АДМИНИСТРАЦИЯ
СЕЛЕКЦИОННОГО СЕЛЬСОВЕТА
ЛЬГОВСКОГО РАЙОНА

РАСПОРЯЖЕНИЕ

№ 12 18 марта 2024г.

О назначении лиц, допущенных к обработке персональных данных и утверждении отдельных Инструкций, Порядка и Положения для осуществления защиты персональных данных в информационной системе персональных данных

В соответствии со «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», утвержденными приказом Гостехкомиссии России, и руководящими и нормативными документами ФСТЭК России и ФСБ России в области защиты персональных данных, а также для организации защиты персональных данных в информационной системе персональных данных:

1. Назначить ответственных лиц, допущенных к обработке персональных данных в информационной системе персональных данных согласно прилагаемому списку (Приложение 1).

2.Утвердить и ввести в действие:

2.1. Инструкцию пользователей информационной системы персональных данных (Приложение 2).

2.1. Инструкцию пользователей по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций (Приложение 3).

2.3. Инструкцию по организации антивирусной защиты (Приложение 4)

2.4. Инструкцию администратора информационной системы персональных данных (Приложение 5).

2.5. Порядок по резервированию и восстановлению работоспособности технических средств и программного обеспечения в информационных системах персональных данных (Приложение 6).

2.6. Положение о разграничении прав доступа к обрабатываемым персональным данным (Приложение 7).

4. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава Селекционного сельсовета
Льговского района С.Ф.Белкин

Приложение № 1
к распоряжению главы Администрации
Селекционного сельсовета
Льговского района
от 18 марта 2024 года

СПИСОК
ответственных лиц, допущенных к обработке персональных данных в информационной системе персональных данных

1) Коростелева Елена Николаевна-заместитель главы Администрации Селекционного сельсовета Льговского района;

2) Фрундин Александр Михайлович - специалист эксперт Администрации Селекционного сельсовета Льговского района .

Приложение 2
к распоряжению главы Администрации
Селекционного сельсовета
Льговского района
от 18 марта 2024 года

Инструкция

пользователю информационной системы персональных данных

Содержание

Сокращения

АРМ	автоматизированное рабочее место
ИСПДн	информационная система персональных данных
ПДн	персональные данные

Общие положения

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку ПДн в ИСПДн Администрации (далее – Администрация).

1.2. Пользователем является каждый сотрудник Администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность согласно действующему законодательству Российской Федерации за свои действия и за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обработке и защите ПДн, руководящими и нормативными документами ФСТЭК России и ФСБ России и регламентирующими документами Администрации.

1.5. Методическое руководство работой пользователя осуществляется Ответственным за защиту ПДн и Администратором ИСПДн.

Должностные обязанности

Пользователь **обязан**:

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

2.2. Выполнять на АРМ только те процедуры, которые определены для него Положением о разграничении прав доступа к обрабатываемым ПДн.

2.3. Знать и соблюдать установленные требования по режиму обработки ПДн, учету, хранению и пересылке носителей информации, защите ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).

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

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Администрации, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к Администратору ИСПДн либо Ответственному за защиту ПДн.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.9. Пользователям **запрещается**:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения Администратора ИСПДн либо Ответственного за защиту ПДн;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своем АРМ;
- запрещено подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;

- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ.

2.10. При отсутствии визуального контроля за АРМ доступ к нему должен быть немедленно заблокирован.

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

Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются Пользователям Администратором ИСПДн.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.4. Правила хранение пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим Пользователям личный пароль и регистрировать их в системе под своим паролем.

3.5. Лица, использующие паролирование, **обязаны**:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
- своевременно сообщать Администратору ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей

Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети **запрещается**:

- осуществлять работу при отключенных средствах защиты (антивирус и др.);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- посещать Интернет-ресурсы, содержащие информацию экстремистского, расистского, порнографического и криминального характера, а также загружать данные, содержащие подобную информацию;
- использовать адрес корпоративной почты при регистрации на Интернет-ресурсах, в ходе деятельности, не связанной с выполнением должностных обязанностей;
- скачивать из Сети медиа-файлы развлекательного характера, программное обеспечение и другие файлы;
- размещать в сети Интернет информацию, принадлежащую нашей Компании, классифицированную как "для служебного пользования", "персональные данные", "коммерческая тайна";

4.3. Организация оставляет **за собой право**:

