РОССИЙСКАЯ ФЕДЕРАЦИЯ

П О С Т А Н О В Л Е Н И Е

ГЛАВЫ НАГОРНОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ

ПЕТУШИНСКОГО РАЙОНА
ВЛАДИМИРСКОЙ ОБЛАСТИ

от 27.06.2012 № 222

Об инструкциях в отношении обработки персональных данных

В соответствии с Федеральным законом от 27.07.200 №152-ФЗ «О персональных данных», с целью обеспечения безопасности персональных данных, обрабатываемых в администрации Нагорного сельского поселения,

п о с т а н о в л я ю:

1.Утвердить следующие инструкции:

1.1.Инструкцию по работе пользователя информационной системы персональных данных администрации Нагорного сельского поселения согласно приложению №1.

1.2.Инструкцию по работе администратора безопасности информационной системы персональных данных администрации Нагорного сельского поселения согласно приложению №2.

1.3.Инструкцию по организации антивирусной защиты информационной системы персональных данных администрации Нагорного сельского поселения согласно приложению №3.

1.4.Инструкцию по применению парольной политики в информационной системе персональных данных администрации Нагорного сельского поселения согласно приложению №4.

1.5.Инструкцию по работе с носителями персональных данных, обрабатываемых в администрации Нагорного сельского поселения согласно приложению №5.

1.6.Инструкцию по работе с обращениями субъектов персональных данных, обрабатываемых в администрации Нагорного сельского поселения согласно приложению №6.

1.7.Инструкцию по обработке персональных данных без использования средств автоматизации в администрации Нагорного сельского поселения согласно приложению №7.

1.8.Инструкцию по обработке персональных данных с использованием средств автоматизации в администрации Нагорного сельского поселения согласно приложению №8.

1.9.Инструкцию о порядке действий во внештатных ситуациях и восстановлению информационной системы после сбоя в администрации Нагорного сельского поселения согласно приложению №9.

2.Постановление вступает в силу со дня подписания и подлежит размещению на официальном сайте администрации Нагорного сельского поселения.

Глава поселения О.И. Копылова

Приложение №1
к постановлению главы
Нагорного сельского поселения
от 27.06.2012 № 222

ИНСТРУКЦИЯ

по работе пользователя информационной системы
персональных данных администрации Нагорного сельского поселения

1. Общие положения

1.1. Пользователем ИСПДн (далее – Пользователь) является штатный сотрудник администрации Нагорного сельского поселения, осуществляющий обработку персональных данных в информационной системе персональных данных.

1.2. Пользователи и уровень их полномочий определяются Разрешительной системой (матрицей) доступа.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю России и регламентирующими документами администрации.

1.5. Методическое руководство работой пользователя осуществляется администратором безопасности информационной системы персональных данных.

2. Должностные обязанности

2.1. Пользователь обязан:

2.1.1. знать и выполнять требования действующих нормативных и руководящих актов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации;

2.1.2. выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены его должностными обязанностями;

2.1.3. знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов;

2.1.4. соблюдать требования парольной политики, определенные Инструкцией по парольной защите ИСПДн;

2.1.5. экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.1.6. обращаться к администратору безопасности ИСПДн для получения консультаций по вопросам работы и настройке элементов ИСПДн;

2.2. Пользователю запрещается:

2.2.1. разглашать защищаемую информацию третьим лицам;

2.2.2. копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

2.2.3. самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

2.2.4. несанкционированно открывать общий доступ к папкам на своей рабочей станции;

2.2.5. подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

2.2.6. отключать (блокировать) средства защиты информации;

2.2.7. обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

2.2.8. сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

2.2.9. привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных;

2.3. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>;

2.4. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных, в пределах возложенных на него функций.

Приложение №2
к постановлению главы
Нагорного сельского поселения
от 27.06.2012 № 222

ИНСТРУКЦИЯ
по работе администратора безопасности информационной системы персональных данных администрации Нагорного сельского поселения

1.Общие положения

1.1.Администратором безопасности ИСПДн (далее – Администратор) является штатный сотрудник администрации Нагорного сельского поселения (далее Администрация), назначенный главой Нагорного сельского поселения.

1.2.Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами администрации.

1.3.Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.4.Администратор безопасности является ответственным должностным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.5.Администратор безопасности осуществляет методическое руководство пользователей ИСПДн, в соответствии со списком допущенных лиц, в вопросах обеспечения безопасности персональных данных.

