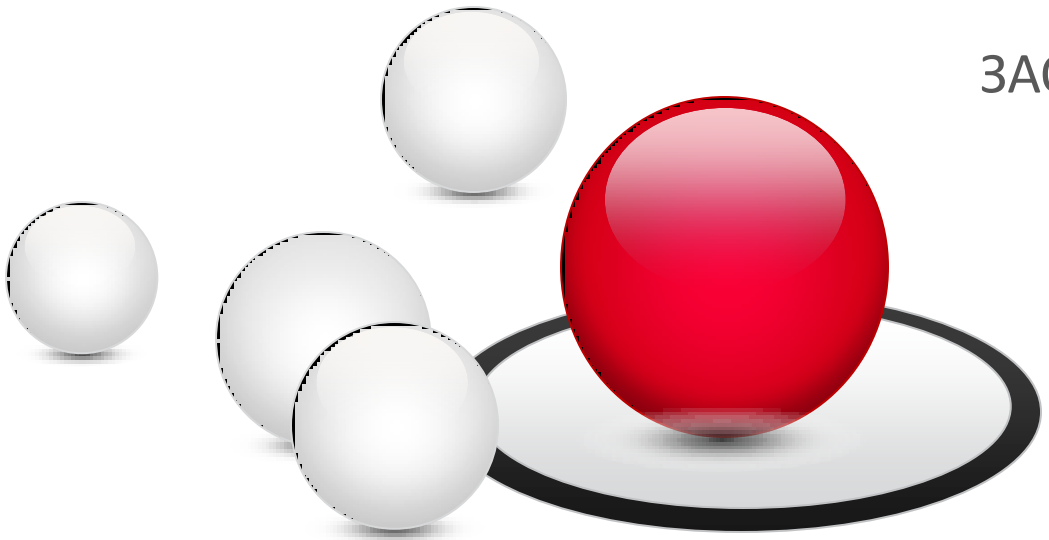
Эшелон
комплексная безопасность

infosecurity RUSSIA

Защита персональных данных

Егоров Михаил,
Директор департамента проектов
ЗАО «НПО «Эшелон»



Федеральное законодательство

152-ФЗ
от 27.07.2006

О персональных данных

149-ФЗ
от 27.07.2006

Об информации, информационных технологиях и о защите информации

363-ФЗ
от 27.12.2009

О внесении изменений в статьи 19 и 25 Федерального закона "О персональных данных"

Эшелон
комплексная безопасность

363-ФЗ

- Исключено требование по **обязательному** использованию шифровальных (криптографических) средств
- ИСПДн должны быть приведены в соответствие не позднее **1 января 2011 года**

Постановления правительства

ПП 781
от 17.11.2007

Положение об обеспечении безопасности ПДн при их обработке в ИСПДн

ПП 687
от 27.07.2006

Положение об особенностях обработки ПДн без использования средств автоматизации

ПП 512
от 06.07.2008

Требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн

ПП 330
от 15.05.2010

Положение об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, отнесенных к охраняемой в соответствии с законодательством РФ информации ограниченного доступа, не содержащей сведения, составляющие гостайну...

Эшелон
комплексная безопасность

ПП 330 (ДСП)

- Распространяется на продукцию, используемую в целях защиты информации конфиденциального характера, являющейся государственным информационным ресурсом и (или) **персональными данными**
- Оценка соответствия продукции осуществляется в формах **обязательной сертификации**
- Организация и проведение обязательной сертификации продукции осуществляются в порядке, определяемом ФСТЭК России (**система аттестация является составной частью системы сертификации**)

Эшелон
комплексная безопасность

ФСТЭК России

Базовая модель
14.02.2008

Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн

Методика
14.02.2008

Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн

Приказ 58
от 05.02.2010

Об утверждении Положения о методах и способах защиты информации в ИСПДн

~~Основные мероприятия 14.02.2008~~

~~Рекомендации 14.02.2008~~

Эшелон
комплексная безопасность

Положение о методах и способах защиты информации в ИСПДн

- Использование средств защиты информации, прошедших в установленном порядке **процедуру оценки соответствия**
- Для ИСПДн К1 программное обеспечение СЗИ должно соответствовать **4 уровню контроля отсутствия НДВ**

Эшелон
комплексная безопасность

Положение о методах и способах защиты информации в ИСПДн

Класс ИСПДн	Класс АС	Класс МЭ ССОП	Класс МЭ	НДВ
К1	3А 2А 1Г	3	5	4
К2	3Б 2Б 1Д	4	5	-
К3	3Б 2Б 1Д	5	5	-
К4	-	-	-	-

