SAFE-DOC.COM
ОНЛАЙН-СЕРВИС ПОДГОТОВКИ ДОКУМЕНТОВ

Порядок работы с пакетом документов по защите информации, формируемый в онлайн сервисе подготовки документов SAFE-DOC.com

Используемые сокращения:
ПДн – персональные данные
ИСПДн – информационная система персональных данных
ГИС – государственная информационная система

Данная памятка содержит перечень действий для Организаций, которые уже выполнили основные работы с сервисом Safe-doc.com (указали всю необходимую информацию об организации и её структуре, информационных системах персональных данных. Определились с ответственными лицами, отделами и составами комиссий), сформировали пакет документов в сервисе Safe-doc и выгрузили его. В данном документе содержится список необходимых действий, которые необходимо выполнить Организации, чтобы привести в соответствии все процессы с требованиями законодательства.

1. После выгрузки пакета Руководителю Организации необходимо утвердить документы. (Приказы/Распоряжение/Постановление/Указание/Решение). Далее по тексту «Приказ».
2. Если ваша Организация ещё не направляла в Роскомнадзор **уведомление об обработке (о намерении осуществлять обработку) ПДн,** то это необходимо сделать (http://pd.rkn.gov.ru/operators-registry/notification/form/). Данную операцию также можно провести при помощи сервиса Safe-doc.com **(**https://pd.safe-doc.com/#/pd/1/4/0). При использовании Safe-doc (с условием того, что Организация указала всю необходимую информацию для генерации пакета документов), часть необходимой для подачи уведомления информации уже будет заполнена в опросном листе. Пользователю останется лишь внести недостающие сведения и нажать кнопку «Отправить». Дальше сервис самостоятельно отправит всю необходимую информацию на Портал персональных данных Уполномоченного органа по защите персональных данных. Пользователь в ответ получит зарегистрированный номер заявления и ключ, по которым можно отслеживать статус поданного уведомления.

Если вы не знаете, регистрировалась ли ваша Организация как оператор, осуществляющий обработку персональных данных, то это можно сделать на портале Роскомнадзора (http://pd.rkn.gov.ru/operators-registry/operators-list/) указав наименование Организации, регистрационный номер или ИНН.

3. Если вы уже подавали уведомление в Роскомнадзор и вам необходимо внести изменения, в сведения, указанные в Уведомлении об обработке (о намерении осуществлять обработку) ПДн, отправить **информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн** (http://rkn.gov.ru/personal-data/forms/p333/), то вы также можете воспользоваться возможностями сервиса safe-doc.com
(ПРИ УСЛОВИИ, ЧТО ВЫ ПОДАВАЛИ УВЕДОМЛЕНИЕ ЧЕРЕЗ СЕРВИС SAFE-DOC.COM)

В случае изменения сведений, указанных в уведомлении, а также в случае прекращения обработки ПДн Оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

!!! ВАЖНО !!!

Помимо электронного заявления необходимо также направить бумажный экземпляр уведомления в Ваше территориальное управление Роскомнадзора. Без данного действия подача уведомления и внесения изменений не будут учтены.

Это касается как подачи, так и внесения изменений в Реестр операторов, осуществляющих обработку персональных данных.

4. Сформировать, выгрузить и утвердить Модели угроз для каждой ИСПДн (https://pd.safe-doc.com/#/pd/1/2/0)

5. Опубликовать на сайте организации Политику в отношении обработки персональных данных.

(Приложение 1 к приказу **«Об организации работы с персональными данными»**).

В случае, если ПДн собираются через сайт, необходимо указать владельца и местоположение базы ПДн.

6. Ответственному за ознакомление с приказами необходимо:

- ознакомить под роспись с приказами сотрудников допущенных к сведениям, содержащим конфиденциальную информацию и персональные данные;
- взять с работников, допущенных к сведениям, содержащим конфиденциальную информацию и персональные данные, обязательство о неразглашении сведений конфиденциального характера.
- ознакомить под роспись сотрудников с инструкцией пользователя информационных систем,

Системных администраторов с инструкцией администратора информационных систем.

7. Ответственному за организацию за обработку ПДн и ответственному за обеспечение безопасности ПДн взять согласия субъектов ПДн (работников, клиентов и т.д.) на обработку их ПДн (форма согласия на обработку ПДн представлена в приложении 11 к приказу **«Об организации работы с персональными данными»**). Данную форму передать в подразделения, работающие с клиентами (гражданами. Пациентами) для своевременного оформления согласий.

8. Ответственному за обеспечение безопасности распечатать, оформить и поддерживать в актуальном состоянии журналы, утвержденные приказами, формируемыми в Сервисе.

