IT-COMPANY

Типовая пошаговая структура реализации комплексного проекта защиты ПДн с учетом последних изменений и опыта LETA в 2009–2010 гг.

Малявкин Александр,
Отдел внешнего аудита и консалтинга

№152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

26 января 2007 года вступил в силу
Федеральный закон № 152-ФЗ «О персональных данных»

- Закон обязывает операторов персональных данных привести свои информационные системы персональных данных в соответствие с требованиями регулирующих органов.
- Ответственными за контроль соблюдения требования Закона определены Роскомнадзор, ФСТЭК России и ФСБ России.

Законом определено:

- **Информационные системы, обрабатывающие персональные данные, должны быть приведены в соответствие с требованиями Закона и регулирующих органов до 01 января 2011 года* (Согласно принятому законопроекту «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных»).**
- **Невыполнение требований ФЗ «О персональных данных» и подзаконных актов может повлечь привлечение к ответственности должностных лиц организации к уголовной, гражданской, административной и дисциплинарной ответственности.**

ОПЕРАТОРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

«Работодатели»

Оператор **«потребляет» услуги** физических лиц (работников, агентов и т.п.) на основе договора (трудовой договор, агентский договор и т.п.)

Практически любое юридическое лицо

«Бизнес»

Оператор **оказывает услуги** (или продает товары) физическим лицам на основе договора (договор об оказании услуг, договор купли-продажи)

Кредитно-финансовые организации; страховщики; учреждения здравоохранения; образовательные учреждения; учреждения культуры и спорта; операторы: связи, транспорта, туристических, жилищно-коммунальных услуг и т.п.

«Прочие»

Оператор обрабатывает ПДн физических лиц, с которыми его **не связывают в явном виде договорные отношения**

Государственные учреждения, политические объединения, интернет-магазины, компании директ-маркетинга, рекрутерские компании и т.п.

УСЛУГИ LETA ПО ЗАЩИТЕ ПДН

В рамках направления **«Защита персональных данных»** LETA IT-company оказывает следующие услуги, которые группируются в три блока:

Стандартные услуги

- ***Обследование процессов обработки персональных данных.***
- ***Проектирование и реализация системы защиты персональных данных.***

Дополнительные услуги

- ***Сопровождение и поддержка построенной системы защиты ПДн.***

(«Дополнительные услуги LETA…» Царев Евгений)

- ***Аудит построенных систем защиты персональных данных***

(«Дополнительные услуги LETA…» Царев Евгений).

