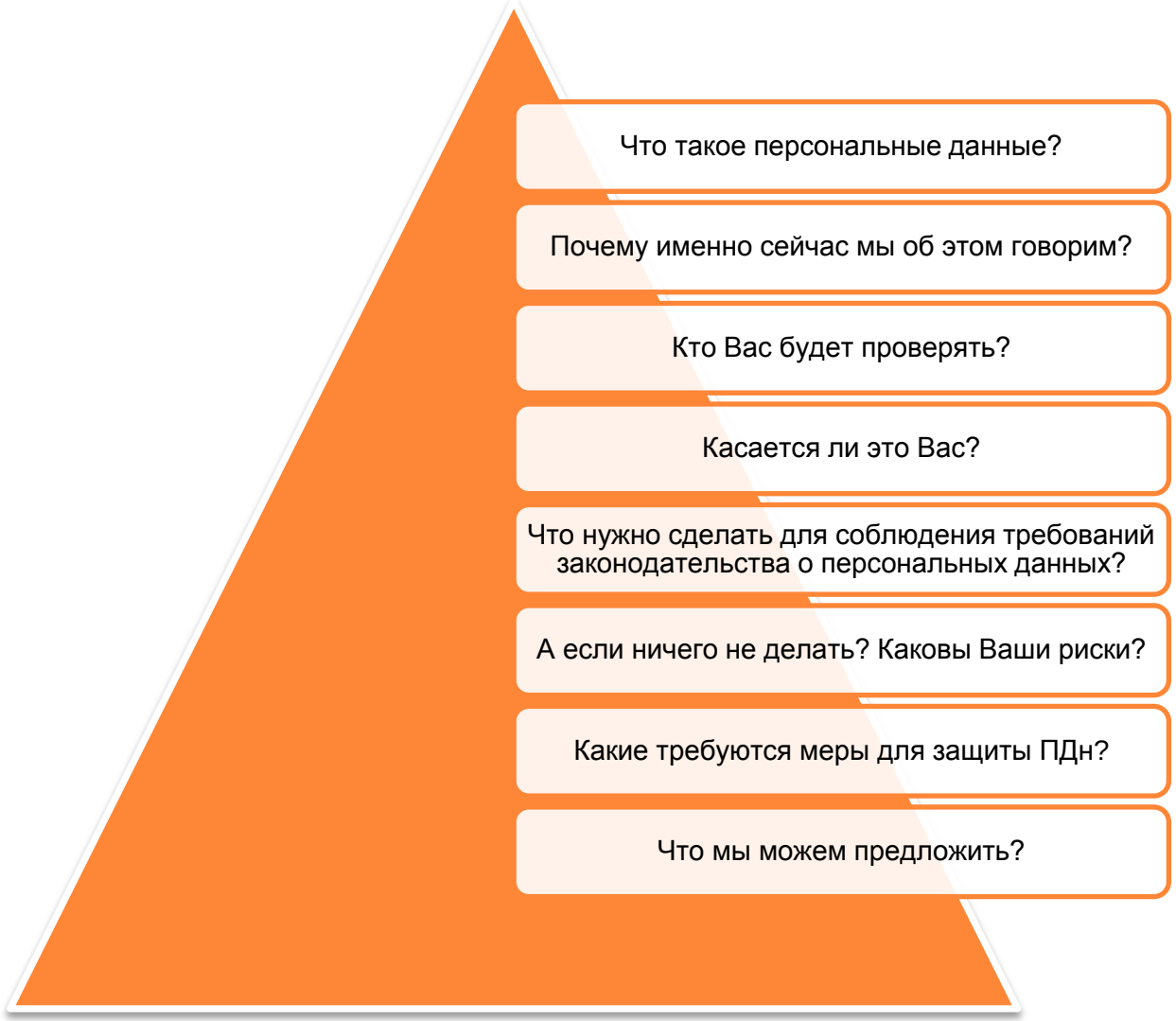
Анастасия Владимирова,
Специалист
по информационной безопасности

Информатика

Содержание


Что такое персональные данные?
Почему именно сейчас мы об этом говорим?
Кто Вас будет проверять?
Касается ли это Вас?
Что нужно сделать для соблюдения требований законодательства о персональных данных?
А если ничего не делать? Каковы Ваши риски?
Какие требуются меры для защиты ПДн?
Что мы можем предложить?

