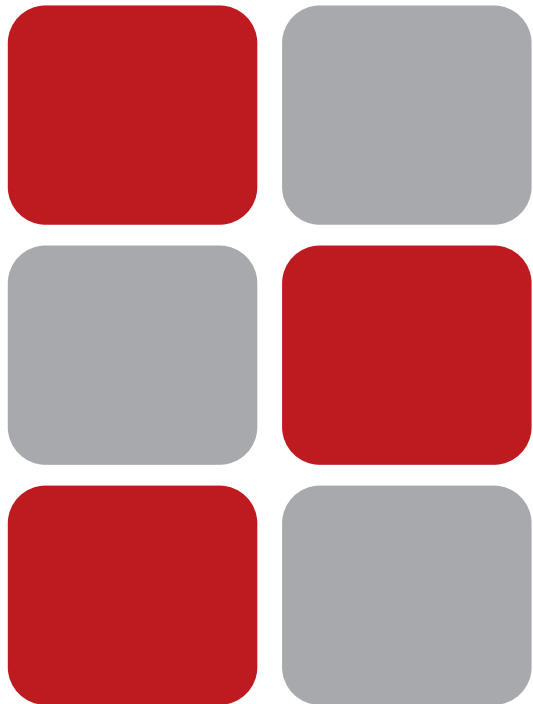


**БЕЗОПАСНОСТЬ
ПЕРСОНАЛЬНЫХ
ДАНЫХ:**
ВОПРОСЫ И ОТВЕТЫ



Кому нужна защита персональных данных?

В первую очередь в безопасности своих персональных данных заинтересованы лица (субъекты персональных данных), информация о которых обрабатывается третьими сторонами. По оценкам экспертов, сведения о каждом россияне обрабатываются в среднем в пяти различных информационных системах (например, в системах учета полисов ОМС, в системах бронирования и продажи билетов, в информационно-справочных и биллинговых системах операторов связи, в кадровых системах предприятий, в банковских информационных системах и т.п.).

С принятием федерального закона № 152-ФЗ «О персональных данных», появлением соответствующих постановлений Правительства России и методических документов федеральных органов исполнительной власти проблема защиты персональных данных остро встала перед операторами персональных данных – государственными и муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку персональных данных.

В сфере действия закона находятся самые разные отрасли и сферы деятельности: телеком, организации кредитно-финансового сектора, страховые компании, транспортные предприятия, медицинские учреждения, государственные организации.

Почему оператор должен обратить внимание на защиту персональных данных? Насколько велики риски?

Невыполнение законодательства в области защиты персональных данных – это правонарушение с точки зрения государственных регуляторов и риск для бизнеса с точки зрения частных инвесторов или учредителей. Несмотря на то, что по разным оценкам до 7 млн операторов персональных данных попадают под действие № 152-ФЗ, их многочисленность не должна создавать иллюзий о невозможности привлечения к ответственности. Имеется информация о проведении проверок предприятий и организаций со стороны федерального органа исполнительной власти, уполномоченного в области защиты прав субъектов персональных данных (Роскомнадзор), и вынесении предупреждений о несоответствии порядка обработки персональных данных требованиям, установленным законодательством в этой области. Учитывая, что одной из мер воздействия на нарушителей закона «О персональных данных» помимо штрафов и дисциплинарной ответственности руководителей может быть приостановление деятельности предприятия (организации) в случае выявления неоднократных нарушений, можно судить об исключительной важности соблюдения требований № 152-ФЗ и других нормативно-правовых актов в области защиты персональных данных.

Какими нормативными документами следует руководствоваться при организации защиты персональных данных?

Основным законодательным актом в этой области является федеральный закон № 152-ФЗ «О персональных данных». Помимо указанного закона в сферу защиты персональных данных попадает еще ряд представленных далее на иллюстрации федеральных нормативных актов: постановления правительства, приказы федеральных органов исполнительной власти, а так же руководящие и методические документы государственных регуляторов.

Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006 г.

Постановление Правительства РФ от 17.11.2007 г. № 781
«Об утверждении положения об обеспечении безопасности ПДн* при их обработке в ИСПДн**»

Постановление Правительства РФ от 15.09.2008 г. № 687
«Об утверждении положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»

Постановление Правительства РФ от 06.07.2008 г. № 512
«Об утверждении требований к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн»

Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. № 55/86/20
«Об утверждении порядка проведения классификации ИСПДн»

Приказ Россвязьзохранкультуры № 154 от 28.03.2008 г.
«Об утверждении положения о ведении реестра операторов, осуществляющих обработку ПДн»

Приказ Россвязькомнадзора № 08 от 17.07.2008 г.
«Об утверждении образца формы уведомления об обработке ПДн»

Приказ ФСТЭК России от 5 февраля 2010 г. № 58
«Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»

Методические рекомендации по обеспечению с помощью криптографических средств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации.
Утв. руководителем 8 Центра ФСБ РФ 21.02.2008 г. № 149/54-144

Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн.
Утверждена заместителем директора ФСТЭК России 15.02.2008 г.

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, содержащей сведения, не составляющие гостайну, в случае их использования для обеспечения безопасности ПДн при их обработке в ИСПДн.
Утв. руководителем 8 Центра ФСБ РФ 21.02.2008 г. № 149/6/6-622

Базовая модель угроз безопасности ПДн при их обработке в ИСПДн.
Утверждена заместителем директора ФСТЭК России 15.02.2008 г.

*ПДн – персональные данные

**ИСПДн – информационные системы персональных данных

Какие действия следует предпринять для выполнения требований законодательства в области защиты персональных данных?

Что является основанием для обработки персональных данных?

В целях правильной организации обработки персональных данных в информационной системе действующими нормативными актами предписано выполнение ряда последовательных шагов. Оператор вправе реализовать все мероприятия самостоятельно, но наиболее оправданным решением представляется передача указанных вопросов в зону ответственности специалистов профильной организации, обладающих необходимыми знаниями и опытом выполнения подобных работ.

Обработка персональных данных с использованием средств автоматизации законна при наличии правового основания обработки персональных данных и при условии выполнения требований действующего законодательства в области защиты персональных данных, что подтверждается необходимыми документами и наличием системы защиты персональных данных, построенной в соответствии с методическими указаниями и рекомендациями регуляторов.

Оформить правовое основание обработки персональных данных (в т. ч. подать уведомление в Роскомнадзор в случаях, предусмотренных НПА) и спланировать мероприятия по их защите

Разработать и ввести в действие документы, регламентирующие обработку и защиту ПДн в организации

Спроектировать и реализовать систему защиты персональных данных с применением средств защиты информации и организационных мер

Провести аттестацию по требованиям безопасности информации (в установленных случаях)

Какими организационно-нормативными документами должен располагать оператор персональных данных?

Необходимый перечень документов определяется как прямыми требованиями нормативно-правовых актов, так и практикой их выполнения. Помимо акта классификации ИСПДн и уведомления об обработке ПДн, направляемого в установленных случаях в Роскомнадзор, потребуется разработка еще целого ряда документов, в т. ч. перечня ПДн, частной модели угроз, плана мероприятий по защите ПДн и плана проверок состояния защиты ПДн, положений и инструкций в области организации обработки и защиты персональных данных, должностных регламентов лиц, имеющих доступ к ПДн, приказов руководителя (о классификации ИСПДн, о назначении ответственных лиц по защите ПДн, о допуске к работе с ПДн, об утверждении мест хранения носителей ПДн и т. п.), письменных согласий субъектов ПДн на обработку их ПДн (в установленных случаях), а так же иных документов, отражающих исполнение оператором требований законодательства в области организации обработки и защиты ПДн. Важно так же наличие выписки из федерального реестра операторов ПДн (выписки из приказа Роскомнадзора о включении в реестр), а так же – в установленных случаях – аттестата соответствия ИСПДн требованиям безопасности информации.

В чем состоят отличия подхода «ИНФОРИОН» к обеспечению безопасности персональных данных?

Главным принципом создания СЗПДн, помимо принципа строгого соответствия требованиям законодательства, мы считаем неразрывность процессов обеспечения конфиденциальной информации вообще и персональных данных в частности.

В большинстве случаев состав угроз информационной безопасности и взгляды руководства организации требуют создания более широкого поля сервисов защиты, нежели это предусмотрено руководящими и методическими документами уполномоченных федеральных органов исполнительной власти. В таких случаях осуществляется разработка системы защиты персональных данных в составе более масштабной комплексной системы обеспечения информационной безопасности, реализующей дополнительные требования по обеспечению защиты информации, в т. ч. за рамками ИСПДн. Объединение в одном проекте системы защиты персональных данных и комплексной системы обеспечения информационной безопасности позволяет более рационально осуществлять инвестиции в ИБ, не отрывая в контексте безопасности персональные данные от других категорий защищаемой конфиденциальной информации и обеспечивая реализацию дополнительных современных механизмов и технологий безопасности.

