

**ГЛАВА ГОРОДСКОГО ПОСЕЛЕНИЯ смышлЯЕВКА муниципального района Волжский**

**самарской области**

 ПОСТАНОВЛЕНИЕ

 от 20.03.2020 г № 225

**Об утверждении** **инструкции пользователя информационных систем персональных данных Администрации городского поселения Смышляевка муниципального района Волжский Самарской области**

 В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Уставом городского поселения Смышляевка муниципального района Волжский Самарской области, ПОСТАНОВЛЯЮ:

1.Утвердить инструкцию пользователя информационных систем персональных данных Администрации городского поселения Смышляевка муниципального района Волжский Самарской области

2.Опубликовать настоящее Постановление в газете « Мой поселок».

3. Настоящее Постановление вступает в силу с момента его официального опубликования.

4. Контроль за исполнением настоящего Постановления оставляю за собой.

Глава администрации

городского поселения Смышляевка В.М. Брызгалов

Дементьева9992482

**Инструкция пользователя информационных систем персональных данных Администрации** **городского поселения Смышляевка муниципального района Волжский Самарской области**

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Пользователем информационных систем персональных данных (далее – Пользователь) является уполномоченный сотрудник Администрации городского поселения Смышляевка муниципального района Волжский Самарской области.

1.2. Пользователь должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности персональных данных (далее – ПДн).

 1.3. В своей деятельности, связанной с обработкой ПДн, Пользователь руководствуется Политикой в отношении обработки персональных данных в Администрации и настоящей Инструкцией.

1.4. Пользователи, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющие доступ к аппаратным средствам, программному обеспечению и обрабатываемой информации, несут персональную ответственность за свои действия.

 2 ОБЯЗАННОСТИ И ПРАВА ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Пользователь обязан:

– соблюдать требования Политики в отношении обработки персональных данных в Администрации и иных нормативных актов Администрации, устанавливающих порядок работы с ПДн;

– выполнять в информационных системах персональных данных (далее – ИСПДн) только те процедуры, которые необходимы для исполнения его должностных обязанностей;

 – использовать для выполнения должностных обязанностей только предоставленное ему автоматизированное рабочее место (далее – АРМ) на базе персонального компьютера (автономной ПЭВМ);

 – пользоваться только зарегистрированными в установленном порядке съемными (отчуждаемыми) машинными носителями информации;

 – обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним;

 – немедленно сообщать руководителю структурного подразделения или ответственному за обеспечение безопасности ПДн в ИСПДн (далее – Ответственный) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;

 – перед началом обработки в ИСПДн файлов, хранящихся на съемных носителях информации, Пользователь должен осуществлять проверку файлов на наличие компьютерных вирусов. Антивирусный контроль на АРМ должен осуществляться Пользователем не реже одного раза в неделю;

 – располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами;

– соблюдать установленный режим разграничения доступа к информационным ресурсам: получать пароль, надежно его запоминать и хранить в тайне. 10.2. Пользователям ИСПДн запрещается:

 – записывать и хранить информацию, относящуюся к конфиденциальной информации или ПДн, на неучтенных материальных носителях информации;

 – оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка информации;

– отключать средства антивирусной защиты;

– отключать (блокировать) средства защиты информации;

– производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

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

– обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИСПДн;

 – сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам в ИСПДн;

– работать в ИСПДн при обнаружении каких-либо неисправностей;

– хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;

– вводить в ИСПДн ПДн под диктовку или с микрофона;

 – привлекать посторонних лиц для производства ремонта технических средств ИСПДн без согласования с Ответственным.

2.3. Пользователь имеет право знакомиться с внутренними документами Администрации Семикаракорского района, регламентирующими его обязанности по занимаемой должности.

3. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ ПРИ РАБОТЕ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

3.1. Пароли доступа к ИСПДн устанавливаются Ответственным или Пользователем. 3.2. При формировании пароля необходимо руководствоваться следующими требованиями:

 – длина пароля должна быть не менее 8-и 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) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;

– 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.);

– 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;

– запрещается использовать ранее использованные пароли. 1

1.3. При организации парольной защиты запрещается:

– записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

 – хранить пароли в записанном виде на отдельных листах бумаги; – сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от НСД.

4. ПОРЯДОК ПРИМЕНЕНИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

4.1. Плановую смену паролей на доступ в ИСПДн рекомендуется проводить один раз в месяц.

4.2. Пользователь обязан незамедлительно сообщить Ответственному факты утраты, компрометации ключевой, парольной и аутентифицирующей информации.

4.3.Внеплановая смена личного пароля должна производиться в обязательном порядке в следующих случаях:

– компрометации (подозрении на компрометацию) пароля;

 – в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) Пользователя (в течение 24 часов после окончания последнего сеанса работы данного с ИСПДн); – по инициативе Ответственного.

5. ТЕХНОЛОГИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При первичном допуске к работе с ИСПДн Пользователь:

– проходит инструктаж по использованию ИСПДн;

– знакомится с требованиями действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;

– получает у Ответственного идентификатор и личный пароль для входа в ИСПДн. 5.2. Перед началом работы Пользователь визуально проверяет целостность пломб, убеждается в отсутствии посторонних технических средств, включает необходимые средства вычислительной техники.

5.3. Авторизацию в ИСПДн (ввод личного идентификатора и пароля) Пользователь осуществляет при отсутствии в помещении посторонних лиц.

5.4.В процессе работы на АРМ ИСПДн Пользователь использует технические средства и установленное Ответственным программное обеспечение согласно Техническому паспорту ИСПДн.

5.5.Копирование ПДн на электронные носители информации осуществляется только при наличии производственной необходимости и только на учтенные электронные носители информации.

5.6. При необходимости создания на АРМ Пользователя дополнительных электронных документов, содержащих ПДн, Пользователь создает и хранит такие документы в строго отведенном для этого месте.

5.7. Печать документов, содержащих ПДн, осуществляется только при наличии производственной необходимости на принтер, подключенный Ответственным к АРМ Пользователя. Все бумажные носители, не подлежащие учету по каким-либо техническим или иным причинам (сбой принтера при печати, обнаружение ошибок в документе после распечатки и т.д.) уничтожаются незамедлительно с применением уничтожителей бумаги. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих ПДн, уничтожаются с применением уничтожителей бумаги незамедлительно после подписания (утверждения) окончательного варианта документа.

 5.8.В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИСПДн, Пользователь обязан выключить компьютер, либо

заблокировать его, для чего нужно нажать комбинацию клавиш и выбрать в диалоговом окне кнопку «Блокировать». Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других служащих Администрации, Пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа.

5.9. Покидая рабочее помещение в конце рабочего дня, Пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.