«Антивирусный центр»

Информационная Безопасность Офиса

Защита персональных данных

Правовые и организационные аспекты

Сергей Золотухин
Антивирусный центр
www.AntiVirusPro.com
project@antiviruspro.com

О компании Антивирусный Центр

- Компания работает с 1998 года, и является одной из ведущих компаний на российском рынке ИБ
- Дистрибутор продуктов и услуг в сфере ИБ
- Партнеры в регионах России
- Лицензия ФСТЭК
- Поставка решений передовых разработчиков

лаборатория Касперского

TREND MICRO

Microsoft

symantec

eset

Aladdin SECURITY SOLUTIONS

INFOWATCH INFORMATION WATCH TECHNOLOGIES

McAfee

Dr.WEB

Продукты ИБ

Включая но не ограничиваясь:

TREND MICRO

symantec

INFOWATCH
INFORMATION WATCH TECHNOLOGIES

лаборатория Касперского

McAfee

Aladdin
SECURITY SOLUTIONS

eset

Microsoft

Dr.WEB

Правовое поле 152-ФЗ

- Доктрина ИБ РФ
- ФЦП "Электронная Россия (2002-2010 годы)"
- Концепция использования ИТ в деятельности федеральных органов государственной власти до 2010 года.
- 149-ФЗ открытость информации о деятельности государственных органов и органов местного самоуправления
- 152-ФЗ Оператор обязан принимать необходимые меры для защиты персональных данных
- Стратегия развития информационного общества

- **Европейская конвенция о защите прав человека**

Развитие правового поля

2006 г. 152-й ФЗ	Федеральный закон №152 «О персональных данных»
2007 г. 781-е Постановление	Постановление Правительства «Положение об обеспечении безопасности ПДн при их обработке…»
2008 г. «Приказ трех»	Приказ ФСТЭК/ФСБ/Мининформсвязи № 55/86/20 «Порядок проведения классификации информационных систем ПДн»
2008 г. 4 документа ФСТЭК	«Рекомендации...» «Основные мероприятия…» «Методика определения…» «Базовая модель угроз…»
2008 г. 2 документа ФСБ	«Типовые требования…» «Методические рекомендации…»

Сто дней до приказа!

Действующие лица

Правительство	Устанавливает правила игры
Уполномоченные органы	Отслеживают и регулируют
Ассоциации, комитеты, отдельные граждане	«Гонят волну»...
Субъект ПДн	Шлёт запросы в Роскомнадзор…
Оператор ПДн	Вынужден соответствовать
Интегратор	**Единственный Союзник Оператора**

Основные определения

- **Персональные данные** - 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.

- **Другая информация**: сведения о работе, о членах семьи, место жительство, почтовый адрес, телефон, e-mail, местонахождение объектов недвижимости, владение языком и т.д.

Важные положения

ВСЕ!!! государственные и муниципальные органы, юридические и физические лица, осуществляющие обработку персональных данных **а также определяющие цели и содержание обработки персональных данных (**исключения : гостайна, архивное дело, единый реестр ИП, личные и семейные нужды

Обработка персональных данных - действия (операции) с персональными данными, включая **сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных**

- Операторы, которые осуществляют обработку персональных данных обязаны направить уведомление не позднее 1 января 2008 года.
- Информационные системы, создаваемые после вступления в силу закона, должны соответствовать его требованиям.
- Информационные системы, созданные до дня вступления в силу закона, должны быть приведены в соответствие с требованиями не позднее 1 января 2010 года.

Определение класса информационной системы

Класс **типовой** информационной системы	**< 1000** или в пределах одной организации	**> 1000** или обрабатывает отрасль, орган госвласти или муниципальный район	**> 100000** или охватывает субъект РФ и более
категория 4 - обезличенные и (или) общедоступные персональные данные	**К4**	**К4**	**К4**
категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных	**К3**	**К3**	**К2**
категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1	**К3**	**К2**	**К1**
категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни	**К1**	**К1**	**К1**

К1 - нарушение может привести к значительным негативным последствиям
К2 - нарушение может привести к негативным последствиям
К3 - нарушение может привести к незначительным негативным последствиям
К4 - нарушение не приводит к негативным последствиям

Требования к защите **специальной информационной системы** определяются на основе модели угроз безопасности персональных данных в соответствии с методическими документами

Кто и как вас контролирует?