Что такое персональные данные?

- Персональные данные - это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Ими могут быть:

основные: фамилия, имя и отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и др.информация;

Особо охраняются Законом.

специальные: состояние здоровья, национальная принадлежность и другая информация;

биометрические персональные данные: фотография, электронные пропуска, биометрический паспорт.

Почему именно сейчас мы об этом говорим?

- С 1 июля 2011 вступили в силу все положения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В проекте изменений ст. 13.11 КоАП, подготовленном Минэкономразвития:

- **для должностных лиц – 30 000-50 000 руб.**
- **для юридических лиц – 200 000-500 000 руб.**

В проекте изменений ст. 13.11 КоАП, подготовленном Роскомнадзором (обработка без согласия и с неправильно оформленным согласием):

- для юридических лиц – до 2% совокупного дохода за прошедший отчетный год
- У большей части организаций нет ни необходимых знаний, ни ресурсов.
- Исполнение требований Закона откладывать нельзя.

Кто Вас будет проверять?

- **Роскомнадзор**
- • Защита прав субъектов ПДн
- • Контроль и надзор за соблюдением ФЗ-152

- **ФСТЭК**
- • Техническая защиты информации
- • Надзор за соблюдением тех. требований

- **ФСБ**
- • Криптографическая защита информации
- • Контроль использования СКЗИ

Касается ли это Вас?

- Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Ими являетесь – Вы.

Кредитные учреждения, организации ЖКХ, туристические, страховые компании, производственные учреждения, больницы, образовательные учреждения, строительные организации, магазины, операторы связи и многие другие.

Что нужно сделать для соблюдения требований законодательства о персональных данных?

- Определить цели и содержание обработки персональных данных.
- Уведомить Управление Роскомнадзора об обработке персональных данных
- Соблюдать права субъектов персональных данных
- Обеспечить безопасность ПДн
- Соблюдать принципы обработки персональных данных
- Привести документооборот в соответствие с требованиями законодательства

А если ничего не делать? Каковы риски?

- - гражданские иски со стороны клиентов или работников
- - приостановление или прекращение обработки персональных данных в организации (приостановление лицензии)
- - привлечение организаций и ее руководителей к административной, уголовной, гражданской и иным видам ответственности
- - приостановление деятельности или аннулирование лицензий на основной вид деятельности организаций
- - ущерб деловой репутации
- - вероятность недобросовестной конкуренции (приостановление деятельности) организации с подачи конкурентов при имеющихся нарушениях правил защиты персональных данных

Меры защиты ПДн

Меры защиты ПДн подразделяются на:

- **Организационные меры**
- **Технические меры**

ПП 1119

- **Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по ТЗКИ**
- **Контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом)**
- **Возложение на одно из структурных подразделений функций по обеспечению безопасности персональных данных**
- **Расширено определение угроз безопасности персональных данных при их обработке**

Уровни защищенности в соответствии с ПП 1119

Количество ПДн субъектов < 100.000 либо только сотрудники

	Специальные	Биометрические	Иные	Общедоступные
1 тип угроз	1	1	1	2
2 тип угроз	2	2	3	3
3 тип угроз	3	3	4	4

Количество ПДн субъектов > 100.000

	Специальные	Биометрические	Иные	Общедоступные
1 тип угроз	1	1	1	2
2 тип угроз	1	2	2	2
3 тип угроз	2	3	3	4

Что необходимо сделать, чтобы привести информационные системы в соответствие с законом?

- Анализ текущей ситуации в компании, обследование и оценка текущего уровня соответствия ИСПДн требованиям нормативных документов по защите ПДн
- Принятие решения о привлечении сторонних специализированных организаций и использования собственных ресурсов для построения системы защиты ПДн.
- Подготовка задания по созданию требуемой системы защиты.
- Выработка и подготовка рекомендаций по использованию технических средств защиты ПДн.

Как снизить расходы?

Мы считаем, что понятию «оптимизация» более всего соответствует:

- Построение реалистичной модели угроз и адекватная классификация ИСПДн (т.е. предъявление к СЗПДн **только необходимых требований**)

Какой вариант решений по защите персональных данных Вам выбрать?