Мы озабочены выполнением требований законодательства и обеспечением безопасности персональных данных. Намерены прибегнуть к помощи профильной организации. Как будет организована работа по созданию системы защиты персональных данных в нашей информационной системе?

Практика компании «ИНФОРИОН» в общем случае предполагает три основных этапа выполнения работ:

1. Предпроектный этап – оценка текущего уровня защищенности персональных данных и правильности процессов организации их обработки.

2. Этап проектирования и развертывания – выработка рекомендаций по защите, выбор и обоснование основных способов защиты, разработка технических решений (проектирование), подготовка пакета ОРД, развертывание системы защиты персональных данных.

3. Этап ввода в действие – опытная эксплуатация и приемка системы защиты персональных данных, в установленных случаях – аттестация информационной системы персональных данных, ввод системы в эксплуатацию. При необходимости – дальнейшее сопровождение (поддержка) СЗПДн.

Предпроектный этап

- Определение перечня ПДн, обрабатываемых в ИСПДн
- Определение конфигурации и топологии ИСПДн
- Определение технических средств, предполагаемых к использованию в ИСПДн
- Определение режимов обработки ПДн в ИСПДн и других характеристик системы
- Составление частной модели угроз ПДн и классификация ИСПДн
- Разработка ЧТЗ на систему защиты персональных данных (СЗПДн)



Этап проектирования и развертывания

- Разработка технического проекта СЗПДн
- Разработка пакета организационно-распорядительных документов
- Разработка и реализация разрешительной системы доступа пользователей к обрабатываемым ПДн
- Разработка рабочей документации на СЗПДн
- Развертывание системы защиты ПДн (монтаж, настройка, пуско-наладка)



Этап ввода в действие

- Опытная эксплуатация СЗПДн в комплексе с техническими и программными средствами ИСПДн
- Доработка системы защиты ПДн по результатам опытной эксплуатации
- Приемо-сдаточные испытания
- Аттестация ИСПДн по требованиям безопасности информации (в установленных случаях)

Чем определяется стоимость реализации новых требований по защите персональных данных?

Выполнение требований по защите персональных данных является мероприятием, связанным с финансовыми затратами. Стоимость работ определяется классом защищаемой системы, ее характеристиками и особенностями, а так же объемом обрабатываемых персональных данных, наличием у заказчика средств защиты информации и налаженных процессов обеспечения информационной безопасности, составом аппаратных и программных средств ИТ-инфраструктуры, параметрами помещений.

Почему выбор компании «ИНФОРИОН» в качестве интегратора по вопросам защиты персональных данных – разумное и рациональное решение?

Имея значительный опыт в области построения систем защиты персональных данных, специалисты «ИНФОРИОН»:

- Максимально учтут особенности построения действующих систем обеспечения информационной безопасности
- Помогут подобрать Вам оптимальное решение для реализации системы защиты персональных данных
- Гарантируют получение аттестата соответствия требованиям по безопасности информации (в случаях, когда его наличие необходимо)
- Минимизируют Ваши финансовые затраты

Вы получите надежную и эффективную систему защиты персональных данных.

На другие, более частные и профильные вопросы о выполнении требований законодательства в области защиты персональных данных готовы ответить наши эксперты. Мы знаем множество нюансов и «подводных камней», поэтому готовы помочь создать систему защиты с минимальными затратами.

Основная цель компании «ИНФОРИОН» – профессиональное предоставление услуг в области обеспечения защиты информации корпоративным заказчикам.

Наши сотрудники – специалисты с большим практическим опытом решения задач обеспечения информационной безопасности.

Принципы нашей работы: высокое качество, конфиденциальность, индивидуальный подход к потребностям заказчика.

«ИНФОРИОН» является партнером многих отечественных и зарубежных ИТ-компаний. Тесное взаимодействие с ведущими вендорами средств защиты информации, вычислительной техники, телекоммуникационного оборудования и программного обеспечения позволяет эффективно решать любые задачи – от типовых до сложных, достигая при этом поставленных целей в разумные сроки и по приемлемой стоимости.

Мы готовы к сотрудничеству любого уровня и рады предложить свои услуги самому широкому спектру клиентов!



Контактная информация:
107023, Россия, Москва
ул. Семеновская Б., 45
Тел.: +7 (495) 730-74-88
Факс: +7 (495) 580-51-15
info@inforion.ru
www.inforion.ru