1.6.Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.7.Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2.Должностные обязанности

Администратор безопасности должен:

-знать и выполнять требования действующих нормативных и руководящих актов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации;

-участвовать в установке и настройке средств защиты, в контрольных и тестовых испытаниях и проверках элементов ИСПДн;

-участвовать в приемке новых программных средств;

-обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам, в соответствии с матрицей доступа;

-уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты;

-вести контроль над процессом осуществления резервного копирования объектов защиты;

-осуществлять контроль над выполнением Плана мероприятий по защите персональных данных;

-анализировать состояние защиты ИСПДн и ее отдельных подсистем;

-контролировать неизменность состояния средств защиты их параметров и режимов защиты;

-контролировать физическую сохранность средств и оборудования ИСПДн;

-контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты;

-контролировать исполнение пользователями парольной политики;

-контролировать работу пользователей в сетях общего пользования и (или) международного обмена;

-своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

-не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;

-не допускать к работе на элементах ИСПДн посторонних лиц;

-осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн;

-оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты;

-периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации;

-в случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

-принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

Приложение №3
к постановлению главы
Нагорного сельского поселения
от 27.06.2012 № 222

ИНСТРУКЦИЯ

по организации антивирусной защиты информационной системы персональных данных администрации Нагорного сельского поселения

1.Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты информационных ресурсов и программных средств вычислительной техники от разрушающего воздействия компьютерных вирусов, а также порядок применения средств антивирусного контроля в автоматизированных системах, предназначенных для обработки информации, содержащей персональные данные (далее ИСПДн).

1.2. Для выполнения антивирусного контроля и защиты ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и рекомендованные к применению Федеральной службой по техническому и экспортному контролю.

1.3. Определение параметров и режимов работы средств антивирусного контроля осуществляется администратором безопасности информации (АБ) ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств и технологическим процессом обработки данных отдельно для каждого рабочего места пользователя.

1.4. Установка и настройка средств антивирусного контроля в ИСПДн осуществляется системным администратором (СА).

2.Требования по применению средств антивирусного контроля

2.1.Обязательному антивирусному контролю подлежат все файлы на машинных носителях, получаемые для обработки в ИСПДн, а также передаваемые из ИСПДн для дальнейшей обработки в других ИСПДн, в том числе других предприятий.

2.2.Вновь получаемые файлы должны пройти антивирусный контроль до начала обработки в ИСПДн.

2.3.Используемые для записи и хранения машинные носители информации (МНИ), перед использованием должны проходить антивирусный контроль.

2.4.Передаваемые в сторонние организации документы и файлы на машинных носителях должны проходить антивирусный контроль непосредственно перед записью на носитель, а запись должна быть выполнена за время текущего сеанса работы пользователя.

2.5.МНИ с программным обеспечением (ПО), при постановке на учет (реестр, список, журнал), должны быть предварительно проверены системным администратором на отсутствие вирусов. В случае отсутствия четкой идентификации вирусов из-за устаревания антивирусной базы, может быть выполнена пробная установка ПО с целью детальной проверки на отсутствия вирусов на «санитарной» ПЭВМ (рабочая модель).

2.6.Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также контроль за соблюдением пользователями ИСПДн установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется АБ и ответственным за обеспечение безопасности персональных данных в ИСПДн.

2.7.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 обязан немедленно сообщить о своих подозрениях АБ. АБ совместно с пользователем и ответственным за обеспечение безопасности персональных данных в ИСПДн должен выполнить внеочередной антивирусный контроль.

2.8.Если при проведении периодической или внеочередной антивирусной проверки информационных ресурсов ИСПДн были обнаружены вирусы или их воздействие на носители информации, АБ обязан:

-приостановить обработку персональных данных в ИСПДн и доложить о случившемся ответственному за эксплуатацию объекта информатизации;

-в присутствии ответственного за обеспечение безопасности персональных данных в ИСПДн провести «лечение» файла;

-в случае обнаружения нового вируса, не поддающегося «лечению» применяемыми антивирусными средствами, исключить из обработки зараженный вирусом файл;

-выполнить проверку всех МНИ в ИСПДн, которые могли стать носителями вируса;

-по факту обнаружения зараженных вирусом файлов АБ составляет служебную записку на имя ответственного за эксплуатацию объекта информатизации, в которой указывает: предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер и степень конфиденциальности информации, тип вируса и выполненные антивирусные мероприятия, список лиц нарушивших (халатное исполнение) установленную технологию обработки данных в ИСПДн, предложения или план мероприятий по ликвидации возможных последствий вирусной атаки.