Список журналов:

- Журнал учета средств защиты информации
- Журнал учета организационно-распорядительных документов
- Журнал выдачи электронных идентификаторов
- Журнал учета парольных карт
- Журнал проверки исправности и технического обслуживания
- Журнал регистрации обращений субъектов персональных данных на предоставление доступа к своим персональным данным
- Журнал проведения инструктажа по информационной безопасности
- Журнал учета мероприятий по контролю за исполнением правил обработки персональных данных
- Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов
- Журнал учета и уничтожения носителей с ключевой информацией
- Журнал выдачи носителей с ключевой информацией

- Журнал регистрации ключей от режимных помещений
- Журнал учета хранилищ
- Журнал регистрации выдачи сдачи ключей от режимных помещений
- Журнал регистрации выдачи сдачи ключей от хранилищ
- Журнал технический (аппаратный)

Все представленные журналы можно вести в электронном виде посредством сервиса safe-doc. (https://pd.safe-doc.com/#/pd/1/1/5). В данном разделе вы можете сами определить, какие журналы вы будете вести в электронном виде.

9. Сотрудникам, входящим в состав комиссии по определению класса ГИС и уровня защищенности ПДн при их обработке в ИС, подписать:

- Акты определения уровня защищенности ПДн при их обработке в ИСПДн (отдельно для каждой ИСПДн) (https://pd.safe-doc.com/#/pd/1/1/6);
- Акты определения класса защищенности ГИС (отдельно для каждой ГИС) (https://pd.safe-doc.com/#/gis/1/1/4)

Так же в сервисе можно в автоматическом режиме сформировать следующие акты.

- Обязательство о неразглашении сведений конфиденциального характера;
- Парольная карта;
- Заявка на внесение изменений в состав аппаратно-программных средств ИС;
- Акт об удалении информации (остаточной), хранившейся на диске компьютера;
- Акт установки оборудования;
- Акт установления уровня защищенности информационной системы персональных данных;
- Акт об удалении (уничтожении) персонифицированных записей из информационных систем персональных данных;
- Заявление о согласии на обработку персональных данных;
- Заявление на создание (продление) учетной записи пользователя;
- Заявление на изменение полномочий пользователя;
- Заявление на блокировку учетной записи пользователя;
- Акт ввода в эксплуатацию средств криптографической защиты информации;
- Протокол проведения внутренней проверки условий обработки ПДн;
- Заключение о допуске к самостоятельной работе с средствами криптографической защиты информации;
- Разъяснение субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
- Уведомление об уничтожении персональных данных;
- Уведомление об устранении нарушений;
- Уведомление субъекта об обработке его персональных данных;
- Заявление об ознакомлении с информацией;
- Отметка об исполнении Заявления субъекта персональных данных;
- Карточка данных об инциденте информационной безопасности.

10. Всем сотрудникам, деятельность которых подразумевает работу с СКЗИ пройти обучение согласно утвержденной программе. Комиссии по допуску к самостоятельной работе СКЗИ провести опрос пользователей и принять решении о допуске к работе с СКЗИ для каждого пользователя.

11. Ответственному пользователю криптосредств (назначается приказом **«О назначении ответственного пользователя криптосредств»**) ознакомить всех сотрудников, допущенных к работе с СКЗИ с Порядоком работы со средствами криптографической защиты информации. (Приложение 3 к приказу **«О назначении ответственного пользователя криптосредств»**)

12. Ответственному пользователю криптосредств завести и поддерживать в актуальном состоянии документы по учету криптосредств.

13. Ответственному пользователю криптосредств ознакомить лиц, имеющих доступ в помещения, где размещены используемые криптосредства, с Порядоком размещения специального оборудования, охраны и организации режима в выделенных (режимных) помещениях. (Приложение 4 к приказу **«О назначении ответственного пользователя криптосредств»**)

14. Внести изменения в должностные регламенты (инструкции) сотрудников необходимую информацию в части обязанности обработки персональных данных.

В случае, когда Ваша организация делегирует полномочия по защите ПДн (полностью или частично) другой организации (Вышестоящей организации, Интегратору в области защиты информации и др.) Вам необходимо внести изменения в уже выгруженные документы и по необходимости изменить ответственных лиц на сотрудников или подразделения Организации которые занимается вопросами информационной безопасности.

Особое внимание нужно уделить договорам на обслуживание информационных систем, где могут встретиться персональные данные (бухгалтерские, программы подачи отчетностей). Для таких договоров необходимо прописать пункты о конфиденциальности и разделение полномочий по облуживанию данных информационных систем. Это также относится к договорам об обеспечении физической безопасности зданий (физическая охрана).