Проект

РОССИЙСКАЯ ФЕДЕРАЦИЯ

РОСТОВСКАЯ ОБЛАСТЬ

МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ «НОВОБЕССЕРГЕНЕВСКОЕ СЕЛЬСКОЕ ПОСЕЛЕНИЕ»

**Администрация Новобессергеневского сельского поселения**

**РАСПОРЯЖЕНИЕ**

от 2021 №

с. Петрушино

|  |
| --- |
| **Об утверждении инструкции «О мерах по обеспечению информационной безопасности на рабочем месте» в Администрации Новобессергеневского сельского поселеиня** |

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» а также в целях обеспечения информационной безопасности на автоматизированных рабочих местах пользователей администрации Новобессергеневского сельского поселения:

1. Утвердить инструкцию «О мерах по обеспечению информационной безопасности на рабочем месте» в Администрации Новобессергеневского сельского поселения согласно приложению к данному распоряжению.

2. Всех работников Администрации ознакомить с настоящей инструкцией под роспись.

4. Контроль за исполнением распоряжения оставляю за собой.

**Глава Администрации**

**Новобессергеневского сельского**

**поселения В.В.Сердюченко**

Распоряжение вносит специалист по правовой и кадровой работе Администрации

Новобессергеневского сельского поселения

Приложение

к распоряжению Администрации

Новобессергеневского сельского поселения

от №

**УТВЕРЖДАЮ:**

**Глава Администрации**

**Новобессергеневского сельского поселеиня**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.В.Сердюченко**

**ИНСТРУКЦИЯ**

**«О мерах по обеспечению информационной безопасности на рабочем месте»**

**в Администрации Новобессергеневского сельского поселения**

**2021 год**

**РАЗДЕЛ 1. Инструкция пользователя информационной системы персональных данных**

# Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных Администрации Новобессергеневского сельского поселения: (далее - Администрация).

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

1.3. Пользователь несёт 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 (ФСТЭК) России и другими регламентирующими документами Администрации по защите информации.

1.5. Методическое руководство работой пользователя системным администратором Администрации.

# 2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования настоящей инструкции и других внутренних распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

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

2.4. Соблюдать требования парольной политики и антивирусной защиты (раздел 3, 4).

2.5. Соблюдать правила при работе в сетях общего доступа и международного обмена – Интернет (раздел 5).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Администрации, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к системному администратору или к ответственному за обеспечение безопасности персональных данных.

2.8. Для получения консультаций по вопросам работы и настройке элементов информационной системы персональных данных необходимо обращаться в сектор информационно-коммуникационных технологий и защиты информации.

2.9. Пользователям запрещается:

* Разглашать защищаемую информацию третьим лицам.
* Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
* Самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
* Хранить личную информацию (фото, музыку, фильмы и т.д.) на любых корпоративных ресурсах, будь то компьютеры или файловые хранилища, а также передавать ее по корпоративной почте и другим каналам связи.
* Забирать свой рабочий ноутбук домой.
* Несанкционированно открывать общий доступ к ресурсам.
* 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 информационной системе персональных данных.
* Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системе персональных данных.
* Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с системным администратором.
* Оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, носители и распечатки, содержащие персональные данные.

2.10. 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>, либо <Windows><L>.

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

# 3. Организация парольной защиты

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям в секторе информационно-коммуникационных технологий и защиты информации, или создаются пользователем самостоятельно.

3.2. Правила формирования пароля:

* Пароль не может содержать имя учетной записи пользователя или какую либо его часть.
* Пароль должен состоять не менее чем из 8 символов.
* В пароле должны присутствовать символы трех категорий из числа следующих четырех:

-прописные буквы английского алфавита от A до Z;

-строчные буквы английского алфавита от a до z;

-десятичные цифры (от 0 до 9);

-символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

* Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.
* Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.
* Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
* Запрещается выбирать пароли, которые уже использовались ранее.

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 хранения 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 в сектор системному администратору об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

**4. Антивирусная защита**

4.1. В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов получаемых:

− по электронной почте;

− через сеть интернет;

− на магнитном, оптическом диске, флеш-накопителе;

− на ином съемном носителе информации;

− полученные иным способом.

4.2. Пользователю запрещается:

* Осуществлять действия, направленные на выключение антивирусной программы.
* Самостоятельно устанавливать на АРМ программное обеспечение.
* Запускать файлы, полученные по сетям связи (электронной почте, интернет), со съемных носителей, даже если они получены от проверенного адресата, без предварительной их проверки антивирусной программой.

4.3. 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 ответственным за обеспечение безопасности персональных данных должен провести внеочередной антивирусный контроль своего рабочего места.

4.4. В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны:

* приостановить работу;
* немедленно поставить в известность о факте обнаружения вирусного заражения ответственного за обеспечение безопасности персональных данных;
* 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 ответственного за обеспечение безопасности персональных данных).

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

5.1. Работа в сетях общего доступа и международного обмена (сети Интернет) (далее – Интернет) на элементах информационной системы персональных данных, должна проводиться при служебной необходимости.

5.2. При работе в Интернете запрещается:

* Осуществлять работу при отключенных средствах защиты (антивирус и других).
* Передавать по Интернету защищаемую информацию без использования средств шифрования.
* Скачивать из Интернета программное обеспечение и исполняемые файлы (файлы с расширением exe, dll, msi).
* Посещение сайтов сомнительной репутации (сайты непристойного содержания, сайты содержащие нелегально распространяемое ПО и другие).
* Нецелевое использование подключения к Интернету и/или в личных целях.
* Осуществлять отправку электронных почтовых сообщений, содержащих конфиденциальную информацию, по открытым каналам.
* Использовать иные, кроме служебных, почтовые ящики для электронной переписки.