Эшелон
комплексная безопасность

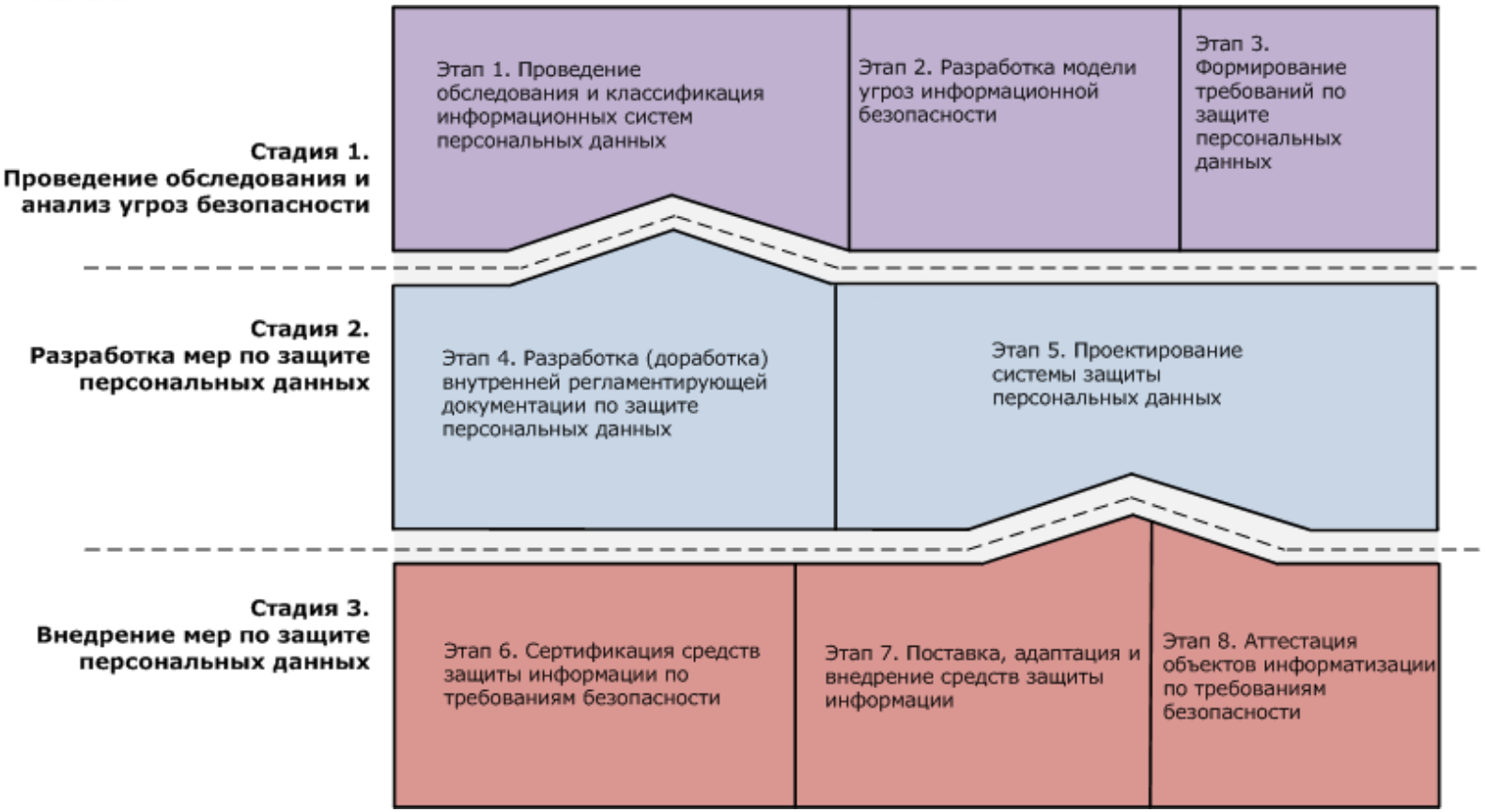
Выводы

- Необходимо привести ИСПДн в соответствие до 01.01.2011
- Применение **сертифицированных** по требованиям безопасности информации средств защиты (на ТУ, МЭ, ЗБ)
  - Для К1 соответствие ПО СЗИ **4 уровню контроля отсутствия НДВ** (предоставление исходных текстов)
- Проведение **аттестационных испытаний** ИСПДн (вне зависимости от класса)

Стадии и этапы проекта

- 3 Стадии:
  - Стадия 1. Проведение обследования и анализ угроз безопасности
  - Стадия 2. Разработка мер по защите персональных данных
  - Стадия 3. Внедрение разработанных мер
- 8 Этапов

