиц;

- на утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных;

- съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению;

- уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией с составлением акта;

- По результатам уничтожения носителей составляется **(Приложение № 2)**

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБЪЕКТАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предмет Инструкции основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) Администрации муниципального образования – Ершичский район Смоленской области.

1.2. Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

1.3. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

ПОЛЬЗОВАТЕЛЬ ДОЛЖЕН:

2.1. Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;

- при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;
- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;
- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ;
- оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- не допускать "загрязнение" ПЭВМ посторонними программными средствами;
- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий,
- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;
- помнить личные пароли, персональные идентификаторы не оставлять без

присмотра и хранить в запирающемся ящике стола или сейфе;

- знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;

- при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

3. ЗАПРЕЩАЕМЫЕ ДЕЙСТВИЯ

ПОЛЬЗОВАТЕЛЬ НЕ ДОЛЖЕН:

3.1. Записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

- самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

- отключать (блокировать) средства защиты информации;

- производить какие-либо изменения в подключении и размещении технических средств;

- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.

- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

4. ПРАВА ПОЛЬЗОВАТЕЛЯ ПЭВМ

ПОЛЬЗОВАТЕЛЬ МОЖЕТ (ИМЕЕТ ПРАВО):

4.1. Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.

4.2. Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

5. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ ПЭВМ

5.1. Пользователь несет ответственность за:

- надлежащее выполнение требований настоящей инструкции;
- соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;
- сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;
- сохранность персональных данных.

Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

ИНСТРУКЦИЯ ПО ПРОВЕДЕНИЮ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И АНТИВИРУСНОГО КОНТРОЛЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации Администрации муниципального образования – Ершичский район Смоленской области.

2. МОНИТОРИНГ АППАРАТНОГО ОБЕСПЕЧЕНИЯ

2.1. Мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование) должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

3. МОНИТОРИНГ ПАРОЛЬНОЙ ЗАЩИТЫ

3.1. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей (не более 3 месяцев);
- периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

4. МОНИТОРИНГ ЦЕЛОСТНОСТИ

4.1. Мониторинг целостности программного обеспечения включает следующие действия:

- проверку контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- обнаружение дубликатов идентификаторов пользователей;
- восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. МОНИТОРИНГ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

5.1.Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

6. МОНИТОРИНГ ПРОИЗВОДИТЕЛЬНОСТИ

6.1. Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

7. СИСТЕМНЫЙ АУДИТ

7.1. Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

7.2. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, тому уровню безопасности, которое удовлетворяет требования политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующим специально составленному списку для проверки.

8. ОБЗОРЫ БЕЗОПАСНОСТИ ДОЛЖНЫ ВКЛЮЧАТЬ

8.1. Отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной

установки домашних каталогов пользователей и уязвимостей пользовательских окружений;

- проверку содержимого файлов конфигурации на соответствие списку для проверки;

- обнаружении информацию об изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);

- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

8.2. Активное тестирование надежности механизмов контроля доступа, которое производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

8.3. Пассивное тестирование механизмов контроля доступа, которое осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

8.4. Внесение изменений в системное программное обеспечение, осуществляемое администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале:

- уведомлением каждого сотрудника, кого касается изменение;

- выслушиванием претензий в случае, если это изменение причинило кому-нибудь вред;

- разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

9. АНТИВИРУСНЫЙ КОНТРОЛЬ

Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD - ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации».

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка:

- на защищаемых серверах и рабочих станциях ИСПДн - ответственным за обеспечение информационной безопасности подразделения;

- на других серверах и рабочих станциях, не требующих защиты ИСПДн - лицом, установившим (изменившим) программное обеспечение, - в присутствии и под контролем руководителя данного подразделения или сотрудника, им уполномоченного.

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале

подразделения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

9.1. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ВИРУСОВ

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник структурного подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации подразделения должен провести внеочередной антивирусный контроль своем рабочем месте. При необходимости привлечь специалиста Администрации для определения ими факта наличия или отсутствия компьютерного вируса.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обеспечение информационной безопасности своего подразделения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

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

- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалиста Администрации);

- в случае обнаружения нового вируса, не поддающегося лечению, применяемыми антивирусными средствами, передать зараженный вирусом файл на гибком магнитном диске специалисту администрации для дальнейшей отправки его в организацию, с которой заключен договор на антивирусную поддержку;

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

9.2. ОТВЕТСТВЕННОСТЬ

Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем подсистему АС, в соответствии с требованиями настоящей Инструкции возлагается на руководителя подразделения.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех сотрудников подразделения, являющихся пользователями АС.

необходимо:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями

Приложение № 1
к положению Администрации муниципального образования – Ершичский район Смоленской области
от 04.08.2014 № 165-р

ЖУРНАЛ

УЧЕТА СЪЕМНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

_____

наименование структурного подразделени

Начат «__» _____ 200_ г.

Окончен «__» _____ 200_ г.

На _____лист

№ п/п	Наименование (тип и емкость носителя)	№ носителя	Местонахождение носителя	Ф.И.О. должность получателя	(получил вернул передал/ дата)	Ответственное за учет лицо (Ф.И.О.)	Примечание*
1	2	3	4	5	6	7	8
1.							
2.							
3.							
4.							
5.							
6.							

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными, уничтожение носителя)

Приложение № 2
к положению Администрации муниципального образования – Ершичский район Смоленской области
от 04.08.2014 № 165-р

Разрешаю уничтожить
_____
_____
_____
_____
(руководитель организации)

«___» _____20__ г.

Акт об уничтожении персональных данных

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации_____ _____ информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего подлежит уничтожению_____носителей
(цифрами и прописью)

После утверждения акта перечисленные носители сверены с записями в акте и на указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

После утверждения акта перечисленные носители сверены с записями в акте и уничтожены путем
_____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии: _____ / /

Члены комиссии: _____ / /

_____ / /

_____ / /

_____ / /

Примечание:
1. Акт составляется раздельно на каждый способ уничтожения носителей.
2. Все листы акта, а так же все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.