

УТВЕРЖДЕНО

Распоряжением Администрации
Кинель-Черкасского района

от «03 » ноября №443-р

**Инструкция пользователя
информационных систем персональных данных
администрации муниципального района
Кинель-Черкасский Самарской области**

2015 г.

1. Общие положения

1.1 Настоящий документ разработан в соответствие с нормативными документами в области защиты персональных данных и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) в Администрации муниципального района Кинель-Черкасский Самарской области (далее – Учреждение).

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

1.3 ИСПДн принадлежат Учреждению.

1.4 В соответствии с «Актом классификации ...» ИСПДн присвоен 4 уровень защищенности.

1.5 Доступ ответственного за обеспечение безопасность персональных данных (далее – ответственное лицо) и пользователей к ресурсам ИСПДн осуществляется в соответствии с утвержденным перечнем.

1.6 Пользователь в своей работе руководствуется настоящей инструкцией, локальными организационно-распорядительными документами Учреждения в области обработки персональных данных, руководящими и методическими документами ФСТЭК России.

1.7 Пользователи получают свои права на доступ к ресурсам ИСПДн через ответственное лицо.

1.8 Общее руководство и контроль за обеспечением информационной безопасности пользователями ИСПДн и обслуживающим персоналом осуществляют ответственное лицо.

1.9 Изменения и дополнения к данной инструкции утверждаются в установленном порядке.

2. Требования к пользователям ИСПДн

2.1 Пользователи, не ознакомленные с данной инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ИСПДн не допускаются.

2.2 Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному лицу.

2.3 Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к ответственному лицу.

2.4 Пользователи **ОБЯЗАНЫ**:

2.4.1 знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите персональных данных;

2.4.2 выполнять требования ответственного лица;

2.4.3 выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены в технологическом процессе обработки ПДн;

2.4.4 строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами ИСПДн;

2.4.5 строго соблюдать правила работы со средствами защиты информации, установленными на объекте информатизации;

2.4.6 знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн;

2.4.7 в процессе первичной регистрации заявить ответственному лицу перечень необходимых для его работы ресурсов, перечень персональных данных, состав необходимого общесистемного программного обеспечения для решения поставленных задач;

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

2.4.9 осуществлять резервное копирование, уничтожение и восстановление информации в рамках выделенных полномочий, либо через обращение к ответственному лицу. Пользователь осуществляет резервное копирование информации в процессе, либо по окончании работы на соответствующим образом учтенные носители;

2.4.10 при отсутствии на рабочем месте блокировать доступ к ПЭВМ путем одновременного нажатия комбинации клавиш **<Ctrl><Alt>** и выбрать опцию **<Блокировка>**;

2.4.11 принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках выделенных полномочий;

2.4.12 немедленно ставить в известность ответственное лицо обо всех неисправностях и нарушениях в работе технических средств (далее – ТС), средств защиты информации (далее – СЗИ), прикладного и системного программного обеспечения (далее – ПО) и в случаях обнаружения:

- факта утраты или подозрения на утечку своих идентификаторов и паролей;
- нарушений целостности пломб (наклеек), нарушении или несоответствии номеров печатей на аппаратных средствах ИСПДн или иных фактов совершения в отсутствие пользователя попыток несанкционированного доступа (НСД) к защищенной ИСПДн;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн, выхода из строя или неустойчивого функционирования узлов ИСПДн или периферийных устройств (приводов, принтера и т.п.), а также перебоев в системе электроснабжения.

2.4.13 перед началом работы:

- исключить пребывание в помещении посторонних лиц;
- получить в установленном порядке необходимые учтенные документы и/или смешной носитель информации.

2.5 Пользователям ИСПДн категорически ЗАПРЕЩАЕТСЯ:

- разглашать обрабатываемые персональные данные третьим лицам.
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- отключать (блокировать) средства защиты информации;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- копировать и хранить персональные данные на неучтенных носителях информации (жестких дисках, гибких магнитных дисках и т.п.);
- оставлять без присмотра включенную ПЭВМ;
- оставлять без личного присмотра на рабочем месте (других местах) распечатки на бумажных, машинных и других носителях, содержащие персональные данные;
- привлекать посторонних лиц для производства ремонта или настройки ПЭВМ, без согласования с ответственным за обеспечение защиты персональных данных

3. Порядок учета и обращения с машинными носителями информации

3.1 Все машинные носители информации (далее – МН), задействованные в процессе обработки персональных данных, подлежат учету в «Журнале учета машинных носителей информации». На отчуждаемых МН указывается инвентарный номер и гриф «Для служебного пользования».

3.2 При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на ПЭВМ. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование.

3.3 При подозрении на неисправность МН пользователь ставит в известность об этом АИБ. Если неисправность подтверждается и исправить ее невозможно, МН подлежит уничтожению в установленном порядке.

4. Порядок работы пользователя с ресурсами ИСПДн

5.1 Начало работы на ПЭВМ

Необходимо включить ПЭВМ и дождаться завершения загрузки и готовности системы защиты информации (СЗИ) и операционной системы (ОС) к идентификации пользователя. Для получения доступа к ресурсам ИСПДн пользователь должен ввести логин и пароль. Если после ввода пароля система выдаст сообщение об ошибке идентификации пользователя, пользователь должен обратиться к ответственному лицу.

5.2 Завершение работы на ПЭВМ

По мере окончания работ пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения ПЭВМ), либо завершить работу ПЭВМ стандартным способом.

5.3 Общие требования к обработке информации на ПЭВМ

При обработке на ПЭВМ персональных данных используется необходимый и достаточный набор программных средств. Перечень программного обеспечения, устанавливаемого на ПЭВМ, утверждается в установленном порядке. Пользователям запрещается устанавливать или удалять какие-либо программные средства в том числе и ПО собственной разработки. Кроме того, пользователям запрещается запускать любые режимы работы и программы (служебные программы СЗИ, ОС и ПО собственной работы), выходящие за рамки установленной для них технологии обработки информации.

Каждый пользователь может работать только с теми ресурсами ИСПДн, к которым ему предоставлен доступ ответственным лицом. В случае невозможности доступа к каким-либо ресурсам ИСПДн или недостаточности прав доступа (чтение, запись, удаление) для обработки персональных данных, а также любых других несоответствий между системой доступа и технологическим процессом пользователь должен обратиться к ответственному лицу.

Работа с программным обеспечением, в рамках технологического процесса осуществляется в соответствии с инструкцией на это ПО.

При выходе из помещения АРМ пользователь обязан завершить сеанс своей работы либо заблокировать АРМ.

Пользователям запрещается изменять местоположение составных частей ПЭВМ, а также подключать к ПЭВМ какие-либо аппаратные средства.

5.4 Вывод документов на печать

Бракованные бумажные носители и черновики документов должны быть уничтожены.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих права доступа к ресурсам ИСПДн, все документы, содержащие ПДн, должны быть недоступны для просмотра и иного их использования.

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

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

5.2 При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации;
- нецелевое использование подключения к Сети.

6. Ответственность

7.1 Пользователь несет личную ответственность за сохранность носителей информации и содержащейся на них информации (в рабочее время).

7.2 Пользователь, участвующий в рамках своих функциональных обязанностей в процессе автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным (ИСПДн), несет персональную ответственность за свои действия.

7.3 Нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность.