Приложение 3
к приказу МБУДО
«Красноармейская ДШИ»
от 18.07.2017 № 28-о.д.

Инструкция
по физической охране и контролю доступа в помещения

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция регламентирует условия и порядок осуществления доступа лиц в помещения со средствами информационных систем персональных данных (далее - ИСПДн) в целях обеспечения предотвращения несанкционированного доступа к сведениям, содержащим персональные данные в Муниципальном бюджетном учреждении дополнительного образования «Красноармейская детская школа искусств» (далее – Учреждение). При обеспечении доступа лиц соблюдаются требования законодательства РФ по защите персональных данных.

1.2. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности Учреждения и определяет порядок пропуска в помещения работников Учреждения и посетителей.

1.3. В помещениях исключено неконтролируемое пребывание посторонних лиц.

1.4. Контроль за порядком обеспечения доступа лиц в помещения возлагается на Руководителя Учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.2. Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

2.3. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.4. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.5. Доступ к информации – возможность получения информации и ее использования.

2.6. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения,

фальсификации) своих прав доступа.

2.7. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

3. ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ РАБОТНИКОВ И ПОСЕТИТЕЛЕЙ

3.1. Не допускается нахождение работников Учреждения в помещениях в нерабочее для них время.

3.2. Нахождение посетителей Учреждения в помещениях допускается только в рабочее время.

3.3. В помещения ИСПДн пропускаются:

3.3.1. беспрепятственно – Руководитель Учреждения и работники, имеющие допуск к работе с персональными данными и с целью выполнения трудовых обязанностей;

3.3.2. при наличии удостоверения, с разрешения Руководителя Учреждения, в сопровождении ответственного за обеспечение безопасности персональных данных или администратора безопасности - сотрудники контролирующих органов, сотрудники пожарных и аварийных служб, сотрудники полиции;

3.3.3. ограниченно - работники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, работники сторонних организаций и учреждений для выполнения договорных отношений.

3.4. Посетители пропускаются в помещения ИСПДн Учреждения в рабочее время в сопровождении работников, допущенных к обработке персональных данных.

3.5. В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных трудовыми обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

4. ОРГАНИЗАЦИЯ И ПОРЯДОК ПРОИЗВОДСТВА РЕМОНТНО-СТРОИТЕЛЬНЫХ РАБОТ В ЗДАНИИ

4.1. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещения для проведения ремонтно-строительных работ на основании заявок, подписанных Руководителем Учреждения.

4.2. В целях предотвращения несанкционированного доступа к сведениям, содержащим персональные данные, работы проводятся только под контролем ответственного за обеспечение безопасности персональных данных или администратора безопасности.

5. ОРГАНИЗАЦИЯ ОХРАНЫ И ДОСТУПА В ПОМЕЩЕНИЯ

5.1. Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных работников запираются на ключ. Помещения должны быть оборудованы специальными инженерными средствами, такими как усиленные

двери, охранная сигнализация и т.п.

5.2. Работники по окончании рабочего дня обязаны убрать все документы в столы, шкафы и сейфы, закрыть окна и форточки, отключить от сети аппаратуру, радиоточки, электроприборы и освещение.

5.3. Оборудование в помещениях должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц. Мониторы компьютеров должны быть ориентированы таким образом, чтобы исключить возможность просмотра отображаемой на них информации лицами, не имеющими допуска к обработке персональных данных.

5.4. Окна помещений, в которых ведется обработка персональных данных, должны быть оборудованы шторами или жалюзи.

5.5. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

6. УБОРКА ПОМЕЩЕНИЙ

6.1. Уборка помещений ИСПДн должна производиться под контролем работника, допущенного к обработке персональных данных в этом помещении.

6.2. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все АРМ, на которых обрабатываются персональные данные. Носители, содержащие персональные данные, должны быть убраны в закрытые шкафы или сейфы.

7. ТРЕБОВАНИЯ ПО ТЕХНИЧЕСКОМУ УКРЕПЛЕНИЮ

7.1. Руководитель Учреждения обеспечивает обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и должен руководствоваться следующими основными требованиями:

7.1.1. двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;

7.1.2. оконные проемы первых этажей зданий должны быть укреплены металлическими решетками, запираемыми с внутренней стороны, если это не противоречит требованиям пожарной безопасности.

7.2. Конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол.

7.3. Стекла в рамах должны быть надежно закреплены в пазах.

Рамы указанных оконных проемов оборудуются запорными устройствами

Приложение 4
к приказу МБУДО
«Красноармейская ДШИ»
18.07.2017 № 28-о.д.