2.9.Ответственность за организацию антивирусного контроля МНИ в ИСПДн, в соответствии с требованиями настоящей Инструкции, возлагается на АБ.

Приложение №4
к постановлению главы
Нагорного сельского поселения
от 27.06.2012 № 222

ИНСТРУКЦИЯ

по применению парольной политики в информационных системах персональных данных администрации Нагорного сельского поселения

1. Общие положения

1.1. Настоящая инструкция определяет порядок использования, генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных ИСПДн, а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн, а также контроль действий исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности информации (АБ).

2. Парольная политика

2.1. Выбираемые пароли для всех учетных записей пользователей ИСПДн, должны выбираться с учетом следующих требований:

2.1.1. длина пароля должна быть не менее 8 символов;

2.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

2.1.3. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

2.1.4. пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования АРМ, организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);

2.1.5. пароль должен легко запоминаться, для этого используется некоторые приемы, например: для задания пароля используется четверостишье: «Ваше благородие, госпожа удача, для кого Вы добрая, для кого иначе», далее для пароля берут первые буквы «ВбгудкВддки» и в конце добавляется число символов – 11, таким образом, получаем пароль – ВбгудкВддки11;

2.1.6. минимальное время применения пароля - не менее 2 дней;

2.1.7. максимальное время применения пароля - не более чем 93 дня;

2.1.8. пароль не должен повторяться;

2.1.9. пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки АБ.

2.2. Пользователи обязаны хранить свой личный пароль в тайне от других и не передавать любым способом пароль никому;

2.3. Хранение сотрудником (пользователем) значений своих паролей на бумажном носителе и личных идентификаторов допускается только в сейфе.

2.4. Смена пароля учетной записи пользователя должна проводиться регулярно и не реже одного раза в квартал.

2.5. Если для идентификации пользователей используются личные идентификаторы, то:

2.5.1. привязку идентификатора к пользователю (учетной записи) выполняет администратор безопасности информации ИСПДн;

2.5.2. пользователи получают свой идентификатор под роспись;

2.5.3. хранить личный идентификатор допускается в сейфе;

2.5.4. пользователям запрещается передавать свой личный идентификатор;

2.5.5. в случае утери личного идентификатора, пользователь должен немедленно доложить об этом администратору безопасности информации ИСПДн.

2.6. В случае компрометации личного пароля или утери личного идентификатора учетной записи пользователя ИСПДн должны быть немедленно предприняты меры, в соответствии с п. 5 настоящей Инструкции. Кроме того, АБ должно быть проведено служебное расследование по выяснению причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины нанесенного ущерба безопасности информации.

2.7. В случае прекращения полномочий учетной записи пользователя (увольнение, переход на другую работу, в другой отдел или помещение, а также и другие обстоятельства) учетная запись должна быть заблокирована и пароль должен быть заменен, а её идентификатор должен быть сдан АБ сразу после окончания последнего сеанса работы данного пользователя в ИСПДн.

2.8. Владельцы личных паролей и идентификаторов должны быть ознакомлены под роспись с перечисленными выше требованиями. Для этих целей рекомендуется ввести отдельный список для каждой ИСПДн.

Приложение №5
к постановлению главы
Нагорного сельского поселения
от 27.06.2012 № 222

ИНСТРУКЦИЯ

по работе с носителями персональных данных,
обрабатываемых в администрации Нагорного сельского поселения

1. Общие положения

1.1. Настоящая Инструкция определяет правила работы и обеспечения безопасности носителей, содержащих персональные данные субъектов.

1.2. Носители информации (накопители на жестких магнитных дисках) и съемные носители информации (USB, диски, дискеты, переносные носители на жестких магнитных дисках) подлежат учету. Каждый носитель должен быть промаркирован.

1.3. По окончанию эксплуатации носителей информации необходимо производить затирание данных без возможности дальнейшего восстановления информации. Относительно дисков и дискет применяется уничтожение самого носителя любым способом, исключающим возможность его восстановления. Уничтожение носителя проводиться комиссионно с оформлением акта. Акты должны хранятся вместе с журналом учета носителей в сейфе администратора безопасности.

1.4. Окончание эксплуатации носителя фиксируется в журнале учета с соответствующей пометкой (произведено затирание данных или уничтожение носителя).

