Ответственность за несоблюдение законодательства о защите конфиденциальной информации

Докладчик:
к.м.н., доцент
Печерей Иван Олегович

Роскомнадзор – регулятор в сфере защиты персональных данных

ПРЕДМЕТ ГОСУДАРСТВЕННОГО КОНТРОЛЯ (НАДЗОРА)

- Документы, характер информации в которых предполагает или допускает включение в них ПДн
- Информационные системы персональных данных (ИСПДн)
- Деятельность по обработке ПДн

ОФИЦИАЛЬНЫЙ САЙТ РОСКОМНАДЗОРА

- https://rkn.gov.ru/

Виды проводимых проверок

Плановая проверка

Внеплановая проверка

- **Документарные проверки**. Роскомнадзор запрашивает список документов, копии которых необходимо предоставить в территориальный орган Роскомнадзора
- **Выездные проверки**. В организацию приезжают представители Роскомнадзора и проводят проверку на предмет соответствия требованиям ФЗ-152
- **Мероприятия систематического наблюдения.** Удаленный контроль за выполнением требований законодательства операторами персональных данных

Плановые проверки Роскомнадзора

- Проводятся раз в 3 года (в соотв. с 294-ФЗ)
- Проводятся в отношении Операторов:
  - включенных в Реестр операторов;
  - не включенных в Реестр операторов, но осуществляющих обработку ПДн.
- О плановых проверках Роскомнадзор предупреждает заранее (не позднее чем за 3 рабочих дня)

Чтобы узнать, стоит ли ожидать плановой проверки, ***зайдите на сайт*** *Управления Роскомнадзора Вашего региона и* ***найдите План проверок***

Внеплановые проверки Роскомнадзора

- Чаще всего проводятся:
  - на основании выявленных нарушений в действиях Оператора;
  - в случае поступления жалобы на действия Оператора;
  - по результатам мероприятий систематического наблюдения.
- О внеплановых проверках Роскомнадзор предупреждает не менее чем за 24 часа до начала проверки
- В случае причинения вреда жизни и здоровью граждан, Оператор не предупреждается о начале внеплановой проверки

Порядок подготовки к проверке Роскомнадзора

1. Назначить **лиц, ответственных** за организацию обработки и за обеспечение безопасности ПДн
2. Провести внутренний **аудит** в целях анализа процессов обработки ПДн в учреждении
3. Разработать и утвердить необходимую **документацию** по защите ПДн (https://alfa-doc.ru/docs/normatives/)
4. **Ознакомить** всех сотрудников, осуществляющих обработку ПДн и имеющих доступ к обрабатываемым ПДн, под роспись с локальными актами по защите ПДн
5. Подать **уведомление** о намерении осуществлять обработку ПДн / информационное письмо о внесении изменений в Роскомнадзор (https://rkn.gov.ru/personal-data/forms/)

Порядок подготовки к проверке Роскомнадзора

6. Определить **места нахождения баз данных** ПДн граждан РФ
7. Завести и поддерживать в актуальном состоянии **журналы:**
   - Журнал учёта обращений субъектов персональных данных
   - Журнал поэкземплярного учёта средств защиты информации
   - Журнал учета хранилищ (сейфов)
   - Журнал учета материальных (отчуждаемых машинных) носителей ПДн
   - Журнал учета передачи персональных данных
   - Журнал проверок электронных журналов
   - Журнал периодического тестирования средств защиты информации
8. Вести **план внутренних проверок** режима обработки и защиты ПДн
9. Обратить внимание на особенности разработки **согласий** для категорий субъектов, чьи ПДн обрабатываются

РОСКОМНАДЗОР

1. Уведомление об обработке ПД (копия).

2. Скриншоты (картинки программных продуктов, используемых в организации, которые содержат персональные данные, например 1С).

3. Согласие работников на обработку ПД.

4. Согласие пациентов на обработку ПД.

5. Положение о защите ПД.

6. Приказ об уничтожении ПД.

7. Приказ о допуске сотрудников к различным ПД.

8. Описание помещений с указанием рабочих мест и ПК.

9. Приказ об утверждении перечня обрабатываемых ПД.

10. Акт классификации ПД.

11. Приказ о порядке хранения материальных носителей ПД.

