Приложение №19

УТВЕРЖДЕНА

распоряжением

администрации

от 23.04.2021 № 82

Инструкция
пользователю информационной системы персональных данных
в администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области

Сокращения

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

1. Общие положения

1.1. Пользователь ИСПДн (далее - Пользователь) осуществляет обработку ПДн в ИСПДн администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области (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 обеспечение безопасности ПДн и администраторами ИСПДн.

2. 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 разрешительной системе допуска пользователей и обслуживающего персонала к информационным ресурсам и системе защиты персональных данных.

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 обеспечение безопасности 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 обеспечение безопасности 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.

3. Организация парольной защиты

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

3.2. Полная плановая смена паролей в ИСПДн проводится администраторами ИСПДн.

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.

4. 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, классифицированную как «для служебного пользования», «персональные данные», «коммерческая тайна»;

4.3. Администратор ИСПДн 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.vk.com, 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.

5. 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 главы администрации.

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

- использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с главой 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 5 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;

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 быто ни было пароль доступа к своему почтовому ящику.

6. Порядок действия пользователя при возникновении инцидента информационной безопасности

При выходе из строя СЗИ необходимо:
- немедленно прекратить обработку информации на объекте;
- обратиться к администратору информационной безопасности.

При выходе из строя составных частей ИСПДн:
- немедленно прекратить обработку информации на объекте;
- обратиться к администратору информационной безопасности.

7. Ответственность пользователя

На пользователя возлагается персональная ответственность за соблюдение установленного режима защиты информации ограниченного распространения в соответствии с его функциональными обязанностями, определенными настоящей Инструкцией.

Пользователь несет ответственность в соответствии с действующим законодательством РФ за нарушение требований настоящей Инструкции.