2. Правила работы со съемными носителями.

2.1. Съемные носители могут использоваться для:

2.1.1. передачи информации, содержащей ПДн, в вышестоящие организации;

2.1.2. переноса информации, содержащей ПДн, между подразделениями организации;

2.1.3. хранения информации, содержащей ПДн.

2.2. Перед работой с отчуждаемым накопителем необходимо проводить антивирусными средствами проверку на вирусы. В случае обнаружения заражения файлов с персональными данными, копирование их на НЖМД АРМ категорически запрещается.

2.3. Съемные носители, на которых могут храниться и передаваться персональные данные, должны храниться в сейфе у администратора

безопасности информационной системы персональных данных.

2.4. Выдача носителей производиться администратором безопасности информационной системы персональных данных сотруднику под роспись в журнале учета. После использования или в конце рабочего дня носитель сдается обратно Администратору безопасности для хранения в сейфе.

Приложение №6
к постановлению главы
Нагорного сельского поселения
от 27.06.2012 № 222

ИНСТРУКЦИЯ

по работе с обращениями субъектов персональных данных,
обрабатываемых в администрации Нагорного сельского поселения

1. Общие положения.

1.1. Настоящая Инструкция определяет правила обработки поступающих к оператору обращений субъектов персональных данных (ПДн).

2. Права субъектов персональных данных.

2.1. В соответствии с действующим законодательством субъект ПДн имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

2.1.1. подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

2.1.2. правовые основания и цели обработки персональных данных;

2.1.3. цели и применяемых оператором способы обработки персональных данных;

2.1.4. наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

2.1.5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

2.1.6. сроки обработки персональных данных, в том числе сроки их хранения;

2.1.7. информацию об осуществленной или о предполагаемой трансграничной передаче данных;

2.1.8. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

2.2. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

2.2.1. обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2.2.2. обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

2.2.3. обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

2.2.4. доступ субъекта персональных данных к его персональным данным нарушает конституционные права и свободы других лиц;

2.2.5. обработка персональных данных осуществляется в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

2.3. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2.4. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3. Действия оператора при обращении субъекта.

3.1. При обращении субъекта или его представителя, сотрудник администрации, ответственный за обработку обращений субъектов, должен предоставить субъекту или его представителю форму заявления/обращения и зарегистрировать его в Журнале установленного образца.

3.2. Заявление/обращение субъекта в течении рабочего дня, в который субъект обратился, передается на рассмотрение главе администрации. На рассмотрение и принятие решения по обращению главе предоставляется 5 рабочих дней, после чего заявление/обращение с резолюцией главы возвращается ответственному за обработку обращений субъектов.

3.3. Ответственный за обработку обращений субъектов в соответствии с вынесенной резолюцией готовит письменный ответ, делает отметку в Журнале и отправляет заказным письмом с уведомлением обратившемуся субъекту, при этом:

3.3.1. администрация обязана сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя;

3.3.2. в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя администрация обязана дать в письменной форме мотивированный ответ, содержащий ссылку на федеральный закон, являющийся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3.4. Администрация обязана сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

Приложение №7
к постановлению главы
Нагорного сельского поселения
от 27.06.2012 № 222

ИНСТРУКЦИЯ

по обработке персональных данных без использования
средств автоматизации в администрации Нагорного сельского поселения

1. Общие положения.

1.1. Настоящая Инструкция разработана на основании требований Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008г. № 687 и устанавливает порядок обработки, распространения и использования персональных данных в администрации Нагорного сельского поселения (далее Администрация) без использования средств автоматизации.

2. Конфиденциальность персональных данных.

2.1. Администрация должна обеспечивать конфиденциальность персональных данных, за исключением:

2.1.1. в случае обезличивания персональных данных;

2.1.2. в отношении общедоступных персональных данных. Общедоступные источники персональных данных могут включать с письменного согласия субъекта его фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

2.2. Конфиденциальность достигается путем разграничения доступа персонала к бумажным носителям с персональными данными.

3. Условия обработки персональных данных.

3.1. Обработка персональных данных должна осуществляться с согласия субъектов персональных данных, за исключением следующих случаев:

3.1.1. обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

3.1.2. обработка персональных данных необходима для осуществления прав и законных интересов администрации или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

4. Порядок обработки персональных данных.

4.1. В администрации поселения обрабатываются персональные данные сотрудников администрации поселения. Список таких персональных данных определен перечнем обрабатываемых персональных данных и перечнем документов, в которых встречаются такие персональные данные.

