Муниципальное бюджетное учреждение дополнительного образования
«Центр детского и юношеского творчества»
муниципального образования городской округ Симферополь
Республики Крым

УТВЕРЖДАЮ
Директор МБ УДО «ЦДЮТ»
г. Симферополя
_____ Т.С. Ельцова
Приказ № 10 от 10.01.2022 г.

ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ И/ИЛИ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ В МБ УДО «ЦДЮТ»

1. Общие положения

1.1. Положение «Об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации в МБ УДО «ЦДЮТ» (далее - Положение) разработано на основании положений ст. 24 Конституции Российской Федерации, гл. 14 Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», от 30.12.2022г. «О внесении изменений в Федеральный Закон «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн) и локальными актами Центра.

1.2. Положение определяет порядок работы лиц ответственных за обработку ПДн.

1.3. Положение обязательно для исполнения всеми работниками МБ УДО «ЦДЮТ», непосредственно осуществляющими защиту ПДн, обрабатываемых в ИСПДн.

2. Цели и задачи обеспечения безопасности персональных данных

2.1.Основной целью обеспечения безопасности ПДн, при их обработке в ИСПДн, является защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

2.2.Задачей, которую необходимо решить для достижения поставленной цели, является обеспечение безопасности ПДн при их обработке в ИСПДн с помощью СЗПДн.

2.3.СЗПДн включает в себя организационные, физические и технические меры, используемых в ИСПДн.

3. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации.

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

3.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа, который издается директором список лиц, ответственных за обработку, хранение персональных данных работников и обучающихся, с целью контроля выполнения необходимых мероприятий по обеспечению безопасности назначается ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн.

3.2. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

3.3. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

3.4. Запись информации, содержащей ПДн, может, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей персональных данных.

3.5. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

3.6. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ в помещение, в котором производится обработка ПДн, аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн.

Немедленно известить ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн в случае утери индивидуального устройства идентификации или при подозрении компрометации паролей.

3.7. Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения персонального компьютера в неслужебных целях;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения).

3.8. Экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами.

4. Порядок обработки персональных данных без использования средств автоматизации.

4.1. Обработка персональных данных без использования средств автоматизации может осуществляться в виде документов на бумажных носителях.

4.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

4.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

4.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

4.4.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

4.4.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

4.4.3. типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

4.4.4. типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с

сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

5. Резервирование и восстановление работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации

4.1 В случае необходимости, восстановление данных из резервных копий производится ответственными работниками.

4.2 Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

4.3 Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

4.4 Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

4.5 Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

4.6 При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

6. Правила антивирусной защиты

6.1. В МБ УДО «ЦДЮТ» к применению допускаются антивирусные программные и (или) программно-аппаратные средства (антивирусные средства).

6.2.Антивирусные средства должны функционировать в течение всего времени работы средств вычислительной техники (от момента загрузки операционной системы до момента ее выгрузки).

6.3.Антивирусное средство не должно существенно затруднять работоспособность средств вычислительной техники информационных систем персональных данных.

6.4.Антивирусной защите подлежит вся, обрабатываемая в МБ УДО «ЦДЮТ» при помощи средств вычислительной техники, информация, независимо от ограничений доступа к ней.

6.5.Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

6.6.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.) пользователь самостоятельно должен провести внеочередной контроль компьютера.

7. Правила парольной защиты

7.1. Авторизация пользователей ИСПДн осуществляется путем ввода идентификатора и/или пароля.

7.2.Требования к формированию паролей и обращению с ними.

7.2.1. Пароль формируется при создании учетной записи ответственным обеспечение безопасности ПДн, при первичном входе в учетную запись пароль должен быть изменен владельцем.

7.2.2. Владельцы личных паролей обязаны обеспечить их тайну.

7.2.3. Пароли генерируются с учетом следующих требований:

- пароль должен знать только его владелец;
- длина пароля должна быть не менее 6 символов;
- в пароле обязательно должны присутствовать как цифры, так и буквы на верхнем и нижнем регистрах;
- пароль не должен включать смысловую нагрузку (имена, фамилии, наименования организаций, улиц, городов и т.д.), общепринятые сокращения (userOl, password02 и т.п.) и последовательные сочетания клавиш клавиатуры (qwertyOl, Ицукен12);
- максимальный срок действия пароля составляет 120 дней;
- минимальный срок действия пароля составляет 2 дня;
- количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 6.

7.3. Требования к формированию паролей обеспечиваются техническими возможностями используемых операционных систем, средств защиты информации и информационных ресурсов.

7.4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода. Внеплановая смена пароля производится в случае его компрометации, а также по просьбе пользователя ИСПДн.

7.5. Хранение пользователями ИСПДн значений своих паролей на бумажном носителе ЗАПРЕЩЕНО.

7.6. Пользователь не имеет права сообщить личный пароль другим лицам (разрешается только с согласования ответственного за обеспечение безопасности при наличии технологической необходимости использования имен и паролей работников в их отсутствие в случае возникновения нештатбных ситуаций, форс-мажорных обстоятельств и т.п.. По возращению работники обязаны сразу же сменить свои пароли на новые значения согласно данного Положения.

7.7. Порядок смены паролей и идентификаторов при изменениях в организационно-штатной структуре (кадровые перестановки, увольнение работников):

7.7.1. При прекращении действия трудового договора с работником все созданные для этого работника учетные записи (пользовательское имя) подлежат блокированию не позднее, чем в день увольнения работника. Полное удаление учетных записей производится в течении 5 рабочих дней со дня увольнения работника.

7.8. При выявлении факта утраты пароля, разглашения пароля, пароля идентификатора, самого идентификатора пользователь обязан незамедлительно сообщить о данных фактах своему непосредственному руководителю и ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн.

8. Управление учетными записями пользователей

8.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должна быть создана уникальная учетная запись пользователя.

8.2. Работу в ИСПДн сотрудник должен осуществлять только с использованием своего уникального имени пользователя.

9. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации.

9.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

9.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

9.3. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

9.4. По факту уничтожения или стирания носителей составляется акт уничтожения персональных данных.

9.5. Процедуры стирания и уничтожения осуществляются комиссией по уничтожению персональных данных.

10. Обезличивание персональных данных

10.1. Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных

10.2. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

10.3. Способы обезличивания при условии дальнейшей обработки персональных данных:

- метод введения идентификаторов;
- метод изменения состава или семантики;
- обобщение (понижение точности некоторых сведений);
- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;
- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

10.4. Для обезличивания персональных данных используются способы обезличивания, определенные приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» в соответствии с рекомендациями по использованию этих методов.

10.5. Решение о необходимости обезличивания персональных данных принимает директор МБ УДО «ЦДЮТ».

10.6. Сотрудники непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

10.7. Порядок работы с обезличенными персональными данными:

10.7.1. Обезличенные персональные данные не подлежат разглашению.

10.7.2. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

10.7.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется).

10.8. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещениях, где они хранятся.