





**Автономная некоммерческая организация  
дополнительного профессионального образования  
«Учебно-курсовой комбинат»**



УТВЕРЖДАЮ

Директор

АНО ДПО «Учебно-курсовой комбинат»

Н.М. Плотникова

20 мая 2019 г.

**ИНСТРУКЦИЯ  
ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ  
ДАННЫХ В АНО ДПО «Учебно-курсовой комбинат»**

20 мая 2019 г.

г. Коркино

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

**1.1.** Данная Инструкция определяет основные обязанности и права ответственного за организацию обработки персональных данных в Автономной некоммерческой организации дополнительного профессионального образования «Учебно-курсовой комбинат» (далее – Организация).

**1.2.** Ответственный за организацию обработки персональных данных является штатным сотрудником Организации и назначается приказом директора.

**1.3.** Решение вопросов организации защиты персональных данных в Организации входит в прямые служебные обязанности ответственного за организацию обработки персональных данных.

**1.4.** Ответственный за организацию обработки персональных данных обладает правами доступа к любым носителям персональных данных Организации.

**2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

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

**2.2. Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

**2.3. Доступ к информации** – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

**2.4. Защита информации** – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на



информацию, то есть процесс, направленный на достижение информационной безопасности.

**2.5. Информация** – сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

**2.6. Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

**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 путём 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 (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

**2.10. Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

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

**2.12. Угрозы безопасности персональных данных (УБПДн)** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (ст. 19 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

**2.13. 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 (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

### 3. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Ответственный за организацию обработки персональных данных обязан:

**3.1.** Знать перечень и условия обработки персональных данных в Организации.

**3.2.** Знать и утверждать изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих трудовых обязанностей.

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

**3.4.** Осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения.

**3.5.** Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

**3.6.** Реагировать на попытки несанкционированного доступа к информации в установленном гл. 4 настоящей Инструкции порядке.

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

**3.8.** Контролировать оперативное внесение изменений в конфигурацию технических средств ИСПДн, требовать отражения соответствующих изменений в «Техническом паспорте информационной системы персональных данных».

**3.9.** Своевременно и точно отражать изменения в локальных нормативных правовых актах по управлению средствами защиты информации в ИСПДн и правилам обработки персональных данных.

**3.10.** Проводить занятия и инструктажи с сотрудниками и руководителями структурных подразделений о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных.

**3.11.** Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

**3.12.** Контролировать соблюдение работниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными.

**3.13.** Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

**3.14.** Организовать учёт обращений субъектов персональных данных, контролировать заполнение «**Журнала учета обращений субъектов персональных данных**».

**3.15.** Представлять интересы Организации при проверках надзорных органов в сфере обработки персональных данных.

**3.16.** Знать законодательство РФ о персональных данных, следить за его изменениями.

**3.17.** Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

#### **4. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ**

##### **ПОПЫТОКНЕСАНКЦИОНИРОВАННОГО ДОСТУПА**

**4.1.** К попыткам несанкционированного доступа относятся:

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

- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

**4.2.** При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных обязан:



- прекратить несанкционированный доступ к персональным данным;
- зафиксировать служебной запиской факт несанкционированного доступа, его результат (успешный, неуспешный) и предпринятые действия;
- известить руководителя организации, в которой работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;
- известить администратора безопасности ИСПДн о факте несанкционированного доступа.

## **5. ПРАВА**

**5.1.** Ответственный за организацию обработки персональных данных имеет право:

**5.1.1.** Требовать от работников выполнения локальных нормативных правовых актов в части работы с персональными данными.

**5.1.2.** Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

**5.1.3.** Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

## **6. ОТВЕТСТВЕННОСТЬ**

**6.1.** Ответственный за организацию обработки персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

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

**6.3.** Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативными правовыми актами (приказами, распоряжениями) Организации, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Организации, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Организации (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

**6.4.** В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

**6.5.** В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.