4.2. Персональные данные сотрудников на бумажных носителях представлены трудовыми договорами, личными делами и учетными картами формы Т2.

4.3. В отношении сотрудников сбор и обработка проводятся на законном основании, в соответствии с трудовым законодательством РФ, без письменного согласия субъекта.

4.4. Персональные данные сотрудников предоставляются ими самими при трудоустройстве в администрацию Нагорного сельского поселения.

4.5. С каждым сотрудником заключается трудовой договор, заводится личное дело и учетная карта формы Т2, к этим документам допускаются только сотрудники, ведущие кадровую работу в администрации.

4.6. Личные дела сотрудников, учетные карты формы Т2 и трудовые договоры хранятся в сейфе отдела организационной и кадровой работы в течение 75 лет.

4.7. Уничтожение бумажных носителей персональных данных производится комиссионно и способами, исключающими возможность восстановления носителя персональных данных.

5. Меры по защите персональных данных.

5.1. Обработка персональных данных, 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 либо имеющих к ним доступ.

5.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер,

необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Приложение №8
к постановлению главы
Нагорного сельского поселения
от 27.06.2012 № 222

ИНСТРУКЦИЯ

по обработке персональных данных с использованием
средств автоматизации в администрации Нагорного сельского поселения

1. Общие положения.

1.1. Настоящая Инструкция разработана на основании требований Федерального закона Российской Федерации от 27 июля 2006 года N 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 17.11.2007г. № 781 и устанавливает порядок обработки, распространения и использования персональных данных в администрации Нагорного сельского поселения (далее - администрация).

2. Конфиденциальность персональных данных.

2.1. Администрация должна обеспечивать конфиденциальность персональных данных работников, за исключением:

2.1.1. в случае обезличивания персональных данных;

2.1.2. в отношении общедоступных персональных данных. Общедоступные источники персональных данных могут включать с письменного согласия субъекта его фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

2.2. Конфиденциальность достигается путем разграничения доступа персонала к ресурсам в соответствии с Разрешительной системой (матрицей) доступа, утвержденной главой администрации.

2.3. Сотрудники администрации несут ответственность за разглашение обрабатываемых персональных данных.

2.4. Администрация при обработке персональных данных обязана принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

3. Условия обработки персональных данных.

Обработка персональных данных должна осуществляться с согласия субъектов персональных данных, за исключением следующих случаев:

-обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

-обработка персональных данных необходима для осуществления прав и законных интересов администрации или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

4. Порядок обработки персональных данных.

4.1. Персональные данные сотрудников вводятся в БД АС «1С v 8.2 Бюджет 2011», «1С v 8.2 Бюджетное государственное учреждение (БГУ)», «СЭД», «1С v 7.7 Камин», «Документы ПУ-5», «1С v 7.7 Бюджеты».

4.2. БД АС «Документы ПУ-5» предназначена для формирования документов индивидуального (персонифицированного) учета страхователем, в соответствии с инструкцией по заполнению форм документов индивидуального (персонифицированного) учета в системе Государственного пенсионного страхования, утвержденной постановлением Правления ПФ РФ и подготовки их для сдачи в электронном виде в территориальный орган ПФ РФ.

4.3. БД АС «1С v 8.2 Бюджет 2011», «1С v 8.2 Бюджетное государственное учреждение (БГУ)», «1С v 7.7 Бюджеты» и «1С v 7.7 Камин» предназначены для ведения кадрового и бухгалтерского учета в администрации.

4.4. Хранение БД происходит локально на АРМ ИСПДн, а так же на сервере ИСПДн.

5. Меры по защите персональных данных.

5.1. Администрация при обработке персональных данных обязана принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.2. Организационные меры:

5.2.1. Оформление перечня персональных данных, подлежащих защите;

5.2.2. Составление матрицы доступа, с указанием должностных лиц, доступных им ресурсов и уровнем доступа (чтение, запись, удаление, модификация);

5.2.3. Назначение ответственных за соблюдением мер безопасности персональных данных;

5.2.4. Расположение мониторов рабочих мест исключающее просмотр видимой информации;

5.2.5. Осуществление охраны помещений во внерабочее время;

5.2.6. Ведение учета съемных носителей с персональными данными. На носителе любым доступным способом указываются следующие учетные реквизиты: учетный номер и дата, пометка «Персональные данные», номер экземпляра, подпись ответственного сотрудника;

5.2.7. Обеспечение оперативной смены паролей и идентификаторов при увольнении или перемещении администраторов безопасности информационных систем персональных данных.

