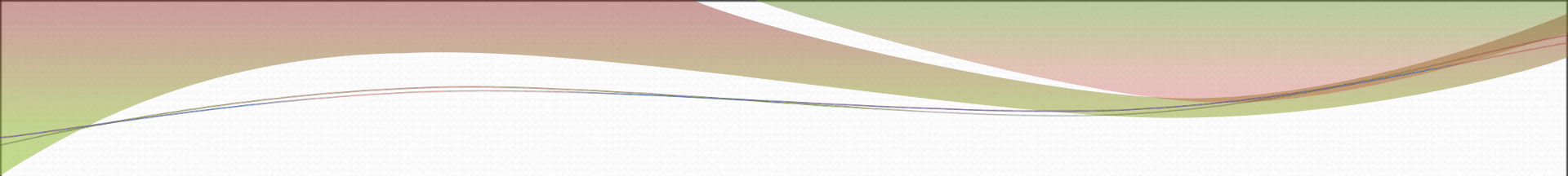


Система защиты персональных данных



Уровень правовой грамотности ИТ-специалистов в области информационной безопасности, в частности защиты персональных данных, с каждым годом растет. Это связано с тем, что именно на специалиста ИТ-отдела возлагают функции по защите информации.

Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Система защиты персональных данных призвана нейтрализовывать актуальные угрозы их безопасности. Она включает в себя организационные и (или) технические меры.

Последние зависят от установленного уровня защищенности персональных данных. Он определяется исходя из типа угроз (приведена их классификация), вида персональных данных (биометрические, общедоступные и пр.), количества их субъектов и прочих факторов.

За безопасность персональных данных отвечает оператор системы, который их обрабатывает, или уполномоченное им лицо.

Оператор системы выбирает средства защиты информации в соответствии с нормативными актами ФСБ России и ФСТЭК России.

Выполнение требований контролируется оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юрлиц и ИП. Последние должны иметь лицензию на занятие деятельностью по технической защите конфиденциальной информации.

ДИСЦИПЛИНАРНАЯ ОТВЕТСТВЕННОСТЬ

К дисциплинарной ответственности за нарушения при работе с персональными данными можно привлечь к ответственности работников, которые в силу трудовых отношений обязаны соблюдать правила работы с личными данными, но нарушили их (ст. 192 ТК РФ).

МАТЕРИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

Материальная ответственность работника может наступить, если в связи с нарушением правил работы с персональными данными организации причинен прямой действительный ущерб (ст. 238 ТК РФ).

Дисциплинарную и материальную ответственность работодатель применяет исключительно по своему усмотрению. Государственные контролирующие органы (в том числе., Роскомнадзор) в этом процессе участия не принимают.

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ

За нарушение порядка сбора, хранения, использования или распространения персональных данных работодателя и должностных лиц контролирующие органы могут привлечь к административной ответственности в виде штрафов, описаны в статьях 13.11 и 13.14 Кодекса РФ об административных правонарушениях.

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ

Уголовная ответственность для директора, главного бухгалтера или начальника отдела кадров организации или другого лица, ответственного за работу с персональными данными, может наступить за незаконные действия: сбор или распространение сведений о частной жизни сотрудника, составляющих его личную или семейную тайну, без его согласия; распространение сведений о работнике в публичном выступлении, публично демонстрирующемся произведении или СМИ.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: УЖЕСТОЧЕНИЕ ОТВЕТСТВЕННОСТИ ДЛЯ РАБОТОДАТЕЛЕЙ С 1 ИЮЛЯ 2017 ГОДА

С 1 июля 2017 года существенно ужесточена ответственность за нарушения при взаимодействии с персональными данными физических лиц. Это следует из положений Федерального закона от 07.02.2017 № 13-ФЗ). Изменения затронут всех без исключения работодателей, которые связаны с обработкой персональных данных сотрудников и подрядчиков - физических лиц.