Особенности формы письменного согласия

Форма письменного согласия должна содержать:

- ФИО, адрес, паспортные данные субъекта ПДн
- наименование (или ФИО) и адрес оператора
- цель обработки ПДн
- перечень ПДн, на обработку которых дается согласие
- наименование или ФИО и адрес оператора, которому ПДн будут переданы для обработки по поручению
- перечень действий, осуществляемых с ПДн (он не должен включать «распространение»)
- срок, в течение которого действует согласие субъекта ПДн
- подпись субъекта ПДн

** При обработке ПДн несовершеннолетних письменное согласие должны давать их родители (законные представители).*

РОСКОМНАДЗОР

Перечень наиболее часто встречающихся замечаний от Роскомнадзора

- **Неопубликование оператором документа, определяющего Политику в отношении обработки ПДн**

рекомендация: выкладывайте Политику в отношении обработки ПДн на сайт организации на видное место, в т.ч. если используется сбор ПДн через онлайн-формы

- **Отсутствие уведомления об обработке ПДн; Представление в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные или недостоверные сведения; непредставление сведений об изменении информации**

рекомендация: вовремя актуализируйте уведомление об обработке ПДн, отправляйте информационное письмо в Роскомнадзор

- **Отсутствие условий соблюдения конфиденциальности ПДн в договорах с третьими лицами, а также требований к защите обрабатываемых ПДн**

рекомендация: в договоре должно быть прописано: с какой целью передаются ПДн другой компании, какие действия она будет совершать с ними, обязанность компании обеспечивать конфиденциальность и безопасность полученных ПДн. (см. ч.3 ст.6 ФЗ-152)

РОСКОМНАДЗОР

Перечень наиболее часто встречающихся замечаний от Роскомнадзора

- **Отсутствие у оператора места (мест) хранения ПДн (материальных носителей), перечня лиц, осуществляющих обработку ПДн, либо имеющих к ним доступ**

рекомендация: обеспечьте раздельное хранение документов, содержащих ПДн разных физических лиц; обеспечьте контролируемые доступ в помещения, в которых обрабатываются ПДн. В конце рабочего дня документы должны быть убраны в запираемые шкафы, сейфы

- **Невыполнение требований по обучению и ознакомлению сотрудников с порядком обработки, хранения ПДн и ответственностью за нарушение требований законодательства при обработке ПДн**

рекомендация: соберите все необходимые подписи сотрудников, которые работают с ПДн. Они должны ознакомиться под роспись с Политикой, положением, инструкцией ответственного, подписать обязательство о соблюдении конфиденциальности, согласие на обработку их ПДн.

Общие рекомендации от экспертов

- Не выкидывайте ранее разработанные документы по защите ПДн
- Ведите все необходимые журналы и формы документов, необходимые для выполнения законодательства
- Ведите план внутренних проверок режима обработки и защиты ПДн
- Будьте готовы предъявить обезличенные копии документов, содержащих ПДн (копии личных дел, согласий, анкет и др.)
- Будьте готовы начать работать с ПДн при представителях Роскомнадзора
- Подготовьте документы по системе видеонаблюдения, если оно ведется
- Готовьтесь заблаговременно к проверке Роскомнадзора

Реализовывать меры по защите ПДн организация должна в любом случае, вне зависимости от того, подавалось уведомление в Роскомнадзор или нет.

ОТВЕТСТВЕННОСТЬ

Статья 13.11 КоАП РФ .

Нарушение законодательства Российской Федерации в области персональных данных

Статья 137 УК РФ . Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации -

Режим видеонаблюдения

Режим видеонаблюдения

Сведения обо всех лицах, которые участвуют в оказании медицинских услуг, относятся к информации ограниченного доступа (ч.4 ст.92 Федерально закона от 21.11.2011 №323-ФЗ РФ) и подлежат защите (ФЗ-ны от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27.07.2006 №152-ФЗ «О персональных данных»)

Изображения лиц медработников, запись голоса, ФИО на бейджике-это персональные данные. По закону (ст.6 Закона №152-ФЗ), когда инициатор видеосъемки пациент, он должен получить письменное согласие субъектов персональных данных – врача и иных медработников. В согласии должны быть указаны цели видеосъемки, а также последующие действия пациента по обработке данных (ст.9 №152-ФЗ)

БЛАГОДАРЮ ЗА ВНИМАНИЕ