5.3. Технические меры:

5.3.1. Обеспечение защиты от несанкционированного доступа к рабочим местам;

5.3.2. Обеспечение защиты от несанкционированного доступа к средствам обработки и БД персональных данных;

5.3.3. Обеспечение защиты от воздействия вредоносных программ;

5.3.4. Обеспечение защиты от программно-математических воздействий;

5.3.5. Обеспечение стирания остаточной информации на жестком диске и в оперативной памяти рабочих мест, по окончанию обработки персональных данных.

Приложение №9
к постановлению главы
Нагорного сельского поселения
от 27.06.2012 № 222

ИНСТРУКЦИЯ

о порядке действий во внештатных ситуациях и восстановлению информационной системы после сбоя в администрации Нагорного сельского поселения

1. Общие положения и основные понятия

1.1. Настоящая Инструкция о порядке действий пользователей во внештатных ситуациях в администрации Нагорного сельского поселения (далее Администрация) определяет основные меры, методы и средства сохранения (поддержания) работоспособности информационных систем персональных данных (далее – ИСПДн) при возникновении различных внештатных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности ИСПДн и ее основных компонентов. Кроме того, она описывает действия различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

1.2. Ситуация, возникающая в результате нежелательного воздействия на ИСПДн, приведшая к угрозе информационной безопасности, называется внештатной. Внештатная ситуация может возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий, стихийных бедствий. По степени серьезности и размерам наносимого ущерба внештатные ситуации разделяются на следующие категории:

1.2.1. угрожающая – приводящая к полному выходу из строя ИСПДн и неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации. К ним можно отнести:

– нарушение подачи электроэнергии в здании;

– выход из строя файлового сервера (с потерей информации);

– выход из строя файлового сервера (без потери информации);

– частичная потеря информации на сервере без потери его работоспособности;

– выход из строя локальной сети (физической среды передачи данных).

1.2.2. серьезная – приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа. К ним относятся:

– выход из строя рабочей станции (с потерей информации);

– выход из строя рабочей станции (без потери информации);

– частичная потеря информации на рабочей станции без потери ее работоспособности;

– стихийные бедствия (пожар, наводнение, ураган и т.д.).

1.2.3. Источники информации о возникновении внештатной ситуации:

– пользователи, обнаружившие подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;

– средства защиты, обнаружившие кризисную ситуацию;

– системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

2. Общие требования

2.1. Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной внештатной ситуации, должны немедленно оповещаться посредством электронной почты администраторами безопасности ИСПДн. Дальнейшие действия по устранению причин нарушения работоспособности ИСПДн, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

2.2. Каждая внештатная ситуация должна анализироваться администратором безопасности ИСПДн. По результатам этого анализа должны вырабатываться предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.п., при необходимости должно проводится расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

2.3. Серьезная и угрожающая внештатная ситуация могут требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

2.4. Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий. Внешнее хранение подразумевает нахождение копий в выделенных хранилищах (сейфах), находящихся в специально отведенных помещениях.

2.5. Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность и выполнение задач системы (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

2.6. Все программные средства, используемые в системе должны иметь эталонные (дистрибутивные) копии.

2.7. Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала – системные администраторы и администраторы безопасности ИСПДн.

3. Меры обеспечения непрерывной работы и восстановления

3.1. Технические меры:

3.1.1. к техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения внештатных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.1.2. Все критичные помещения администрации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.1.3. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы

ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

– дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. Д.);

– резервные линии электропитания в пределах комплекса зданий;

– аварийные электрогенераторы.

3.1.5. Системы обеспечения отказоустойчивости:

– кластеризация;

– технология RAID.

3.1.6. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

3.1.7. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.1.8. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2. Организационные меры:

3.2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для обрабатываемых персональных данных – не реже раза в неделю;

– для технологической информации – не реже раза в месяц;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

3.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2.4. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

3.2.5. Носители должны храниться не менее года, для возможности восстановления данных.

4. Действия персонала при возникновении внештатных ситуаций

4.1. Сотрудник обнаруживший сбой в работе ИСПДн в результате внештатной ситуации должен незамедлительно поставить в известность администратора безопасности ИСПДн.

4.2. В кратчайшие сроки, не превышающие одного рабочего дня администратором безопасности ИСПДн совместно с системным администратором предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.