Pointlane

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. О ЗАКОНЕ

Федеральный закон N 152-ФЗ “О персональных данных” был принят 27 июля 2006 года.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПД) – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

ОПЕРАТОР - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

2. КЛАССИФИКАЦИЯ ПД

В зависимости от состава персональных данных (например, фамилия, имя, отчество, год, месяц, дата и место рождения, адрес и т.п.) определяется категория, к которой они относятся:

КАТЕГОРИЯ 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

КАТЕГОРИЯ 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

КАТЕГОРИЯ 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

КАТЕГОРИЯ 4 - обезличенные и (или) общедоступные персональные данные.

3. КОНТРОЛЬ

Контроль за выполнением законодательства возложен на следующие органы:

1. Роскомнадзор (федеральная служба по надзору в сфере связи и массовых коммуникаций) – осуществляет контроль и надзор за соответствием обработки ПД требованиям законодательства.
2. ФСТЭК России (федеральная служба по техническому и экспортному контролю) – устанавливает методы и способы защиты информации в информационных системах в пределах своих полномочий.
3. ФСБ РФ (Федеральная служба безопасности РФ) - устанавливает методы и способы защиты информации в информационных системах в пределах своих полномочий (регулирует сферу использования криптографических средств защиты информации).

4. СРОКИ

До **01 января 2010 года** компании (операторы), обрабатывающие персональные данные в информационных системах, обязаны обеспечить:

А. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

Б. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

В. Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование.

Г. Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Д. Постоянный контроль за обеспечением уровня защищенности персональных данных.

5. ОТВЕТСТВЕННОСТЬ

Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

НПА	Статья	Название статьи	Максимальная мера наказания
УК РФ	137	Нарушение неприкосновенности частной жизни	Штраф до 300000 рублей, арест на 4 месяца, исправительные работы до 1 года
	171	Незаконное предпринимательство	Штраф до 300000 рублей, арест до 6 месяца, исправительные работы до 1 года, лишение права занимать должность на срок до 5-ти лет
КоАП РФ	13.12	Нарушение правил защиты информации	Штраф до 20000 рублей, конфискация средств, приостановление деятельности
	13.13	Незаконная деятельность в области защиты информации	Штраф до 20000 рублей, конфискация
	13.14	Разглашение информации с ограниченным доступом	Штраф до 5000 рублей
	19.5	Невыполнение в срок законного предписания	Штраф до 500000 рублей
	19.7	Непредставление сведений (информации)	Штраф до 5000 рублей
	19.20	Осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии)	Штраф до 20000 рублей

6. МЕРОПРИЯТИЯ

ОРГАНИЗАЦИОННЫЕ МЕРЫ по защите персональных данных включают в себя:

А. Разработка организационно – распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных.

Б. Проведение мероприятий по защите ПД.

Меры организационного характера осуществляются на предприятии независимо от того:

- нужно подавать уведомление в Россвязькомнадзор или нет,
- обработка ПД осуществляется с использованием средств автоматизации или без использования таких средств.

В каждой организации перечень мероприятий и документов может варьироваться в зависимости от специфики обработки ПД, организационной структуры и других особенностей конкретного предприятия.

Реализация организационных мер защиты информации осуществляется с учетом категорий персональных данных – чем выше категория, тем выше требования защиты.

ТЕХНИЧЕСКИЕ МЕРЫ защиты информации предполагают использование программно - аппаратных средств защиты информации.

При обработке ПД с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется исходя из класса системы.

В отличие от организационных мер, техническая защита информации является сложным и трудоемким делом, при выполнении которого требуется соблюдать определенные условия, например, наличие соответствующих лицензий, обследование информационных систем в соответствии с методическими рекомендациями ФСТЭК и т.д.

7. ОСНОВНЫЕ ЭТАПЫ

Для приведения информационных систем персональных данных в соответствие требованиями законодательства необходимо:

1. Провести инвентаризацию ПД:
    - А. Сформировать перечень всех ПД, обрабатываемых в компании.
    - Б. Зафиксировать предельные сроки обработки ПД.
    - В. Составить ограниченный список лиц, допущенных к обработке ПД.
2. Получить согласие субъектов (в том числе клиентов компании) на обработку ПД.
3. Привести систему обработки ПД в соответствие требованиям законодательства, а именно:
    - А. Провести классификацию систем обработки ПД.
    - Б. Построить модель угроз системе обработки ПД.
    - В. Составить и направить Уведомление об обработке ПД.
    - Г. Принять необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПД, а также от иных неправомерных действий.
    - Д. Получить лицензию на осуществление деятельности по технической защите конфиденциальной информации (это зависит от результатов классификации системы обработки ПД, в частности, от количества субъектов ПД и типа ПД).
    - Е. Провести сертификацию (аттестацию) системы обработки ПД по требованиям безопасности информации (это зависит от результатов классификации системы обработки ПД, в частности, от количества субъектов ПД и типа ПД).
4. Организовать эксплуатацию системы обработки ПД, в том числе контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

8. РЕЗУЛЬТАТ

После внедрения системы по защите персональных данных оператор получает:

- Возможность продолжать свою деятельность, не опасаясь претензий со стороны клиентов и собственных сотрудников;
- Возможность работы с персональными данными не только внутри компании, но и при передаче их сторонним организациям;
- Защиту от претензий со стороны регулирующих органов;
- Защиту от непредвиденной и принудительной остановки бизнеса;
- Защиту от недобросовестных конкурентов;
- Информационную систему соответствующую требованиям законодательства.

9. УСЛУГИ

Компания “Pointlane” оказывает полный цикл услуг по защите персональных данных, а так же по вопросам прохождения аттестации на работу с персональными данными:

- Консультации по вопросам разъяснения требований законодательства и определения их действия применительно к Вашей организации;
- Подготовка заявки на регистрацию Вашей организации как оператора персональных данных;
- Инвентаризация персональных данных;
- Построение модели угроз;
- Определение класса ИСПДн (информационных систем персональных данных) и выработка мер по его понижению, тем самым снизив затраты на средства защиты, не уменьшая степени защищенности персональных данных;
- Внедрение средств защиты персональных данных;
- Подготовка ИСПДн к аттестации;
- Подготовка Вашей организации к получению лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации;
- Составление ответов на обращения граждан в рамках законодательства по ПД.

О КОМПАНИИ

«Pointlane» – российская консалтинговая компания, предоставляющая услуги в области информационной безопасности для бизнеса.

Направления деятельности «Pointlane»:

- Аудит информационной безопасности;
- Разработка и внедрение процессов управления информационной безопасностью;
- Внедрение систем и средств защиты информации;
- Управление непрерывностью бизнеса;
- Защита персональных данных.

Мы обеспечиваем:

- Индивидуальный и комплексный подход в решении задач конкретного клиента;
- Максимальную эффективность при минимизации затрат клиента;
- Информационную и техническую поддержку клиента.

Наша работа направлена на укрепление конкурентоспособности наших клиентов и их подготовке к будущим условиям рынка и конкуренции.

КОНТАКТЫ

Консалтинговая компания «Pointlane» (ООО «Пойнтлэйн»)
109012, г. Москва, ул. Ильинка, д. 4, офис № 407
Тел.: (495) 233-65-08
E-mail: consult@pointlane.ru
WEB: www.pointlane.ru