Инструкция
обслуживающего персонала информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с нормативными документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ обслуживающим персоналом в информационных системах персональных данных (далее – ИСПДн) Муниципального бюджетного учреждения дополнительного образования

1.2. Субъектами доступа к ресурсам ИСПДн являются пользователи, администратор безопасности и обслуживающий персонал (работники, осуществляющие техническое обслуживание, ремонт) в соответствии с утвержденным перечнем.

1.3. Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

1.4. Машинные носители с защищаемой информацией имеют пометку «ПДн».

1.5. Работники, осуществляющие ремонт и обслуживание компонентов ИСПДн (обслуживающий персонал) получают доступ к ресурсам ИСПДн по согласованию с администратором безопасности (далее – АБ).

1.6. Обслуживающий персонал осуществляет плановые и внеплановые мероприятия по обеспечению работоспособности основных и вспомогательных технических средств, и систем (далее – ОТСС и ВТСС), входящих в состав ИСПДн.

1.7. Методическое руководство по информационной безопасности объектов вычислительной техники (далее – ОВТ) осуществляет АБ.

1.8. Обслуживающий персонал имеет право вносить предложения по изменению и дополнению данной Инструкции.

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

1.10. Право толкования положений настоящей Инструкции возлагается на Руководителя Учреждения.

2. ТРЕБОВАНИЯ К ОБСЛУЖИВАЮЩЕМУ ПЕРСОНАЛУ

2.1. Обслуживающий персонал, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе в ИСПДн не допускается.

2.2. Обслуживающий персонал обязан выполнять требования АБ.

2.3. Обслуживающий персонал обязан периодически (согласно

утвержденному плану) производить проверку работоспособности технических средств.

2.4. Обслуживающий персонал обязан немедленно реагировать на сообщения АБ о любых неисправностях в работе ИСПДн.

2.5. Обслуживающий персонал обязан отчитаться АБ по факту выполнения работ в ИСПДн.

3. ДОСТУП К РЕСУРСАМ ИСПДН

3.1. Обязательным условием получения доступа к ресурсам ИСПДн обслуживающего персонала является знание технологии обработки информации в ИСПДн с учетом требований информационной безопасности.

3.2. Все работы выполняются в присутствии работника, имеющего право доступа к ресурсам ИСПДн.

3.3. Обслуживающий персонал не имеет права требовать у пользователей раскрытия их паролей и/или передачи персональных идентификаторов.

3.4. Обслуживающий персонал не имеет право требовать у пользователей распечатывать и/или выводить информацию на экран монитора.

3.5. Обслуживающий персонал не имеет права требовать у пользователей предоставления любых машинных носителей (далее – МН) информации, в т. ч. во временное использование.

4. ПОРЯДОК РАБОТЫ ОБСЛУЖИВАЮЩЕГО ПЕРСОНАЛА

Ниже приводится перечень работ, производимых обслуживающим персоналом с ресурсами ИСПДн.

4.1. Обеспечение работоспособности ИСПДн

В соответствии с утвержденным графиком, а также по требованию АБ обслуживающий персонал проводит проверку работоспособности технических средств, используемых на ОВТ. В случае обнаружения неисправностей необходимо произвести следующие действия:

- для устранения неисправности технических средств, требующего нарушения целостности защитной наклейки, необходимо поставить в известность АБ, а в случае его отсутствия – ответственного за обеспечение безопасности персональных данных Учреждения;
- для замены комплектующих, учтенных в «Техническом паспорте…» (за исключением съемного жесткого диска), необходимо изъять ПЭВМ с рабочего места пользователя (при этом жесткий диск сдается АБ по месту хранения отчуждаемых МН) и произвести его ремонт в установленном в организации порядке;
- при устранении неисправности съемного жесткого диска, все работы производятся в присутствии АБ;
- для замены комплектующих, не учтенных в «Техническом паспорте…» (оперативная память, кабели и др.), допускается проведение ремонтных работ на рабочем месте пользователя (в присутствии АБ или ответственного за обеспечение безопасности персональных данных Учреждения).

4.2. Обеспечение работоспособности ВТСС и прочие работы

В соответствии с утвержденным графиком, а также по требованию АБ обслуживающий персонал проводит проверку работоспособности ВТСС (датчики сигнализации, соответствующие кабели и др.) и прочие работы в помещении

(ремонт системы электропитания, освещения и пр.). При этом необходимо выполнять следующие требования:

- график проведения работ согласовывается с ответственным за обеспечение безопасности персональных данных Учреждения;
- вне графика производится обязательная проверка в случае обнаружения неисправностей в работе ВТСС;
- при установлении неисправности ВТСС необходимо поставить в известность АБ или ответственного за обеспечение безопасности персональных данных Учреждения;
- при демонтаже неисправных ВТСС присутствие АБ является обязательным;
- если для устранения неисправности демонтаж ВТСС не требуется, присутствие АБ или ответственного за обеспечение безопасности персональных данных Учреждения при проведении работ также является обязательным;
- аналогично производятся прочие работы в помещениях.