НАРУШЕНИЕ

- 1. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В «ИНЫХ» ЦЕЛЯХ**
- 2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ СОГЛАСИЯ**
- 3. ДОСТУП К ПОЛИТИКЕ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**
- 4. СОКРЫТИЕ ИНФОРМАЦИИ**
- 5. УТОЧНЕНИЯ ИЛИ БЛОКИРОВКА**
- 6. СОХРАННОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ**
- 7. ОБЕЗЛИЧИВАНИЕ**

Купить сертифицированную ФСТЭК учетную программу и успокоиться — это ли не мечта кадровика, бухгалтера, ИТ-специалиста!

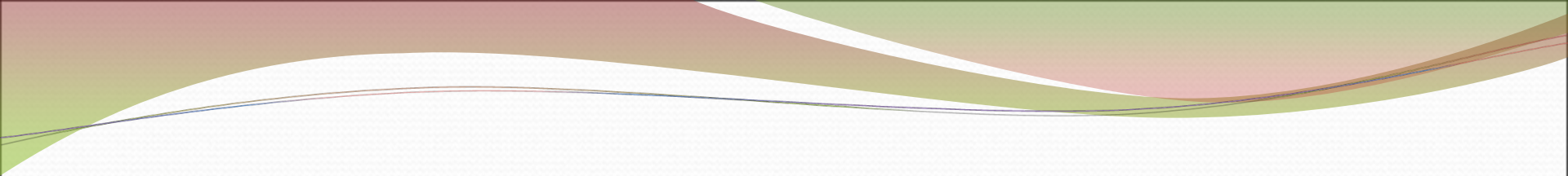
К сожалению, работа в прикладной сертифицированной программе не отменяет выполнение комплекса мер по защите персональных данных при их обработке в информационных системах.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Программа — данные, предназначенные для управления конкретными компонентами системы обработки информации в целях реализации определенного алгоритма («Обеспечение систем обработки информации программное. Термины и определения. ГОСТ 19781-90»).

Таким образом, информационная система включает в себя базы данных, компьютеры, на которых располагаются эти базы данных, а также программы, обрабатывающие эту информацию. Программа — лишь одна из составляющих всей информационной системы.

Федеральный закон № 152-ФЗ предъявляет требования в первую очередь к защите информационной системы, обрабатывающей персональные данные, а не конкретно к программе.



Семь шагов к созданию системы
защиты персональных данных в
организации

1 шаг

издание Приказа по организации о начале работ по созданию системы защиты персональных данных в организации. Этот шаг оформляется приказом по организации «Об организации работ по обеспечению безопасности ПДн». Приказ состоит:

- назначается ответственный сотрудник организации за осуществление мероприятий, по защите персональных данных;
- дается указание о разработке локальной документации, относящейся к защите персональных данных;
- создается комиссия по защите и обработке персональных данных в организации;
- утверждается и вводится в действие Положение по защите и обработке персональных данных в организации.

2 шаг

Проведение обследования информационных систем ПДн организации и определения класса информационной системы персональных данных.

По результатам реализации этого шага в организации появляются следующие документы:

- отчет об обследовании информационных систем персональных данных;
 - Приказ «О создании комиссии по классификации информационных систем персональных данных»;
 - Акт классификации типовой информационной системы персональных данных
- и, как приложение к Положению о защите и обработке ПДн в организации, «Примерная модель угроз безопасности данных, обрабатываемых в информационных системах персональных данных».

3 шаг

Направление Уведомления об обработке (о намерении осуществлять обработку) персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Кемеровской области. Бланк Уведомления можно скачать на сайте, но отправить документ нужно обязательно по почте, электронного вида недостаточно. При заполнении имеет смысл пользоваться Рекомендациями по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных.

4 шаг

Разработка, утверждение и применение документов:

«Согласие на обработку персональных данных» и
«Отзыв согласия на обработку ПДн».