**6. Установка программного обеспечения на АРМ**

6.1. Правом установки и настройки операционной системы (ОС) и средств криптографической защиты информации (СКЗИ) должен обладать только сотрудник системный администратор.

6.2. Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.

6.3. На технических средствах АРМ с установленным СКЗИ необходимо использовать только лицензионное программное обеспечение фирм-изготовителей, полученное из доверенных источников.

6.4. На АРМ должна быть установлена только одна операционная система. При этом не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

6.5. Рекомендуется ограничить возможности пользователя запуском только тех приложений, которые разрешены сотрудниками системный администратор

6.6. Рекомендуется установить и использовать на АРМ антивирусное программное обеспечение, а также обновлять антивирусные базы.

**7. Установка и настройка СКЗИ**

7.1. Установка и настройка СКЗИ на АРМ должна выполняться в присутствии работника системного администратора.

7.2. Установка СКЗИ на АРМ должна производиться только с дистрибутива, полученного по доверенному каналу.

7.3. Установка СКЗИ и первичная инициализация ключевой информации осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

7.4. При установке ПО СКЗИ на АРМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ.

7.5. Рекомендуется перед установкой произвести проверку ОС на отсутствие вредоносных программ с помощью антивирусных средств.

7.6. По завершении инициализации осуществляются настройка и контроль работоспособности ПО.

7.7. Запрещается вносить какие-либо изменения, не предусмотренные эксплуатационной документацией, в программное обеспечение СКЗИ.

## ****8. Порядок работы с носителями ключевой информации****

8.1. В некоторых подсистемах организации для обеспечения контроля за целостностью передаваемых по технологическим каналам электронных документов (**ЭД**), а также для подтверждения их подлинности и авторства могут использоваться средства электронной подписи (**ЭП**).

8.2. Работнику организации (владельцу ключа ЭП), которому в соответствии с его должностными обязанностями предоставлено право постановки на ЭД его ЭП, выдается персональный ключевой носитель информации, на который записана уникальная ключевая информация (ключ ЭП), относящаяся к категории сведений ограниченного распространения.

8.3. Персональные ключевые носители (эталон и рабочую копию) владелец ключа ЭП должен хранить в специальном месте, гарантирующем их сохранность.

8.4. Владелец ключа **ОБЯЗАН**:

* под подпись в получить ключевые носители, убедиться, что они правильно маркированы и на них установлена защита от записи;
* использовать для работы только рабочую копию своего ключевого носителя;
* сдавать свой персональный ключевой носитель на временное хранение руководителю подразделения или ответственному за обеспечение безопасности персональных данных в период отсутствия на рабочем месте (например, на время отпуска или командировки);
* в случае порчи рабочей копии ключевого носителя (например, при ошибке чтения) владелец ЭП обязан передать его уполномоченному сотруднику, который должен в присутствии исполнителя сделать новую рабочую копию ключевого носителя с имеющегося эталона и выдать его взамен испорченного. Испорченная рабочая копия ключевого носителя должна быть уничтожена.

8.5. Владельцу ключа ЭП **ЗАПРЕЩАЕТСЯ**:

* оставлять ключевой носитель без личного присмотра;
* передавать свой ключевой носитель (эталонную или рабочую копию) другим лицам (кроме как для хранения руководителю подразделения или ответственному за обеспечение безопасности персональных данных);
* делать неучтенные копии ключевого носителя, распечатывать или переписывать с него файлы на иной носитель информации (например, жесткий диск персонального компьютера), снимать защиту от записи, вносить изменения в файлы, находящиеся на ключевом носителе;
* использовать ключевой носитель на заведомо неисправном дисководе и/или персональном компьютере;
* подписывать своим персональным ключом ЭП любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом;
* сообщать третьим лицам информацию о владении ключом ЭП для данного технологического процесса.

8.6. Действия при компрометации ключей

8.6.1. Если у владельца ключа ЭП появилось подозрение, что его ключевой носитель попал или мог попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу с ключевым носителем, сообщить об этом системному администратору, сдать скомпрометированный ключевой носитель с пометкой в журнале учета ключевых носителей о причине компрометации, написать служебную записку о факте компрометации персонального ключевого носителя на имя руководителя подразделения.

8.6.2. В случае утери ключевого носителя владелец ключа ЭП обязан немедленно сообщить об этом в сектор информационно-коммуникационных технологий и защиты информации, написать объяснительную записку об утере ключевого носителя на имя руководителя подразделения и принять участие в служебной проверке по факту утери ключевого носителя.

8.6.3. Ответственный за обеспечение безопасности персональных данных обязан немедленно оповестить о факте утраты или компрометации ключевого носителя руководство организации для принятия действий по блокированию ключей для ЭП указанного исполнителя.

8.6.4. По решению руководства организации установленным порядком владелец ключа ЭП может получить новый комплект персональных ключевых носителей взамен скомпрометированных.

8.6.5. В случае перевода владельца ключа ЭП на другую работу, увольнения или прекращения трудовых отношений иным образом он обязан сдать (сразу по окончании последнего сеанса работы) свой ключевой носитель ответственному за обеспечение безопасности персональных данных под подпись в журнале учёта.

# 9. Ответственность

9.1. Пользователи, нарушившие требования данной инструкции, расцениваются как нарушители Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных» и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.