Государственное автономное профессиональное образовательное учреждение Свердловской области «Ирбитский политехникум» (ГАПОУ СО «ИПТ»)

ПРИКАЗ

«14» марта 2018 г. № 202

Ирбит

О назначении ответственных лиц

Во исполнение требований Федерального закона № 149-ФЗ от 27 июля 2006г. «Об информации, информационных технологиях и о защите информации», Федерального закона №152-ФЗ от 27 июля 2006г. «О персональных данных», приказа ФСТЭК России №21 от 18 февраля 2013г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и приказа ФСТЭК России №17 от 11 февраля 2013г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Назначить Ответственным за организацию обработки персональных данных в ГАПОУ СО «ИПТ» специалиста отдела кадров И. Я. Рудакову.
2. Назначить Ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных ГАПОУ СО «ИПТ» электроника А. С. Ильиных.
3. Назначить Администратором информационных систем персональных данных ГАПОУ СО «ИПТ» электроника А. С. Ильиных.
4. На время временного отсутствия (болезнь, отпуск и т.д.) ответственных лиц, указанных в п. 1–3 настоящего Приказа, ответственность за организацию обработки персональных данных, осуществление организационных и технических мероприятий по защите персональных данных и осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону №152-ФЗ от 27 июля 2006 г. и принятыми в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, и иным локальным нормативным актам, возложить на лиц, исполняющих их обязанности, назначенных и допущенных в установленном порядке.
5. Утвердить и ввести в действие Инструкцию ответственного за организацию обработки персональных данных в ГАПОУ СО «ИПТ» (Приложение 1 к настоящему Приказу).
6. Утвердить и ввести в действие Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных ГАПОУ СО «ИПТ» (Приложение 2 к настоящему Приказу).
7. Утвердить и ввести в действие Инструкцию администратора информационных систем персональных данных ГАПОУ СО «ИПТ» (Приложение 3 к настоящему Приказу).

8. Требования настоящего Приказа довести до назначенных ответственных лиц.
9. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор Н. Н. Журавлева

Приложение 1
к приказу ГАПОУ СО «ИПТ»
от «14» ноября 2018 г. № 202

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в ГАПОУ СО «ИПТ»

1. Термины и определения

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция определяет функциональные обязанности, ответственность и права ответственного за организацию обработки персональных данных в ГАПОУ СО «ИПТ» (далее – Ответственный).

2.2. Настоящая Инструкция разработана в соответствии с нормативными правовыми актами Российской Федерации в области защиты персональных данных (далее – ПДн), методическими и руководящими документами уполномоченных федеральных органов исполнительной власти.

2.3. Ответственный назначается приказом Директора ГАПОУ СО «ИПТ» (далее – Учреждение).

2.4. Ответственный непосредственно подчиняется Директору Учреждения.

2.5. На время временного отсутствия (болезнь, отпуск, пр.) Ответственного, его обязанности возлагаются на работника, назначенного и допущенного к обработке ПДн в установленном порядке.

2.6. Ответственный в своей работе руководствуется настоящей Инструкцией.

2.7. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Функциональные обязанности

3.1. Ответственный выполняет следующие функции:

- осуществляет внутренний контроль за соблюдением работниками, обрабатывающих ПДн, законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
- актуализирует «Перечень должностей работников, имеющих доступ к обработке персональных данных в ГАПОУ СО «ИПТ»»;
- актуализирует «Перечень работников, допущенных в помещения, в которых осуществляется обработка персональных данных»;
- проводит первоначальный, плановый и внеплановый инструктаж работников, обрабатывающих ПДн, в целях доведения до данных лиц положений законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн, в том числе правил работы со средствами защиты информации;
- организовывает прием и обработку обращений и запросов субъектов ПДн, чьи ПДн обрабатываются в Учреждении, или их представителей, и осуществляет контроль за приемом и обработкой таких обращений и запросов;
- готовит предложения по совершенствованию (актуализации) локальных нормативных актов (внутренних документов) по вопросам обработки и обеспечения безопасности ПДн, по совершенствованию организационных и технических мер по защите ПДн.