- Сделать все самим

Кто? Сроки? Квалификация? Опыт?

- Воспользоваться услугами нашей компании

Что мы можем Вам предложить?

- Оценка процессов обработки персональных данных требованиям законодательства
- Помощь в подаче Уведомления об обработке персональных данных или при явных несоответствиях в уведомлении- подготовка проекта письма о внесении изменений
- Разработка организационно-распорядительной документации по обработке и защите персональных данных
- Инвентаризация ИСПДн, оптимизация ИСПДн
- Исследование угроз безопасности персональных данных при их обработке в ИСПДн и проведение классификации ИСПДн
- Разработка технического задания на построение системы защиты персональных данных
- Консультирование по вопросам внедрения разработанных документов
- Годовая поддержка в виде вебинаров

Комплект разрабатываемых документов

- Проектные документы
- Положения
- Планы работ
- Инструкции
- Приказы
- Акты
- Журналы и перечни
- Письменные согласия, обязательства, запросы, уведомления
- Всего более 40 готовых документов

Преимущества документов, разработанных компанией «Информатика»

- Гарантии качества документов
  - Соответствие законодательству, нормативной базе
  - Нешаблонный подход к заказам, разработка дополнительных документов

И самое главное:

- Сами встретим проверку, сами ответим на вопросы, за свой счет устраним недостатки.

пункт договора 2.1.2

Исполнитель обязан своими силами и за свой счет устранить допущенные по вине исполнителя в выполненных работах недостатки

Поддержка

Поддержка будет осуществляться по желанию клиента в форме вебинара. Наш клиент получает:

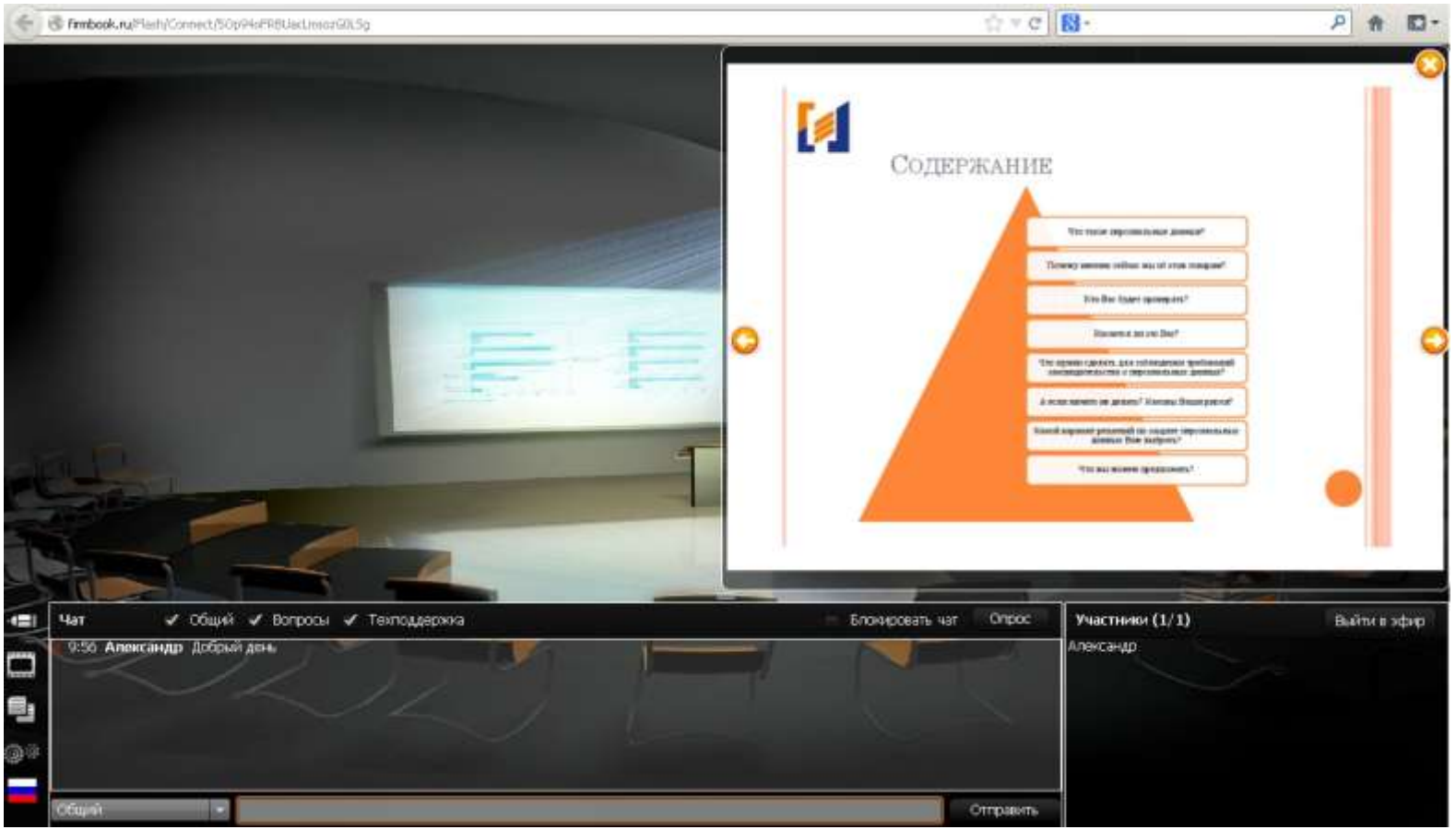
- Экономию сил и времени у сотрудника на отслеживание изменений действующего законодательства;
- Поддержание документов в актуальном состоянии сотрудником клиента с нашей помощью в виде онлайн консультаций;
- Получение подробных консультаций от специалистов по защите информации по возникающим вопросам
- Возможность обсуждения острых вопросов с другими участниками конференции;

