**Порядок работы с пакетом документов по защите персональных данных**

|  |
| --- |
| Используемые сокращения:  **ПДн** – персональные данные;  **ИСПДн** – информационная система персональных данных |

1. Руководителю организации утвердить разработанные документы.
2. В случае, если организация не внесена в Реестр операторов, осуществляющих обработку ПДн (<http://rkn.gov.ru/personal-data/register/>), направить в Роскомнадзор **уведомление об обработке (о намерении осуществлять обработку) ПДн** (<http://pd.rkn.gov.ru/operators-registry/notification/form/>).
3. В случае изменения данных, указанных в Уведомлении об обработке (о намерении осуществлять обработку) ПДн, отправленном ранее, направить в Роскомнадзор **информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн** (<http://rkn.gov.ru/personal-data/forms/p333/>).
4. Опубликовать на сайте организации Политику в отношении обработки ПДн / Положение об обработке ПДн.
5. Ответственному за организацию обработки ПДн (назначается приказом/ распоряжением «Об ответственном за организацию обработки ПДн») ознакомиться со всеми документами, с Инструкцией ответственного за организацию обработки ПДн ознакомиться под роспись.
6. Ответственному за организацию обработки ПДн контролировать порядок сбора согласий субъектов ПДн (работников, клиентов и т.д.) на обработку их ПДн (универсальная форма согласия на обработку ПДн представлена в приложении к приказу/ распоряжению «Об утверждении правил обработки ПДн»).
7. Ответственному за обеспечение безопасности ПДн в ИСПДн (назначается приказом/ распоряжением «Об ответственном за обеспечение безопасности ПДн в ИСПДн») ознакомиться с Инструкцией ответственного за обеспечение безопасности ПДн в ИСПДн под роспись.
8. Ответственному за обеспечение безопасности ПДн в ИСПДн завести и поддерживать в актуальном состоянии Журнал учета материальных носителей ПДн (форма Журнала приведена в приложении к приказу/ распоряжению «Об обеспечении безопасности материальных носителей ПДн»).
9. Сотрудникам, осуществляющим обработку ПДн и имеющим доступ к обрабатываемым ПДн, подписать следующие формы, приведенные в приложениях к приказу/ распоряжению «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области ПДн»:

* Уведомление о факте обработки ПДн без использования средств автоматизации;
* Обязательство о соблюдении конфиденциальности ПДн;
* Форму ознакомления с положениями законодательства Российской Федерации о персональных данных,локальными актами организации по вопросам обработки персональных данных;
* Типовое обязательство о прекращении обработки ПДн в случае расторжения служебного контракта (трудового договора) (для государственных или муниципальных служащих);
* Разъяснение субъекту ПДн юридических последствий отказа предоставить свои ПДн (для государственных или муниципальных служащих).

1. Сотрудникам, осуществляющим обработку ПДн и имеющим доступ к обрабатываемым ПДн, ознакомиться под роспись:

* с Политикой в отношении обработки ПДн / Положением об обработке ПДн;
* с Инструкцией пользователя ИСПДн (Инструкция является приложением к приказу/ распоряжению «Об утверждении перечней сотрудников, осуществляющих обработку ПДн и имеющих доступ к обрабатываемым ПДн»);
* с Порядком хранения, использования и передачи ПДн сотрудников;
* с Порядком доступа в помещения, в которых осуществляется обработка ПДн и размещены ИСПДн (Порядок является приложением к приказу/ распоряжению «Приказ о контролируемой зоне помещений»);
* с Приказом/ распоряжением «О введении в действие документов, направленных на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами» (для государственных или муниципальных служащих).

1. Сотрудникам, входящим в состав комиссии по определению уровня защищенности ПДн при их обработке в ИСПДн, подписать Акты определения уровня защищенности ПДн при их обработке в ИСПДн (отдельно для каждой ИСПДн).
2. Ответственному пользователю криптосредств (назначается приказом/ распоряжением «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты») ознакомиться с Инструкцией ответственного пользователя криптосредств под роспись.
3. Ответственному пользователю криптосредств завести и поддерживать в актуальном состоянии документы по учету криптосредств (формы документов утверждены приказом/ распоряжением «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты»).
4. Пользователям криптосредств ознакомиться с Инструкцией пользователя криптосредств под роспись (Инструкция является приложением к приказу/ распоряжению «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты»).
5. Лицам, имеющим доступ в помещения, где размещены используемые криптосредства, ознакомиться с Порядком доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств, под роспись (Порядок является приложением к приказу/ распоряжению «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты»).
6. Лицам, включенным в Перечень сотрудников, ответственных за выявление инцидентов информационной безопасности и реагирование на них, ознакомиться с Регламентом выявления инцидентов информационной безопасности и реагирование на них под роспись (Регламент является приложением к приказу/ распоряжению «О сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них») (при наличии данного документа).
7. Лицам, включенным в Перечень сотрудников, которым разрешены действия по внесению изменений в базовую конфигурацию информационных систем и системы защиты персональных данных, ознакомиться с Регламентом внесения изменений в конфигурацию информационных систем и системы защиты персональных данных под роспись (Регламент является приложением к приказу/ распоряжению «О сотрудниках, которым разрешены действия по внесению изменений в базовую конфигурацию информационных систем и системы защиты персональных данных») (при наличии данного документа).
8. Распечатать, оформить и поддерживать в актуальном состоянии журналы, приведенные в приложениях к:

* Приказу/распоряжению «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области ПДн»;
* Приказу/распоряжению «Об обеспечении безопасности материальных носителей ПДн»;
* Приказу/распоряжению «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты»;
* Приказу/распоряжению «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации при ведении журнала, содержащего ПДн, необходимые для однократного пропуска субъекта ПДн на территорию оператора».

1. Распечатать и оформить в виде журнала План внутренних проверок режима защиты персональных данных, приведенный в приложении к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
2. Ознакомиться и принять меры, указанные в следующих рекомендациях:

* Рекомендации по внесению изменений в Должностные инструкции персонала в части обеспечения безопасности ПДн при их обработке в ИСПДн;
* Рекомендации по выполнению требований по обеспечению безопасности ПДн в ИСПДн, эксплуатируемых с использованием криптосредств.