



УТВЕРЖДАЮ
Директор МБУДО «ДШИ №3»

Л.П.Мова

«27» февраля 2017 г. Приказ № 43-а-д

Инструкция по работе ответственного лица за обеспечение безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности, права и ответственность лица, ответственного за обеспечение безопасности персональных данных, обрабатываемых в ИСПДн Муниципального бюджетного учреждения дополнительного образования «Детская школа искусств №3» города Челябинска (далее – Учреждение).

1.2. Лицо, ответственное за обеспечение безопасности персональных данных, является штатным работником Учреждения и назначается Приказом Директора Учреждения.

1.3. Лицо, ответственное за обеспечение безопасности персональных данных (далее - Ответственный), отвечает за организацию и состояние процесса обработки персональных данных в информационных системах персональных данных.

1.4. Решение вопросов организации защиты персональных данных, обрабатываемых в информационных системах персональных данных Учреждения, 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 нормативными 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. **Персональные данные (ПДн)** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

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

2.7. **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.

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

2.9. 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.

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

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

Ответственный обязан:

3.1. Обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации ИСПДн, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью.

3.2. Знать и предоставлять ответственному за организацию обработки ПДн изменения к списку лиц, доступ которых к ПДн необходим для выполнения трудовых обязанностей.

3.3. Проводить инструктаж и консультации пользователей ПЭВМ по соблюдению режима конфиденциальности.

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

3.5. Организовывать 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.

3.6. Взаимодействовать с администратором безопасности ИСПДн по вопросам обеспечения и выполнения требований обработки персональных данных.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

3.8. Организовывать работы по плановому контролю работоспособности технических средств защиты ПДн, охраны объекта, средств защиты информации от НСД.

3.9. Контролировать периодическое резервное копирование баз ПДн и сопутствующей защищаемой информации.

3.10. По указанию Директора Учреждения своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и по правилам обработки ПДн.

3.11. Знать перечень и условия обработки ПДн в Учреждении.

3.12. Знать перечень установленных технических средств, входящих в состав ИСПДн, и перечень задач, решаемых с их использованием.

3.13. Обеспечивать соблюдение работниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава ИСПДн.

3.14. Осуществлять контроль за порядком учета, создания, хранения и использования машинных носителей, содержащих ПДн.

3.15. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к ПДн и техническим средствам из состава ИСПДн, сообщать о них Директору Учреждения.

3.16. Инструктировать работников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами защиты информации.

3.17. Знать законодательство Российской Федерации о ПДн, следить за его изменениями.

3.18. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с документами, содержащими

ПДн, или по другим нарушениям, которые могут привести к снижению уровня защищенности ПДн.

3.19. Выполнять иные мероприятия, требуемые нормативными документами по защите ПДн.

4. ПРАВА ОТВЕТСТВЕННОГО

Ответственный имеет право:

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

4.2. Инициировать блокирование доступа работников к ПДн, если это необходимо для предотвращения нарушения режима защиты ПДн.

4.3. Участвовать в разработке мероприятий по совершенствованию системы защиты ПДн.

4.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей ПДн, нарушения правил работы с документами, содержащими ПДн, НСД, утраты, порчи защищаемых носителей ПДн и технических средств из состава ИСПДн или по другим нарушениям, которые могут привести к снижению уровня защищенности ПДн.

4.5. Обращаться к Директору Учреждения с предложением о приостановке процесса обработки ПДн или отстранению от работы пользователя в случаях нарушения установленной технологии обработки ПДн данных или нарушения режима конфиденциальности.

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

5. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НСД

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы с ПДн 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 безопасности ИСПДн 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 ПДн;

5.2.2. доложить Директору Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить ответственного за организацию обработки ПДн и администратора безопасности ИСПДн о факте НСД.

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 ПДн.

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 ПДн субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.