- ***Подготовка к получению лицензий ФСТЭК России и ФСБ России.***

Перспективные услуги

- ***Обучение специалистов Заказчика (Коучинг)***

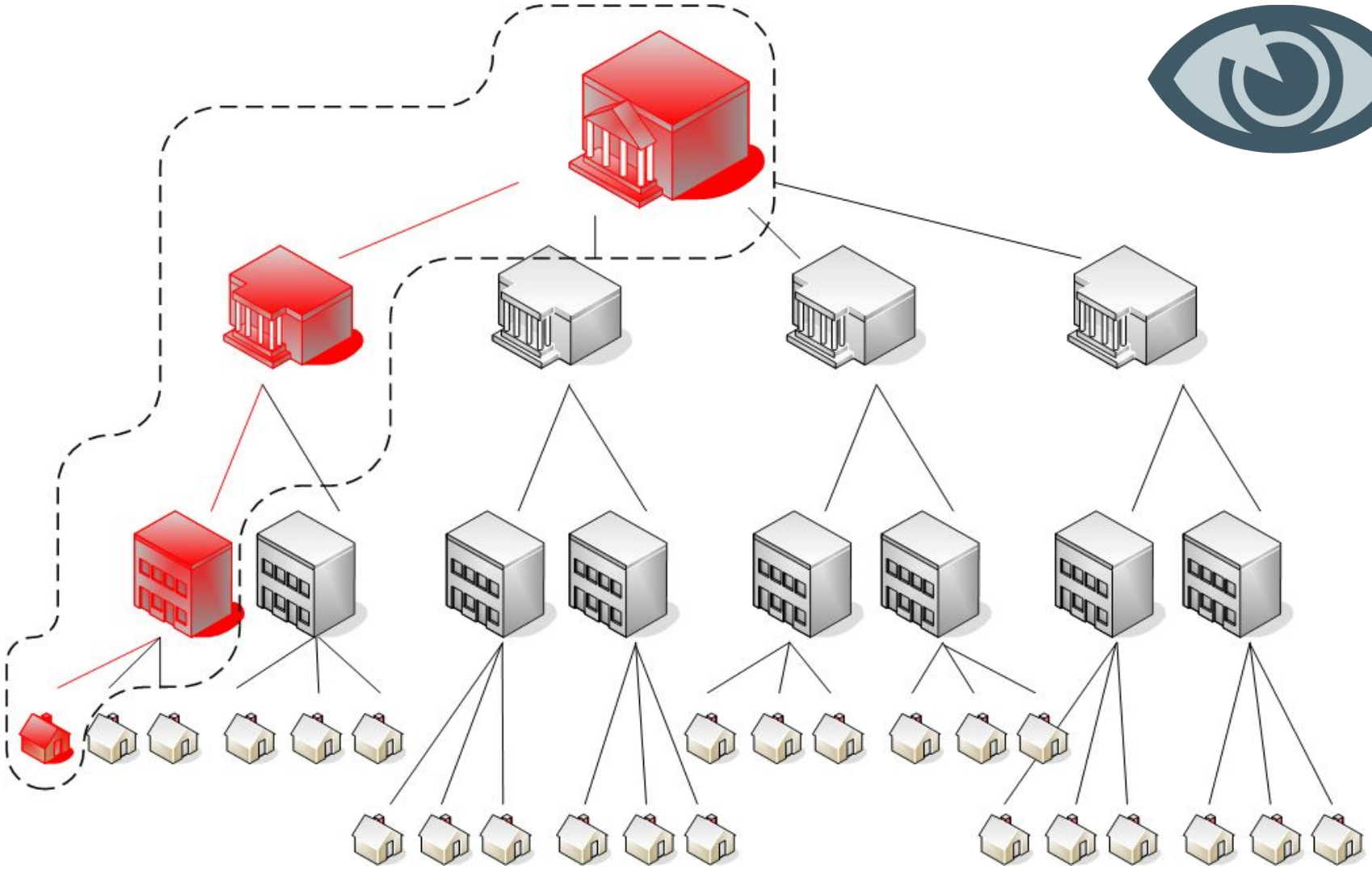
(«Практика привлечения интегратора…» Санин Александр).

КОНЦЕПЦИЯ ОКАЗАНИЯ СТАНДАРТНОЙ УСЛУГИ ПО ЗАЩИТЕ ПДН

Работы по защите персональных **в рамках стандартной услуги** выполняются в **четыре последовательные стадии**

0 **Выделение типовых объектов**	Выделение из территориально обособленных подразделений Компании типовой цепочки объектов, схожих по функционалу, организации процессов, способам взаимодействия и построения ИС, для последующего обследования.
1 **Обследование**	Оценка текущей обстановки, заключение о степени выполнения требований, рекомендации по приведению в соответствие требованиям
2 **Проектирование**	Проектирование организационной и технической составляющей системы защиты персональных данных (документы и средства защиты)
3 **Реализация**	Внедрение СЗИ и выстраивание процессов обработки/защиты ПДн на основе разработанной документации

НУЛЕВАЯ СТАДИЯ
ВЫДЕЛЕНИЕ ТИПОВЫХ ОБЪЕКТОВ



ПЕРВАЯ СТАДИЯ
ОБСЛЕДОВАНИЕ ПРОЦЕССОВ ОБРАБОТКИ ПДН

- Выявляются **все внутренние и внешние процессы** (взаимодействие с третьими сторонами) обработки ПДн, осуществляемые как с использованием СрАвт, так и без использования таковых.

Выполняемые работы в рамках обследования

- Выявляются **все подразделения и отдельные лица Компании**, участвующие в обработке ПДн.
- Выявляется **состав и объем обрабатываемых ПДн**, а также определяются цели и правовые основания обработки этих сведений.
- Выявляются **все категории субъектов ПДн**, чьи данные обрабатываются в Компании.
- Выявляются и **документируются информационные системы**, в которых производится обработка ПДн, как и с использованием СрАвт, так и без использования таковых.
- Разрабатываются **модели угроз безопасности персональных данных** при их обработке в информационных системах персональных данных.
- Проводится **классификация информационных систем персональных данных**.
- Разрабатываются **рекомендации и мероприятия по приведению процессов обработки** персональных данных Компании в соответствие требованиям законодательства РФ.