- **Роскомнадзор** - является основным исполнительным и надзорным органом по защите прав физических лиц, чьи персональные данные обрабатываются (проверяет сведения содержащиеся в уведомлении с привлечением ФСТЭК и ФСБ)

- **ФСТЭК** России - осуществляет контроль деятельности по защите информации с использованием технических средств

- **ФСБ** России - курирует вопросы защиты информации (надзор за деятельностью и соблюдение правил) с использованием средств шифрования (криптографии)

Роскомнадзор: примерный список документов

- учредительные документы Оператора
- копия уведомления об обработке персональных данных
- положение о порядке обработки персональных данных
- положение о подразделении, осуществляющем функции по организации защиты персональных данных
- должностные регламенты лиц, имеющих доступ к персональным данным;
  план мероприятий по защите персональных данных
- план внутренних проверок состояния защиты персональных данных
- приказ о назначении ответственных лиц по работе с персональными данными
- типовые формы документов, предполагающие или допускающие содержание персональных данных
- журналы, реестры, книги, содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях
- договоры с субъектами персональных данных, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных
- выписки из ЕГРЮЛ, содержащие актуальные данные на момент проведения мероприятия по контролю (надзору)
- приказы об утверждении мест хранения материальных носителей персональных данных
- письменное согласие субъектов персональных данных на обработку их персональных данных (типовая форма)
- распечатки электронных шаблонов полей, содержащие персональные данные
- справки о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка персональных данных
- заключения экспертизы ФСБ России, ФСТЭК России об оценке соответствия средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке (проверяется только наличие данных документов)
- приказ о создании комиссии и акты проведения классификации информационных систем персональных данных (проверяется только наличие данных документов)
- журналы (книги) учета обращений граждан (субъектов персональных данных);
  акт об уничтожении персональных данных субъекта(ов) персональных данных (в случае достижения цели обработки)
- иные документы, отражающие исполнение Оператором требований законодательства Российской Федерации в области персональных данных

Общим числом около 30 документов…

Что будет, если …

- **Статья 24 152-ФЗ:**

  «Лица, виновные в нарушении требований настоящего федерального закона несут

  гражданскую

  уголовную

  административную

  дисциплинарную

  и иную

  предусмотренную законодательством Российской Федерации ответственность»

Что будет, подробнее …

- наложение административных штрафов от 500руб. до 500000руб. или в размере дохода за период до 3 лет
- административное приостановление деятельности на срок до 90 суток
- конфискацию несертифицированных средств защиты
- обязательные работы на срок до 180 часов
- исправительные работы на срок до одного года
- лишение свободы на срок до 5 лет
- лишение права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет

Административные санкции – сразу. Уголовные – через суд

Всего 4 шага…

- **Уведомить** уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных
- **Разработать** комплект документов, регламентирующих обработку персональных данных в организации (положение по обработке персональных данных, регламенты, положения по защите персональных данных)
- **Создать** систему защиты персональных данных, в т.ч. выполнить требования по инженерно-технической защите помещений
- **Аттестовать** или декларировать соответствие информационных систем персональных данных требованиям безопасности информации

Стратегии поведения

- «Сами с усами…»
- «Закон что дышло…»
- «Куплю индульгенцию…»
- «Авось пронесет…»

«Путь длиною в тысячу миль начинается с первого шага…»

Зоны рисков

- CSO (информационная безопасность)
- CIO (информационные технологии)
- CFO (финансы)
- CEO (операционная деятельность)
- Owner (репутация)

Разделите зоны риска!

Выводы

- Соблюдайте закон
- Сотрудничайте с регуляторами
- Выработайте стратегию
- Обрабатывайте риски
- Привлекайте экспертов

Спасибо за внимание!