4. Права

4.1. Ответственный имеет право:

- требовать от работников, обрабатывающих ПДн, соблюдения установленной технологии обработки ПДн и выполнения локальных нормативных актов (внутренних документов) по обеспечению безопасности ПДн;
- запрашивать у Директора, иных руководителей Учреждения, работников, участвующих в обработке и обеспечении безопасности ПДн, информацию и (или) документы, необходимые для выполнения своих функциональных обязанностей;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, уничтожения ПДн и технических средств, обрабатывающих ПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
- представлять Директору Учреждения свои предложения по совершенствованию локальных нормативных актов (внутренних документов) по обеспечению безопасности ПДн, совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

5.1. На Ответственного возлагается персональная ответственность за качество выполняемых им функций.

5.2. Ответственный несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации о ПДн предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.3. Ответственный несет ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента её утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.

Приложение 2
к приказу ГАПОУ СО «ИПТ»
от «14» Ноября 2018 г. № 302

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных ГАПОУ СО «ИПТ»

1. Термины и определения

Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие право доступа к информации в соответствии с локальными актами и законодательством Российской Федерации, могут беспрепятственно реализовывать данное право;

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Конфиденциальность информации – свойство безопасности информации, при котором доступ к информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации;

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;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации;

Целостность информации – свойство безопасности информации, при котором изменение информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации.

2. Общие положения

2.1. Настоящая Инструкция определяет функциональные обязанности, ответственность и права ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных ГАПОУ СО «ИПТ» (далее – Ответственный).

2.2. Настоящая Инструкция разработана в соответствии с нормативными правовыми актами Российской Федерации в области защиты персональных данных (далее – ПДн), методическими и руководящими документами уполномоченных федеральных органов исполнительной власти.

2.3. Ответственный назначается приказом Директора ГАПОУ СО «ИПТ» (далее – Учреждение).

2.4. На время временного отсутствия (болезнь, отпуск, пр.) Ответственного его обязанности по осуществлению организационных и технических мероприятий по защите ПДн в информационных системах персональных данных (далее – ИСПДн) ГАПОУ СО «ИПТ», возлагаются на работника, назначенного и допущенного к обработке ПДн в установленном порядке.

2.5. Ответственный в своей работе руководствуется настоящей Инструкцией.

2.6. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Функциональные обязанности

3.1. Ответственный выполняет следующие функции:

3.1.1. Управляет доступом пользователей в ИСПДн;

3.1.2. Управляет полномочиями пользователей в ИСПДн;

3.1.3. Поддерживает установленные правила разграничения доступа в ИСПДн;

3.1.4. Управляет системами защиты информации (далее – СиЗИ) ИСПДн:

- управляет средствами защиты информации (далее – СЗИ)
- управляет параметрами настройки программного обеспечения СЗИ;
- восстанавливает работоспособность СЗИ;
- устанавливает обновления программного обеспечения СЗИ, выпускаемые разработчиками (производителями) СЗИ;
- анализирует события в ИСПДн, связанные с защитой информации (события безопасности);
- информирует пользователей ИСПДн об угрозах безопасности ПДн;
- информирует пользователей ИСПДн о правилах эксплуатации СЗИ;
- обучает пользователей ИСПДн работе со СЗИ;

- управляет доступом к съемным машинным носителям информации, используемым в ИСПДн (определяет должностных лиц, имеющих доступ к съемным машинным носителям информации);
- сопровождает функционирование СиЗИ в ходе эксплуатации ИСПДн, включая корректировку эксплуатационной документации;
- поддерживает конфигурацию СиЗИ (структуру СиЗИ, состав, места установки и параметры настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СиЗИ (поддержание базовой конфигурации СиЗИ);
- определяет лиц, которым разрешены действия по внесению изменений в базовую конфигурацию СиЗИ;
- управляет изменениями конфигурации СиЗИ, в том числе:
  - определяет типы возможных изменений;
  - разрешает или отказывает во внесении изменений;
  - документирует действия по внесению изменений;
  - хранит данные об изменениях.

3.1.5. Поддерживает конфигурацию ИСПДн (структуру ИСПДн, состава, мест установки и параметров программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на ИСПДн;

3.1.6. Анализирует потенциальные воздействия планируемых изменений в базовой конфигурации СиЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

3.1.7. Определяет параметры настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и СиЗИ;

3.1.8. Выявляет инциденты информационной безопасности ПДн (далее – Инциденты), и реагирует на них.

3.1.9. Обнаруживает и идентифицирует Инциденты, в том числе:

- отказы в обслуживании;
- сбои (перезагрузки) в работе средств защиты информации;
- нарушения правил разграничения доступа;
- неправомерные действия по сбору информации;
- иные события, приводящие к возникновению Инцидентов.