- осуществлять мониторинг использования сотрудниками Администрации сети Интернет;
- определять перечень запрещенных Интернет-ресурсов и осуществлять блокировку доступа к ним;
- осуществлять мониторинг появления адресов корпоративной почты на страницах Интернет-ресурсов;
- осуществлять мониторинг появления информации конфиденциального характера о деятельности Администрации в сети Интернет, в том числе и на страницах социальных сетей, таких как www.vkontakte.ru, www.odnoklassniki.ru и др.;
- предоставлять информацию об использовании Интернет-ресурсов сотрудниками Администрации правоохранительным органам в случаях, предусмотренных законодательством Российской Федерации;
- принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей инструкции.

Правила работы с корпоративной электронной почтой

5.1 Электронная почта является собственностью Администрации и может быть использована **ТОЛЬКО** в служебных целях. Использование электронной почты в других целях категорически **ЗАПРЕЩЕНО**.

5.2 Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию руководства Администрации.

5.3 При работе с корпоративной системой электронной почты сотрудникам компании **запрещается**:

- использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с руководством Администрации;
- публиковать свой адрес, либо адреса других сотрудников компании на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- отправлять сообщения с вложенными файлами общий объем которых превышает ___ Мегабайт.
- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
- осуществлять массовую рассылку почтовых сообщений внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;
- осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с руководством Администрации;
- рассылка через электронную почту материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;
- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны.
- распространять информацию содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.
- распространять информацию ограниченного доступа, представляющую коммерческую тайну;
- предоставлять, кому бы-то ни было пароль доступа к своему почтовому ящику.

Ответственный за защиту ПДн Е.Н.Коростелева

Приложение № 3
к распоряжению главы Администрации
Селекционного сельсовета
Льговского района
от 18 марта 2024 года

Инструкция
пользователю по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

Содержание

Сокращения

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные

1 Назначение и область действия

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Организации, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех сотрудников Организации, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

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

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в год.

2 Порядок реагирования на аварийную ситуацию

Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых Пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении 1.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Организации (Ответственный за защиту ПДн, Администратор ИСПДн, Пользователи ИСПДн) 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.

Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

- Уровень 1 – **Незначительный инцидент**. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты.
- Уровень 2 – **Авария**. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты.

К авариям относятся следующие инциденты:

- отказ элементов ИСПДн и средств защиты из-за:
  - повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
  - сбоя системы кондиционирования;
- отсутствие Ответственного за защиту ПДн, Администратора ИСПДн более чем на сутки из-за:
  - химического выброса в атмосферу;
  - сбоев общественного транспорта;
  - эпидемии;

- массового отравления персонала;
- сильного снегопада;
- торнадо;
- сильных морозов.

- Уровень 3 – **Катастрофа**. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки в непосредственной близости от ИСПДн.

3 Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

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

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех сотрудников Организации, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу.

По окончанию ознакомления сотрудник расписывается в журнале, предоставляемом Ответственным за реагирование сотрудником. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

Должно быть проведено обучение должностных лиц Организации, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

Администратор ИСПДн должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

Ответственный за защиту ПДн Е.Н.Коростелева

Приложение
к Инструкции пользователя по
обеспечению безопасности обработки
персональных данных при возникновении
внештатных ситуаций

Источники угроз

Таблица №1 – Источники угроз

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телеком и ИТ угрозы	
17	Сбой системы кондиционирования
18	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
19	Ошибка персонала, имеющего доступ к серверной
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21	Отключение электроэнергии
22	Сбой в работе интернет-провайдера
23	Физический разрыв внешних каналов связи

Ответственный за защиту ПДн Е.Н.Коростелева

Приложение № 4
к распоряжению главы Администрации
Селекционного сельсовета
Льговского района
от 18 марта 2024 года

ИНСТРУКЦИЯ
по организации антивирусной защиты

Содержание

Сокращения

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные

1 Общие положения

1.1. Настоящая Инструкция определяет требования к организации антивирусной защиты ИСПДн Администрации.

1.2. Установка средств антивирусной защиты осуществляется Администратором ИСПДн в соответствии с эксплуатационной документацией на антивирусное средство. Настройка параметров средств антивирусной защиты осуществляется Администратором ИСПДн в соответствии с руководством по применению антивирусного средства.

2 Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы и др.), получаемая на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

2.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические антивирусные проверки электронных архивов должны проводиться еженедельно.