ПЕРВАЯ СТАДИЯ
ОБСЛЕДОВАНИЕ ПРОЦЕССОВ ОБРАБОТКИ ПДН

Результаты обследования

- **Проведена оценка текущего состояния** процессов обработки ПДн, а также информационных систем (в т.ч. уровень их защищенности), задействованных в обработке ПДн.
- **Составлено заключение о степени выполнения требований** законодательства РФ, а также руководящих документов ФСТЭК России и ФСБ России, в области обработки и защиты персональных данных в Компании.
- **Определены дальнейшие организационные и технические мероприятия** по приведению процессов обработки и информационных систем персональных данных Компании в соответствие требованиям законодательства РФ, а также руководящих документов ФСТЭК России и ФСБ России, в области обработки и защиты персональных данных.

ПЕРВАЯ СТАДИЯ
ОБСЛЕДОВАНИЕ ПРОЦЕССОВ ОБРАБОТКИ ПДН

Материальные результаты обследования

ОТЧЕТ ПО РЕЗУЛЬТАТАМ ПРОВЕДЕНИЯ ОБСЛЕДОВАНИЯ ПРОЦЕССОВ ОБРАБОТКИ ПДН В КОМПАНИИ

Данный отчет содержит детальное описание приведенных выше результатов обследования (оценка обстановки, заключение о степени выполнения требований и рекомендации по приведению в соответствие требованиям). Кроме того, в отчет входит первичный пакет документов, необходимых для выполнения основных требований законодательства РФ, а также руководящих документов ФСТЭК России и ФСБ России, в области обработки и защиты ПДн:

- **Перечень персональных данных, обрабатываемых в Компании.**
- **Перечень сотрудников и подразделений, допущенных к обработке персональных данных, обрабатываемых в Компании.**
- **Перечень и описания информационных систем персональных данных Компании.**
- **Частные модели угроз безопасности персональных данных в Компании.**
- **Акты классификации информационных систем персональных данных.**
- **Требования по обеспечению безопасности ПДн при их обработке в ИСПДн.**

ВТОРАЯ СТАДИЯ
ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПДН

Выполняемые работы в рамках проектирования

- Разрабатывается **Техническое задание** на создание системы защиты персональных данных.
- Разрабатывается **Эскизный проект** на создание системы защиты персональных данных.
- Совместно с Заказчиком производится **выбор окончательного проектного решения**.
- Разрабатывается **Технический проект** на создание системы защиты персональных данных
- Разрабатывается **Пакет проектов организационно-распорядительной документации** (в т.ч. доработка существующих документов), регламентирующей порядок обработки и защиты персональных данных в Компании.

ВТОРАЯ СТАДИЯ
ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПДН

Результаты проектирования

- Утвержденное **Техническое задание** на создание СЗПДн (для каждой ИСПДн).
- Утвержденный **Технический проект** на создание СЗПДн.
- Адаптированный **Пакет организационно-распорядительной документации**, удовлетворяющий всем требованиям, предъявляемым к документационному обеспечению операторов ПДн.

Все документы разрабатываются в соответствии с требованиями:

- Пакет ОРД оформляется в соответствии с требованиями ГОСТ Р 6.30-2003 «Унифицированная система организационно-распорядительной документации. Требование к оформлению документов».
- Техническое задание и технический проект на СЗПДн оформляются в соответствии с требованиями РД 50-34.698-90 «Автоматизированные системы требования к содержанию документов».

ТРЕТЬЯ СТАДИЯ
РЕАЛИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ПДН

Выполняемые работы в рамках реализации

- Устанавливаются и настраиваются **технические средства защиты информации в пилотной зоне**.
- Проводятся **испытания в пилотной зоне**.
- Устанавливаются и настраиваются **технические средства защиты информации в зоне внедрения**.
- Проводятся **испытания в зоне внедрения**.
- Сдача системы защиты ПДн в **промышленную эксплуатацию**.
- **Обучение персонала** Заказчика правилам работы с компонентами системы защиты ПДн.

ТРЕТЬЯ СТАДИЯ
РЕАЛИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ПДН

Результаты реализации

- **Внедренная система защиты персональных данных, включающая установленные технические средства защиты информации и выстроенные процессы обработки/защиты персональных данных.**

КОНТАКТНАЯ ИНФОРМАЦИЯ

Малявкин Александр
Ведущий консультант по ИБ/Руководитель группы
Тел.: +7 (495) 921-1410 доб. 2016
Моб. тел.: +7 (965) 113-1806
e-mail: AMalyavkin@leta.ru

LETA IT-company
109129, Россия, Москва, ул. 8-я Текстильщиков, д.11, стр. 2
Тел./факс: +7 (495) 921-1410
Единая служба сервисной поддержки: + 7 (495) 921-1410
www.leta.ru