

Инструкция

ответственного за обеспечение безопасности персональных данных в информационных системах персональных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – Ответственный) назначается приказом (далее – Учреждение) и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн) Учреждения.

1.2. Ответственный должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.

1.3. Методическое руководство работой Ответственного осуществляет Ответственный за организацию обработки ПДн.

2. ОСНОВНЫЕ ФУНКЦИИ И ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Функции Ответственного:

2.1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по защите ПДн при решении следующих основных вопросов: проведение аналитической работы по комплексной защите и предупреждению утечки ПДн; подготовка решений в отношении сведений о работах, выполняемых Учреждением, подлежащих защите; рассмотрение проектов технических заданий, нормативных актов и– указаний, договоров на выполнение работ, отчетной документации, с целью определения достаточности предусмотренных в них требований и мероприятий по комплексной защите ПДн, при координация внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами; проведение работ по контролю эффективности принимаемых мер по выявлению и закрытию возможных каналов утечки ПДн; подготовка предложений по совершенствованию действующей системы защиты ПДн с последующим предоставлением Ответственному за организацию обработки ПДн Учреждения и/или директору; учет

применяемых средств защиты информации, эксплуатационной и технической документации к ним носителей ПДн; обеспечение соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда; осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

Ответственный обязан:

2.2. Соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.

2.3. Знать состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн.

2.4. Осуществлять общее техническое сопровождение ИСПДн: контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств; контролировать сохранность пломб на оборудовании автоматизированных рабочих мест; вести журнал учета и выдачи используемых материальных носителей ПДн; контролировать использование съемных материальных носителей информации, в том числе запрещать использование неучтенных носителей информации; проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ИСПДн Учреждения (далее – Пользователи ИСПДн) по правилам работы в ИСПДн.

2.5. Осуществлять настройку и сопровождение подсистемы регистрации и учета ИСПДн: реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка сотрудников, допущенных к работе в ИСПДн; назначать пароли Пользователей ИСПДн; контролировать плановую смену паролей Пользователями ИСПДн– для доступа в ИСПДн; своевременно удалять профиль Пользователя ИСПДн при увольнении или переводе сотрудника; вводить в базу данных системы защиты от несанкционированного доступа (далее НСД) описания событий, подлежащих регистрации в системном журнале; регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа к ИСПДн; своевременно информировать Ответственного за организацию обработки ПДн о несанкционированных действиях персонала для организации расследования попыток НСД.

2.6. Сопровождать подсистему обеспечения целостности рабочего

программного обеспечения (ПО) ИСПДн: обеспечивать регулярное и своевременное обновление– антивирусного программного обеспечения Учреждения; обеспечивать поддержание установленного порядка эксплуатации– антивирусного программного обеспечения; обеспечивать регулярное и своевременное создание резервных– копий ИСПДн Учреждения; осуществлять настройку и сопровождение системы защиты от НСД в ИСПДн.

2.7. Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИСПДн.

2.8. Требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

2.9. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований фактов НСД.

2.10. Участвовать при проведении внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн.

2.11. Контролировать выполнение Пользователями ИСПДн требований Инструкции пользователя информационных систем персональных данных , а также установленных требований для обеспечения уровней защищенности ПДн.

2.12. Контролировать правильность применения Пользователями ИСПДн средств защиты информации.

2.13. В случае получения от Пользователей ИСПДн информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности ПДн в пределах своих полномочий.

2.14. Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИСПДн: антивирусного программного обеспечения;– средств защиты от несанкционированного доступа.

2.15. В случае нарушения работоспособности технических средств и программного обеспечения ИСПДн. в том числе средств защиты ИСПДн. принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

2.16. Своевременно информировать Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ИСПДн.

3. ПРАВА ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственный имеет право:

3.1. Знакомиться с нормативными актами Учреждения, регламентирующими процессы обработки и защиты ПДн.

3.2. Вносить предложения директору по совершенствованию существующей системы защиты информации.

3.3. Привлекать по согласованию Ответственным за организацию обработки ПДн и директором к работе по созданию и совершенствованию системы защиты ПДн других сотрудников Учреждения.

3.4. Требовать от Пользователей ИСПДн соблюдения требований Инструкции пользователя информационных систем персональных данных , а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.

3.5. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность ПДн. вносить свои предложения по совершенствованию организационных и технических мер защиты ПДн в ИСПДн.