5 шаг

внедрение системы защиты персональных данных. С точки зрения организационных мероприятий этот шаг включает в себя:

- составление и утверждение перечня лиц, допущенных к обработке ПДн (здесь очень важно не забыть уведомить самих лиц о то, что они обрабатывают персональные данные!);
- создание и утверждение Перечня ПДн, обрабатываемых в организации;
- создание и утверждение Положения об обработке и защите ПДн в организации с обязательным листом ознакомления Положением и еще, как минимум, двумя документами к ним - Обязательством об обеспечении конфиденциальности персональных данных сотрудниками организации, Приказом о выделении помещений для обработки персональных данных;
- создание и утверждение документа с названием «Описание системы защиты персональных данных при их обработке в информационных системах персональных данных в организации. К описанию необходимо приложить:

- создание и утверждение документа с названием «Описание системы защиты ПДн при их обработке в информационных системах ПДн в организации. К описанию необходимо приложить:
- инструкцию пользователю по соблюдению режима защиты информации при работе в информационных системах ПДн;
- инструкцию администратору безопасности информационных систем ПДн организации;
- инструкцию по резервному копированию и восстановлению данных в информационных системах ПДн;
- положение о разграничении прав доступа к обрабатываемым ПДн в информационных системах ПДн в организации.

6 шаг

необходимо определиться с техническими средствами защиты персональных данных. Технические средства защиты ПДн:

- от несанкционированного доступа;
- антивирусные средства;
- межсетевые экраны;
- криптографические средства.

Все применяемые средства должны быть сертифицированы. Реестр сертифицированных средств защиты информации можно найти на сайте ФСТЭК России. После выбора, приобретения и установки средства необходимо правильно настроить!

Документами, подтверждающими реализацию шестого шага, являются:

- перечень средств защиты персональных данных;
- журнал учета и хранения носителей персональных данных;
- акт установки средств защиты информации;
- утвержденная форма акта списания и уничтожения электронных носителей информации;
- утвержденная форма акта уничтожения документов;
- подписанные соглашения о неразглашении персональных данных с третьими лицами (организациями) или соответствующие оговорки в контрактах и соглашениях (в особенности при трансграничной передаче данных).

7 шаг

- создание и подписание «Заключения о соответствии системы защиты персональных данных, обрабатываемых в информационных системах персональных данных организации».

Если Вы сделали все эти шаги и завели в организации «Журнал учета обращений субъектов персональных данных о выполнении их законных прав в области выполнения требований действующего законодательства (в части обеспечения безопасности персональных данных)», то требования **Закона Российской Федерации от 27.07.2006 № 152 – ФЗ «О персональных данных»** Вы, в **основном**, выполняете.

Распространенные ошибки при построении СЗПДн:

1. Неверно определено число информационных систем, обрабатывающих ПДн.
2. Неверный выбор средств защиты информации.
3. Пренебрежение организационными мерами, концентрация исключительно на технической защите.
4. Средства защиты информации верно подобраны, но неверно настроены (или не настроены вообще).

Важно помнить, что когда Вы приобретаете новое оборудование, устанавливаете новые программы, и вносите изменения в структуру – нужно не забывать вносить изменения в весь комплекс вышеперечисленных документов.

Выводы:

- 1.** Для того чтобы не упустить из виду информационные системы персональных данных, необходимо провести аудит всех имеющихся информационных систем, а затем установить факт обработки в них ПДн. Не забывайте про системы видеонаблюдения, так как в отдельных случаях они также являются ИСПДн.
- 2.** Не забывайте об организационно-распорядительных документах.

3. Используйте известный алгоритм создания системы защиты персональных данных:

проведите обследование информационной системы;

определите актуальные угрозы безопасности персональных данных, в соответствии с нормативными документами ФСТЭК России;

определите требуемый уровень защищенности персональных данных, обрабатываемых в информационной системе;

руководствуясь приказом ФСТЭК России № 21, определите организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных.

Наличие у программы сертификата соответствия ФСТЭК не решает проблемы защиты ПДн. Существует множество средств защиты информации и сценариев их использования. Для построения эффективной и адекватной системы защиты персональных данных важно понимать принципы и порядок реализации мер, направленных на обеспечение безопасности ПДн.