3.1.10. Анализирует Инциденты, в том числе определяет источники и причины возникновения Инцидентов, а также оценивает их последствия;

3.1.11. Планирует меры по устранению Инцидентов, в том числе:

- по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев;
- устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению Инцидентов.

3.1.12. Планирует и принимает меры по предотвращению повторного возникновения Инцидентов.

3.1.13. Контролирует обеспечение уровня защищенности ПДн, обрабатываемых в ИСПДн:

- контролирует события безопасности и действия пользователей в ИСПДн;
- контролирует (анализирует) уровень защищенности ПДн;
- контролирует перемещение съемных машинных носителей информации за пределы контролируемой зоны лицами, которым оно необходимо для выполнения своих должностных обязанностей (функции);
- анализирует и оценивает функционирование СиЗИ ИСПДн, включая выявление, анализ и устранение недостатков в функционировании СиЗИ ИСПДн;
- выполняет периодический анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности ПДн;
- документирует процедуры и результаты контроля (мониторинга) за обеспечением уровня защищенности ПДн, обрабатываемых в ИСПДн;
- принимает решения по результатам контроля (мониторинга) за обеспечением уровня защищенности ПДн о доработке (модернизации) СиЗИ ИСПДн.

3.1.14. Ведет учет:

- используемых СЗИ в ИСПДн;
- используемых шифровальных (криптографических) СЗИ в ИСПДн, эксплуатационной и технической документации к ним;
- съемных машинных носителей (при их наличии).

3.1.15. Обеспечивает защиту ПДн при выводе из эксплуатации ИСПДн или после принятия решения об окончании обработки ПДн:

- обеспечивает архивирование ПДн, содержащихся в ИСПДн (архивирование должно осуществляться при необходимости дальнейшего использования ПДн);
- обеспечивает уничтожение (стирание) ПДн и остаточной информации с машинных носителей информации, при необходимости передачи машинного носителя информации в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения;
- при выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка ПДн, осуществляет физическое уничтожение этих съемных машинных носителей информации.

4. Права

4.1. Ответственный имеет право:

- требовать от работников – пользователей ИСПДн соблюдения установленной технологии обработки ПДн и выполнения требований локальных нормативных

актов и иной организационно-распорядительной документации по обеспечению безопасности ПДн;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты ПДн, несанкционированного доступа к ПДн, утраты, порчи ПДн и технических средств, входящих в состав ИСПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования СиЗИ;
- участвовать в анализе ситуаций, касающихся функционирования СЗИ и расследования фактов несанкционированного доступа к ПДн;
- представлять Директору Учреждения свои предложения по совершенствованию локальных нормативных актов (внутренних документов) по обеспечению безопасности ПДн, организационных и технических мер по защите ПДн.

5. Ответственность

5.1. Ответственный обязан:

- знать и выполнять требования законодательства Российской Федерации в сфере обеспечения безопасности ПДн;
- знать и выполнять требования настоящей Инструкции, а также действующих локальных нормативных актов (внутренних документов), регламентирующих порядок действий по защите информации;
- выполнять на автоматизированном рабочем месте только те процедуры, которые требуются для выполнения его должностных обязанностей;
- покидая свое рабочее место, в том числе на кратковременный срок, блокировать доступ к операционной среде автоматизированного рабочего места.

5.2. Ответственному категорически запрещается:

- разглашать сведения конфиденциального характера, ставшие известными ему при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией;
- использовать неучтенные внешние машинные носители информации;
- подключать к автоматизированному рабочему месту мобильные устройства;
- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных (личных) целях;
- оставлять автоматизированное рабочее место без присмотра, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках СЗИ, которые могут привести к инцидентам информационной безопасности.

5.3. На Ответственного возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты ПДн;

5.4. Ответственный несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах.

определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации о ПДн предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность;

5.5. Ответственный несет ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.

Приложение 3
к приказу ГАПОУ СО «ИПТ»
от «17» ноября 2018 г. № 202

Инструкция
администратора информационных систем персональных данных ГАПОУ СО «ИПТ»

1. Термины и определения

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

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;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция определяет функциональные обязанности, ответственность и права администратора информационных систем персональных данных ГАПОУ СО «ИПТ» (далее по тексту – Администратор).

