МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«СТАНЦИЯ ЮНЫХ ТЕХНИКОВ»

УТВЕРЖДАЮ:
Директор МБУДО «СЮТ»
_____Д.А. Егорова
Приказ № ___ от _____

ИНСТРУКЦИЯ

пользователя информационных систем персональных данных

муниципального бюджетного учреждения
дополнительного образования
«Станция юных техников»

г. Приморско-Ахтарск

1.Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее - Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

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

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 учреждении 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 МБУДО «СЮТ» и иных нормативных актов муниципального учреждения, 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 ответственному за обеспечение безопасности ПДн 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.

2.2. 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, 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.

3.3. 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. Копирование Пдн на электронные носители информации осуществляется только при наличии производственной необходимости и только на учтенные электронные носители информации.

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

5.4. 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. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих ПДн, уничтожаются незамедлительно после подписания (утверждения) окончательного варианта документа.

5.5. 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.

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

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

6.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

6.2. 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 с потенциально опасным содержимым (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

7. Права и ответственность пользователей ИСПДн

7.2. Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.