Сопровождение

Выездной сервис. Наш клиент получает:

- Поддержание документов в актуальном состоянии нашими силами при изменении организационной структуры организации, при изменении структуры ИСПДн, при изменении действующего законодательства

Как выглядит вебинар



Наиболее часто задаваемые вопросы

Вопрос:

«Мы и так никому ничего не рассказываем, все наши данные защищены!»

«О какой защите персональных данных может идти речь, если люди сами все раскрывают в социальных сетях?»

Ответ:

Мы не обсуждаем справедливость законодательства и его приближенность к реальной жизни. Наша задача – предложить наилучший вариант, как избежать юридических рисков

Наиболее часто задаваемые вопросы

Вопрос:

«Мы все расчеты производим через расчетно-кассовый центр, нам ваши услуги не требуются»

Ответ :

Существует заблуждение относительно того, что переход УК, ТСЖ, ЖСК к сотрудничеству с РКЦ, может освободить данных организаций от соблюдения ими требований законодательства о персональных данных, т.к. РКЦ - специализированное учреждение, созданное для организации расчётов за жилищно-коммунальные услуги между гражданами и организациями, оказывающими такие услуги. В данном случае РКЦ будет являться посредником для осуществления расчетов. В любом случае, такие организации как: УК, ТСЖ, ЖСК будут являться операторами, обрабатывающими персональные данные, т.к. они осуществляют сбор, хранение данных о собственниках жилья, а это и есть обработка. К тому же есть и сотрудники, по которым тоже собираются определенные сведения

Наиболее часто задаваемые вопросы

Вопрос:

«А мы сами уже все разработали, скачали шаблоны документов из Интернета»

Ответ:

…и сами несете в настоящий момент все юридические риски. Вы уверены, что хорошо ориентируетесь в этих документах и сможете ответить на возможные вопросы надзорных органов?

Мы не «разрабатываем документы», мы защищаем вас от проверки.

Наиболее часто задаваемые вопросы

Вопрос:

«А давайте когда к нам проверка придет – мы вас и позовем, или давайте мы к вам обратимся после проверки, что бы вы устранили наши нарушения»

Ответ:

1. Процесс приведения инфраструктуры в соответствие с законодательством занимает около 2 месяцев, а уведомление о внеплановой проверке высылается за 24 часа до начала проверки

2.Мы не гарантируем, что наша загрузка позволит нам мгновенно отработать ваш срочный запрос – а предписание имеет ограниченный срок на выполнение

3.Любое предписание – это минус к вашей репутации, и оно увеличивает шанс повторной проверки

Вопросы?
Спасибо.