2.2. Настоящая Инструкция разработана в соответствии с нормативными правовыми актами Российской Федерации в области защиты персональных данных (далее – ПДн), методическими и руководящими документами уполномоченных федеральных органов исполнительной власти.

2.3. Администратор назначается приказом Директора ГАПОУ СО «ИПТ» (далее – Учреждение).

2.4. На время временного отсутствия (болезнь, отпуск, пр.) Администратора, его

обязанности возлагаются на работника, назначенного и допущенного к обработке ПДн в установленном порядке.

2.5. Администратор в своей работе руководствуется настоящей Инструкцией.

2.6. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Функциональные обязанности

3.1. Администратор выполняет следующие функции:

3.1.1. Управляет параметрами ИСПДн:

- управляет заведением и удалением учетных записей пользователей ИСПДн;
- управляет полномочиями пользователей ИСПДн;
- поддерживает правила разграничения доступа в ИСПДн;
- управляет параметрами настройки программного обеспечения;
- управляет учетными записями пользователей программных средств обработки ПДн;
- оказывает помощь пользователям ИСПДн в смене и восстановлению паролей;
- управляет установкой обновлений программного обеспечения;
- регистрирует события в ИСПДн, связанные с защитой ПДн (события безопасности);
- поддерживает конфигурацию ИСПДн (структуру ИСПДн, состава, мест установки и параметров программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на ИСПДн;
- восстанавливает работоспособность программного обеспечения и технических средств ИСПДн.

3.1.2. Администратор выявляет инциденты информационной безопасности в ИСПДн, и реагирует на них:

- обнаруживает и идентифицирует инциденты, в том числе:
  - отказы в обслуживании;
  - сбои (перезагрузки) в работе средств защиты информации;
  - нарушения правил разграничения доступа;
  - неправомерные действия по сбору информации;
  - иные события, приводящие к возникновению инцидентов.
- своевременно информирует ответственного за обеспечение безопасности ПДн в ИСПДн, о возникновении инцидентов информационной безопасности в ИСПДн;
- анализирует инциденты, в том числе определяет источники и причины возникновения инцидентов, а также оценивает их последствия;
- совместно с ответственным обеспечение безопасности ПДн в ИСПДн принимает меры по устранению инцидентов, в том числе:

- по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев;
- по устранению последствий нарушения правил разграничения доступа, несанкционированного доступа к защищаемой информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов информационной безопасности.

3.1.3. Администратор ведет учет пользователей ИСПДн;

3.1.4. Принимает участие в подготовке, пересмотре, уточнении локальных нормативных актов (внутренних документов) по обеспечению безопасности ПДн, организационных и технических мер по защите ПДн.

4. Права

4.1. Администратор имеет право:

- требовать от пользователей ИСПДн соблюдения установленной технологии обработки ПДн и выполнения требований локальных нормативных актов и иной организационно-распорядительной документации по обеспечению безопасности ПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты от несанкционированного доступа, утраты, порчи защищаемой информации и технических средств, входящих в состав ИСПДн;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа в ИСПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств защиты информации;
- подавать свои предложения по совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

5.1. Администратор обязан:

- знать и выполнять требования настоящей Инструкции, а также действующих нормативных и руководящих документов регламентирующих порядок действий по защите информации;
- выполнять на автоматизированном рабочем месте только те процедуры, которые требуются для выполнения его должностных обязанностей;
- соблюдать установленные правила разграничения доступа;
- покидая свое рабочее место на кратковременный срок блокировать доступ к операционной среде автоматизированного рабочего места.

5.2. Администратору ИСПДн категорически запрещается:

- разглашать сведения конфиденциального характера, ставшие известными при выполнении служебных обязанностей;

- использовать неучтенные внешние машинные носители информации;
- подключать к автоматизированному рабочему месту мобильные устройства;
- самостоятельно устанавливать или модифицировать программное и (или) аппаратное обеспечение ИСПДн;
- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных (личных) целях;
- оставлять автоматизированное рабочее место без присмотра, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к инцидентам информационной безопасности.

5.3. На Администратора возлагается персональная ответственность за качество проводимых им работ по обеспечению бесперебойного и стабильного функционирования ИСПДн.

5.4. Администратор несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации о ПДн предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.5. Администратор несет ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.4. Настоящая Инструкция вступает в силу с момента её утверждения и действует бессрочно.

6.5. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.6. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.