2.4. Непосредственно после установки программного обеспечения должна быть выполнена его антивирусная проверка.

2.5. 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 самостоятельно или вместе с Администратором ИСПДн должен провести внеочередной антивирусный контроль.

2.6. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи **обязаны**:

- остановить обработку информации;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора ИСПДн и владельца зараженных файлов;
- совместно с Администратором ИСПДн провести анализ возможности дальнейшего их использования;
- провести уничтожение вирусов в зараженных файлах.

2.7. В случае обнаружения на жестком магнитном диске не поддающегося лечению вируса, Администратор ИСПДн обязан поставить в известность Ответственного за защиту ПДн, запретить работу на АРМ и в возможно короткие сроки обновить антивирусное средство. После обновления антивирусного средства произвести повторное лечение вируса. При невозможности вылечить вирус необходимо поставить в известность Ответственного за защиту ПДн для принятия решения об его уничтожении.

3 Ответственность

Ответственность за организацию антивирусного контроля ИСПДн в соответствии с требованиями настоящей Инструкции возлагается на

Администратора ИСПДн.

Ответственность за непосредственное проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на Администратора ИСПДн и пользователей ИСПДн.

Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции пользователями ИСПДн организуется Администратором ИСПДн.

Ответственный за защиту ПДн Е.Н.Коростелева

Приложение № 5
к распоряжению главы Администрации
Селекционного сельсовета
Льговского района
от 18 марта 2024 года

Инструкция
администратору информационной системы
персональных данных

Содержание

Сокращения

ИСПДн	Информационная система персональных данных
ПДн	Персональные данные

Общие положения

1.1. Администратор ИСПДн (далее – Администратор) назначается Распоряжением главы Администрации сельского поселения.

1.2. Администратор в своей работе руководствуется настоящей Инструкцией, Положением об обработке и защите персональных данных, законодательными и иными нормативными актами Российской Федерации в области защиты ПДн, руководящими и нормативными документами ФСТЭК России и ФСБ России, приказами и указаниями руководства Организации.

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

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке ПДн.

1.5. Администратор должен иметь специальное рабочее место, размещенное в здании Организации так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.6. Методическое руководство работой Администратора осуществляется Ответственным за защиту ПДн.

Должностные обязанности

Администратор **обязан**:

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

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

- программного обеспечения автоматизированных рабочих мест и серверов (операционные системы, прикладное и специальное программное обеспечение);
- средств антивирусной защиты;
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.4. Участвовать в приемке новых программных средств.

2.5. Обеспечивать доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.6. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.7. Контролировать физическую сохранность средств и оборудования ИСПДн.

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

2.9. Обеспечивать функционирование и поддерживать работоспособность средств защиты.

2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.11. Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.12. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.13. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.14. Осуществлять периодические контрольные проверки автоматизированных рабочих мест.

2.15. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по

их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.16. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля пользователями ИСПДн. Проводить полную плановую смену паролей в ИСПДн не реже одного раза в 3 месяца

2.17. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по защите информации.

2.18. Информировать Ответственного за защиту ПДн о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

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

2.20. Обеспечивать строгое выполнение требований по защите информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки ПДн, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения защищаемой информации.

2.21. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

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

2.23. Принимать меры по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.24. Оказывать помощь Пользователям в части применения средств защиты и консультировать по вопросам введенного режима защиты.

Порядок парольной защиты

3.1. Администратор осуществляет организационно-техническое обеспечение процессов установки и смены действия паролей пользователей ИСПДн.

3.2. Личные пароли должны генерироваться и распределяться централизованно Администратором, и при этом необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 6-ти буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567, qwerty и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;
- не использовать ранее использованные пароли.

3.3. Внеплановая смена пароля пользователя должна производиться в случае прекращения полномочий работника Организации (увольнение, переход на другую должность/работу и другие обстоятельства).

3.4. В случае компрометации личного пароля пользователя ИСПДн Администратор производит замену пароля данного пользователя и информирует Ответственного за защиту ПДн о произошедшем факте компрометации.

3.5. Хранение значений паролей на бумажном носителе допускается только в «Журнале учета персональных идентификаторов и паролей», хранящемся в запираемом сейфе.