5. ОТВЕТСТВЕННОСТЬ

Обслуживающий персонал несет персональную ответственность за:

- неразглашение сведений, ставших им известными при выполнении своих обязанностей;
- сохранность ресурсов ИСПДн, изъятых для ремонта;
- качество выполняемых работ;

соблюдение требований данной Инструкции и правомерное использование ресурсов ИСПДн.

Приложение 5
к приказу МБУДО
«Красноармейская ДШИ»
18.07.2017 № 28-о.д.

Инструкция
по работе ответственного лица за организацию обработки персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности, права и ответственность ответственного лица за организацию обработки персональных данных Муниципального бюджетного учреждения дополнительного образования «Красноармейская детская школа искусств» (далее – Учреждение).

1.2. Ответственное лицо за организацию обработки персональных данных является штатным работником Учреждения и назначается Приказом Руководителя Учреждения.

1.3. Ответственное лицо за организацию обработки персональных данных (далее - Ответственный) - лицо, отвечающее за организацию обработки персональных данных с использованием средств автоматизации и без использования таких средств.

1.4. Решение вопросов организации защиты персональных данных в Учреждении входит в прямые трудовые обязанности Ответственного.

1.5. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

1.6. Ответственный в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства, руководящими и нормативными документами ФСТЭК России, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами Учреждения.

1.7. Требования Ответственного, связанные с выполнением им своих трудовых обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к персональным данным.

1.8. Ответственный обладает правами доступа к любым носителям персональных данных Учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Блокирование персональных данных - временное прекращение обработки персональных данных.

2.2. Доступ к информации – возможность получения информации и ее использования.

2.3. Защита информации — деятельность по предотвращению утечки

информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.4. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.5. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.6. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.7. Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

2.8. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.9. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.10. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.11. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

3.1. В области автоматизированной обработки персональных данных Ответственный обязан:

3.1.1. взаимодействовать с администратором безопасности и ответственным за обеспечение безопасности персональных данных по вопросам обеспечения и выполнения требований обработки персональных данных;

3.1.2. контролировать осуществление мероприятий по установке и настройке средств защиты;

3.1.3. осуществлять контроль за порядком учета, создания, хранения и использования резервных копий и машинных носителей, содержащих персональные данные.

3.2. В области обработки персональных данных без использования средств автоматизации Ответственный обязан:

3.2.1. контролировать порядок обработки бумажных носителей персональных данных;

3.2.2. осуществлять проверки наличия документов, содержащих персональные данные.

3.3. В области информирования работников Ответственный обязан:

3.3.1. доводить до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3.3.2. осуществлять методическое руководство работников, имеющих санкционированный доступ к персональным данным, в вопросах обеспечения безопасности персональных данных;

3.3.3. организовывать повышение квалификации работников в области защиты персональных данных.

3.4. В области работы с субъектами персональных данных Ответственный обязан:

3.4.1. разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных;

3.4.2. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

3.5. В области контроля работников Ответственный обязан:

3.5.1. планировать мероприятия по организации обеспечения безопасности персональных данных;

3.5.2. организовывать и осуществлять периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами;

3.5.3. организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

3.6. В области учета лиц, имеющих доступ к персональным данным, Ответственный обязан:

3.6.1. знать и предоставлять на утверждение Руководителю Учреждения изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих трудовых обязанностей;

3.6.2. участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

3.7. Иные обязанности Ответственного:

3.7.1. по указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по правилам обработки персональных данных;

3.7.2. знать перечень и условия обработки персональных данных в Учреждении;

3.7.3. осуществлять организацию учёта документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения;

3.7.4. выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

4. ПРАВА ОТВЕТСТВЕННОГО

Ответственный имеет право:

4.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам организации обработки и обеспечения безопасности персональных данных.

4.2. Требовать от всех пользователей ИСПДн выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

4.3. Инициировать блокирование доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

4.4. Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

4.5. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

4.6. Обращаться к руководителю подразделения с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

4.7. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

5. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

5.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа Ответственный обязан:

5.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

5.2.2. доложить Руководителю Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и

предпринятых действиях;

5.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

5.2.4. известить ответственного за обеспечение безопасности персональных данных и администратора безопасности о факте несанкционированного доступа.

6. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный несет персональную ответственность за:

6.1.1. соблюдение требований настоящей Инструкции,

6.1.2. правильность и объективность принимаемых решений,

6.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных,

6.1.4. за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.