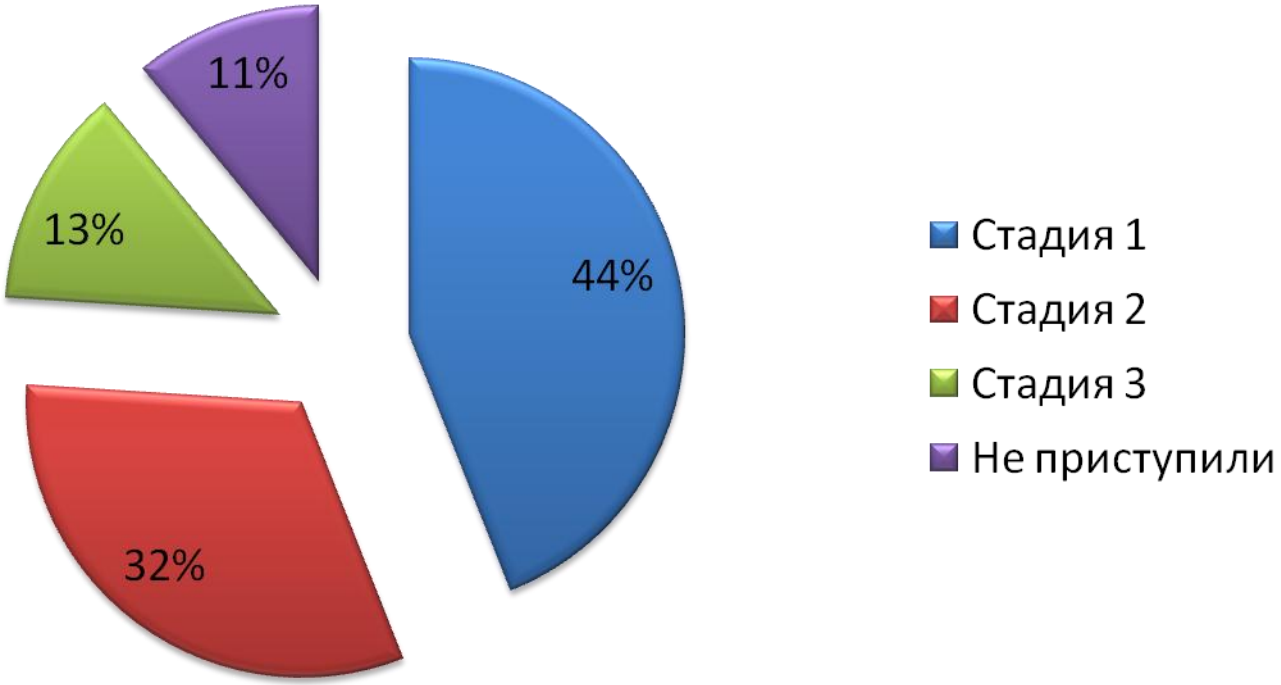
Стадии и этапы проекта



Эшелон
комплексная безопасность

На какой стадии Вы находитесь?

- Опрос на ISPDN.ru (**188** респондентов)



Эшелон
комплексная безопасность

Стоимость внедрения

- 2 – 3 млн. рублей для средней ИСПДн
- 3 – 7 млн. рублей для крупной ИСПДн

Эшелон
комплексная безопасность

Защита ПДн в Банках

Эшелон
комплексная безопасность

Отраслевые стандарты

- Комплект документов в области стандартизации Банка России – 4 документа:
  - СТО БР ИББС 1.0 – 2010. Общие положения.
  - СТО БР ИББС 1.2 – 2010. Методика оценки соответствия.
  - РС БР ИББС 2.3 – 2010. Требования по обеспечению безопасности ПДн в ИСПДн.
  - РС БР ИББС 2.4 – 2010. Отраслевая частная модель угроз.
- Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях БС РФ.

Программа действий

- Присоединение к стандартам Банка России. Выпуск приказа.
- Разработка плана мероприятий.
- Реализация плана. Выпуск (доработка) необходимых документов.
- Проведение оценки соответствия (аудит/самооценка).

Эшелон
комплексная безопасность

Оценка соответствия

- СТО БР ИББС 1.2-2010. Содержит методику проведения оценки соответствия.
- Оценка соответствия проводится внешней организацией либо в форме самооценки.
- По результатам выпускается подтверждение соответствия в пяти экземплярах и направляется регулирующим органам (ЦБ, ФСТЭК, ФСБ, Роскомнадзор) до **31.12.2010**.

Самое интересное

- При введении Стандартов Банка России в организации БС РФ приказом требования по получению **лицензий** на деятельность по технической защите конфиденциальной информации и требования **аттестации** ИСПДн **не являются обязательными**.
- Угрозы утечки персональных данных по техническим каналам являются для организаций БС РФ **неактуальными**.