Ответственность

3.1. Администратор **несет персональную ответственность за**:

- правильное и своевременное выполнение приказов, распоряжений, указаний руководства Организации и Ответственного за защиту ПДн по вопросам, входящим в возложенные на него функции;
- выполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией;
- соблюдение трудовой дисциплины, охраны труда;
- качество проводимых работ по защите ПДн в соответствии с функциональными обязанностями.

3.2. Администратор также **несет персональную ответственность** согласно действующего законодательства Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду деятельности.

Ответственный за защиту ПДн Е.Н.Коростелева

Приложение № 6
к распоряжению главы Администрации
Селекционного сельсовета
Льговского района
от 18 марта 2024 года

Инструкция

по резервированию и восстановлению работоспособности технических средств и программного обеспечения в информационных системах персональных данных

СОДЕРЖАНИЕ

Назначение и область действия

Инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации (далее – Инструкция) определяет действия, связанные с функционированием ИСПДн Администрации и, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей Администрации, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

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

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Ответственный за защиту ПДн.

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор ИСПДн.

Порядок реагирования на инцидент

В настоящей Инструкции под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти в результате:

- непреднамеренных действий пользователей;
- преднамеренных действий пользователей и третьих лиц;
- нарушения правил эксплуатации технических средств ИСПДн;
- возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники (Ответственный за защиту ПДн, Администратор ИСПДн и Пользователь ИСПДн) 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.

Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

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

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

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

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.

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.

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

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.

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.

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

Организационные меры

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).

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

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

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

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

Ответственный за защиту ПДн Е.Н.Коростелева

Приложение № 7
к распоряжению главы Администрации
Селекционного сельсовета
Льговского района
от 18 марта 2024 года

ПОЛОЖЕНИЕ
о разграничении прав доступа к обрабатываемым персональным данным

Настоящее Положение о разграничении прав доступа к обрабатываемым персональным данным разработан на основании нормативно-методического документа «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» и определяет порядок и правила доступа работников Организации к информационным ресурсам информационных систем персональных данных (ИСПДн) Организации.

Перед предоставлением работнику доступа к информационным ресурсам ИСПДн, условия предоставления доступа отражаются в трудовом договоре работника в разделе о защите сведений ограниченного доступа, а также должностных обязанностях работников Организации.

К работе в ИСПДн допускаются работники, ознакомившиеся с настоящим Положением, Положением по организации и проведению работ по обеспечению безопасности персональных данных, Перечнем персональных данных и технологической информации, подлежащих защите в информационных системах персональных данных Организации.

Учетная запись нового работника (пользователя) с соответствующими правами доступа создается администратором ИСПДн по представлению начальника структурного подразделения данного работника с письменного разрешения Главы Администрации.

Сотрудники, допущенные к работе с персональными данными, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с требованиями законодательных, правовых актов и нормативно-распорядительных документов Российской Федерации.

Контроль доступа работников (пользователей) структурных подразделений Организации к информационным ресурсам ИСПДн и обеспечение информационной безопасности при работе с информационными ресурсами ИСПДн возлагается на администратора ИСПДн.

Перечень ИСПДн Организации определен по результатам «Отчёта о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных Организации:

1. АИС "ЗУМО"
2. АИС ВУС
3. АИС Похозяйственный учет
4. АИС Система обработки запросов (СОЗ)

Доступ работников к защищаемым информационным ресурсам ИСПДн приведен ниже.

Таблица 1 – Доступ к ресурсам ИСПДн

№ п/п	Фамилия и инициалы сотрудника	Должность	ИСПДн	Полномочия[1]
1.	Ахунова Р.М.	Управляющий делами	ВУС	+
			Похозяйственный учет	+
			СОЗ	+
2.	Ахматьянова И.З.	Специалист	Похозяйственный учет	+
			ЗУМО	+

Ответственный за защиту ПДн Е.Н. Коростелева

[1] «+» – полные права на доступ; «-» – отсутствуют права на доступ; «Ч» – читать файлы (массивы информации); «З» – записывать: добавлять (создавать) файлы (массивы информации), вносить изменения, удалять файлы (массивы информации), сохранять (записывать) на учтенные магнитные носители, распечатывать на принтере файлы (массивы информации).

Ознакомлены:

№ пп	Фамилия, имя и отчество	Наименование подразделения	Должность	Дата	Подпись
1.	Ахунова Р.М.		Управляющий делами		
2.	Ахматьянова И.З.		Специалист		
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					