

2.1.3. Обеспечение выполнения организационных и технических мер защиты информации и ПДн в рамках системы защиты информации информационной системы;

2.1.4. Анализ угроз безопасности информации и ПДн в информационной системе;

2.1.5. Обеспечение должного уровня защищенности информации и ПДн при их обработке в информационной системе;

2.1.6. Координация и контроль деятельности лиц, обеспечивающих защиту информации и ПДн в ходе эксплуатации информационной системы:

* сотрудников, ответственных за управление (администрирование) системой защиты информации информационной системы;
* сотрудников, ответственных за планирование и контроль мероприятий по защите информации в информационной системе;
* сотрудников, ответственных за выявление инцидентов и реагирование на них;
* сотрудников, которым разрешены действия по внесению изменений в конфигурацию информационной системы и ее системы защиты информации;

2.1.7. Содействие лицам, указанным в пункте 2.1.6. по вопросам защиты информации и ПДн;

2.1.8. Взаимодействие с государственными органами Российской Федерации, регулирующими вопросы защиты информации и ПДн, при проведении проверок, а также при обработке запросов указанных органов;

2.1.9. Обеспечение информирования и обучения пользователей информационной системы по вопросам обеспечения информационной безопасности и правилам работы в информационной системе, по вопросам защиты ПДн и правилам безопасной обработки ПДн;

2.1.10. Организация подготовки и периодической переподготовки (повышения квалификации) сотрудников Школы, непосредственно отвечающих за проведение работ по защите информации и ПДн;

2.1.11. Организация и участие в мероприятиях по контролю за обеспечением уровня защищенности информации и ПДн.

2.2. Ответственный обязан:

2.2.1. Знать и соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности информации;

2.2.2. Знать и соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;

2.2.3. Знать состав, структуру, назначение и выполняемые задачи информационной системы, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку информации и ПДн;

2.2.4. Знать состав, структуру и назначение систем защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;

2.2.5. Не разглашать информацию ограниченного доступа, ставшую доступной в ходе исполнения должностных обязанностей;

2.2.6. Контролировать деятельность лиц, обеспечивающих защиту информации и ПДн в ходе эксплуатации информационной системы;

2.2.7. Координировать внедрение и эксплуатацию средств защиты информации;

2.2.8. Периодически (в соответствии с планом мероприятий по защите информации в информационной системе) проводить анализ информационной системы на наличие известных уязвимостей (недостатков, слабостей), угроз безопасности информации в информационной системе;

2.2.9. Периодически (в соответствии с планом мероприятий по защите информации в информационной системе) проводить анализ изменения угроз безопасности информации в информационной системе и оценку возможных последствий от реализации угроз безопасности информации;

2.2.10. Принимать меры по устранению выявленных уязвимостей или по снижению возможностей их использования (эксплуатации);

2.2.11. Информировать пользователей информационной системы о появлении актуальных угроз безопасности информации:

2.2.12. Доводить до пользователей информационной системы требования по защите информации и ПДн, а также положения организационно-распорядительных документов по защите информации и ПДн с учетом внесенных в них изменений;

2.2.13. Обучать пользователей информационной системы правилам эксплуатации средств зашиты информации (при необходимости);

2.2.14. Проводить практические занятия и тренировки с пользователями информационной системы по блокированию угроз безопасности информации и реагированию на инциденты:

2.2.15. Периодически проводить контроль осведомленности пользователей информационной системы об угрозах безопасности информации и проверку уровня знаний пользователей информационной системы по вопросам обеспечения защиты информации и ПДн;

2.2.16. Участвовать в мероприятиях по внутреннему контролю за обеспечением уровня защищенности информации и ПДн;

2.2.17. Обеспечивать поддержание в актуальном состоянии локальных актов по защите информации;

2.2.18. Контролировать соблюдение требовании законодательства Российской Федерации и локальных актов в области зашиты информации пользователями (в том числе привилегированными) информационной системы;

2.2.19. Участвовать в реагировании, анализе и расследованиях инцидентов информационной безопасности;

2.2.20. Организовывать и участвовать в проведении периодического контроля за обеспечением уровня защищенности информации и ПДн;

2.2.21. Документировать процедуру и результаты контроля за обеспечением уровня защищенности информации;

2.2.22. Осуществлять организацию доработки (модернизации) системы защиты информации (при необходимости).

**3. ПРАВА ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ЗА ЗАЩИТУ ИНФОРМАЦИИ, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ, В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

3.1. Ответственный имеет право:

3.1.1. Знакомиться с локальными актами Школы, регламентирующими процессы обработки и зашиты информации и ПДн;

3.1.2. Вносить предложения директору Школы по совершенствованию существующей системы зашиты информации;

3.1.3. Привлекать по согласованию с директором Школы, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011г. №99-ФЗ «О лицензировании отдельных видов деятельности», к работам по созданию, совершенствованию (модернизации, развитию) системы зашиты информации и контролю за обеспечением уровня защищенности информации и ПДн;

3.1.4. Требовать от пользователей информационной системы (в том числе привилегированных) соблюдения требований законодательства Российской Федерации и локальных актов в области защиты информации, обработки и защиты ПДн;

3.1.5. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность информации и ПДн, вносить свои предложения по совершенствованию организационных и технических мер обеспечения безопасности информации и ПДн в информационной системе;

3.1.6. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности и зашиты информации и ПДн;

3.1.7. Обращаться за необходимыми разъяснениями по вопросам обработки персональных данных к ответственному за организацию обработки персональных данных при их обработке в информационных системах.

**4. ОТВЕТСТВЕННОСТЬ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ЗА ЗАЩИТУ ИНФОРМАЦИИ, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ, В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

4.1. Ответственный в соответствии с возложенными на него обязанностями несет персональную ответственность за:

4.1.1. Реализацию Политики в отношении обработки персональных данных в Школе;

4.1.2. Ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией;

4.1.3. Разглашение информации в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации;

4.1.4. Несоблюдение требований локальных актов Школы по защите информации и ПДн, в пределах, установленных трудовым договором (служебным контрактом).

С инструкцией ознакомлена:

Ответственный за организацию

обработки персональных данных в Школе / Г.М.Мухаметшина /