Эшелон
комплексная безопасность

Самое интересное

- В организации БС РФ должен быть **определен** и **документально зафиксирован** подход к отнесению АБС к ИСПДн.
  - АБС, реализующие банковские **платежные технологические процессы**, не относятся к ИСПДн.
- Все ИСПДн организаций БС РФ относятся к **специальным**.
- ИСПДн организации БС РФ классифицируются на основе **категорий** обрабатываемых в ИСПДн персональных данных (ИСПДн-Б, ИСПДн-С, ИСПДн-И, ИСПДн-Д).

Самое интересное

- Требования по обеспечению безопасности ПДн при их обработке в ИСПДн определяются для каждого класса ИСПДн на основе:
  - Требований 7-го и 8-го разделов СТО БР ИББС 1.0.
  - Требований к соответствующему классу ИСПДн (РС БР ИББС2.3).
  - Оценки рисков нарушения безопасности персональных данных.
- Необходимо защищать **общедоступные** и **обезличенные** персональные данные.

Классификация информации

- Банковская тайна
- Коммерческая тайна
- Служебная тайна
- Персональные данные

Эшелон
комплексная безопасность

Банковская тайна

- **Статья 857** ГК РФ
- **Статья 26** 395-1 ФЗ «О банках и банковской деятельности»
- 214-ФЗ «О кредитных историях»

Банковская тайна

- Гражданская ответственность:
  - Банковская тайна (статья 857 ГК РФ).
- Административная ответственность:
  - Разглашение информации с ограниченным доступом (статья 13.14 КоАП РФ).
- Уголовная ответственность:
  - Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (статья 183 УК РФ).

Границы банковской тайны

- *«…Банк гарантирует тайну банковского счета и банковского вклада, операций по счету **и сведений о клиенте**»*

  статья 857 ГК РФ

- *«… Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, **а также об иных сведениях**, устанавливаемых кредитной организацией, если это не противоречит федеральному закону»*

  Статья 26 ФЗ «О банках и банковской деятельности»

Границы банковской тайны

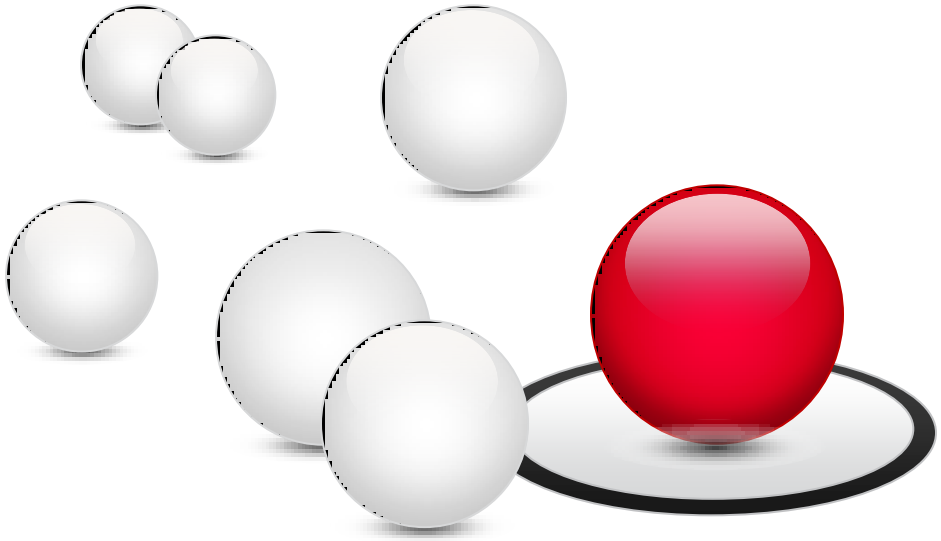
- Сведения о клиенте при условии, что такие сведения получены банком в ходе его профессиональной деятельности

Границы банковской тайны

- Сведения о состоянии счетов и операциях по счетам, сведения о клиентах
- Персональная информация о клиенте, ставшей известной Банку в процессе ведения досье клиента:
  - Паспортные данные
  - Сведения о месте проживания
  - Сведения о месте работы
  - Сведения о движимом и недвижимом имуществе
  - Сведения об обязательствах перед третьими лицами

Границы банковской тайны

- Сведения о вкладах
- Сведения об операциях без открытия счета (денежные переводы)
- Сведения об операциях по банковским картам



Михаил Егоров

Директор департамента проектов

E-mail: m.egorov@npo-echelon.ru

Тел.: +7(495) 645-38-09

Эшелон
комплексная безопасность