|  |
| --- |
| Приложение № 1 |
| УТВЕРЖДЕНО  приказом ГКУСО «Центр социального обслуживания Пустошкинского района»  от 29.12.2018 № 116 |

ИНСТРУКЦИЯ

пользователя информационной системы персональных данных

ГКУСО «Центр социального обслуживания Пустошкинского района»

I. Общие положения

1.1. Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных ГКУСО «Центр социального обслуживания Пустошкинского района» (далее — Центр).

1.2. Пользователем является каждый сотрудник Центра, 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 несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Положением о защите и обработке персональных данных в информационных системах ГКУСО «Центр социального обслуживания Пустошкинского района» и регламентирующими документами в области защиты персональных данных Центра.

1.5. Методическое руководство работой Пользователя осуществляется ответственным за обеспечение защиты персональных данных.

II. Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, Положения о защите и обработке персональных данных в информационных системах ГКУСО «Центр социального обслуживания Пустошкинского района», распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры, которые определены для него в Положении о защите и обработке персональных данных в информационных системах Центра.

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 (раздел III).

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

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась 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 Центра, необходимо сообщать ответственному за организацию обработки персональных данных Центра.

2.8. 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;

- несанкционированно открывать общий доступ к папкам на своей рабочей станции;

- подключать к рабочей станции 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 информационным системам персональных данных;

- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к информационным системам персональных данных;

- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

III. Организация парольной защиты

3.1. Личные пароли доступа выдаются централизованно ответственным за организацию обработки персональных данных или создаются самостоятельно.

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

3.3. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

- пароль должен состоять не менее чем из 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы ($, @, #, %, & и другие символы);

- 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.

3.4. 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.).

3.5. 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.

3.6. Лица, использующие пароли, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по парольной защите;

- своевременно сообщать ответственному за организацию обработки персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

IV. 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) должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);

- передавать по Сети защищаемую информацию без использования средств шифрования;

- запрещается скачивать из Сети программное обеспечение и другие файлы;

- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие);

- запрещается нецелевое использование подключения к Сети.

|  |
| --- |
| Приложение № 2 |
| УТВЕРЖДЕНО  приказом ГКУСО «Центр социального обслуживания Пустошкинского района»  от 29.12.2018 № 116 |

ИНСТРУКЦИЯ

по антивирусной защите пользователя

информационной системы персональных данных

ГКУСО «Центр социального обслуживания Пустошкинского района»

I. Общие требования

1.1. Настоящая инструкция определяет требования к организации защиты информационной системы персональных данных от разрушающего воздействия компьютерных вирусов. Инструкция распространяется на все существующие информационные системы персональных данных в ГКУСО «Центр социального обслуживания Пустошкинского района».

1.2. К использованию в информационной системе допускаются только лицензионные антивирусные средства.

1.3. Установка и настройка средств антивирусного контроля в информационной системы персональных данных обеспечивается администратором информационной безопасности или специально назначенным лицом в соответствии с руководствами по применению конкретных антивирусных средств.

1.4. Ярлык для запуска антивирусной программы должен быть вынесен (там, где это возможно) на окно "Рабочий стол" операционной системы.

1.5. На объекте вычислительной техники запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

II. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов рабочих станций.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.3. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), администратором информационной безопасности должна быть выполнена антивирусная проверка на защищаемых серверах и рабочих станциях.

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.) сотрудник самостоятельно или вместе с администратором информационной безопасности должен организовать проведение внеочередного антивирусного контроля своей рабочей станции.

2.6. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

* приостановить работу в информационной системы персональных данных;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения;
* по указанию руководителя подразделения организовать проведение лечения или уничтожения зараженных файлов.

При обнаружении нового вируса, не поддающегося лечению, пользователь обязан прекратить какие-либо действия на объекте вычислительной техники и немедленно принять меры по обеспечению обновления антивирусных пакетов.

III. Ответственность

3.1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.