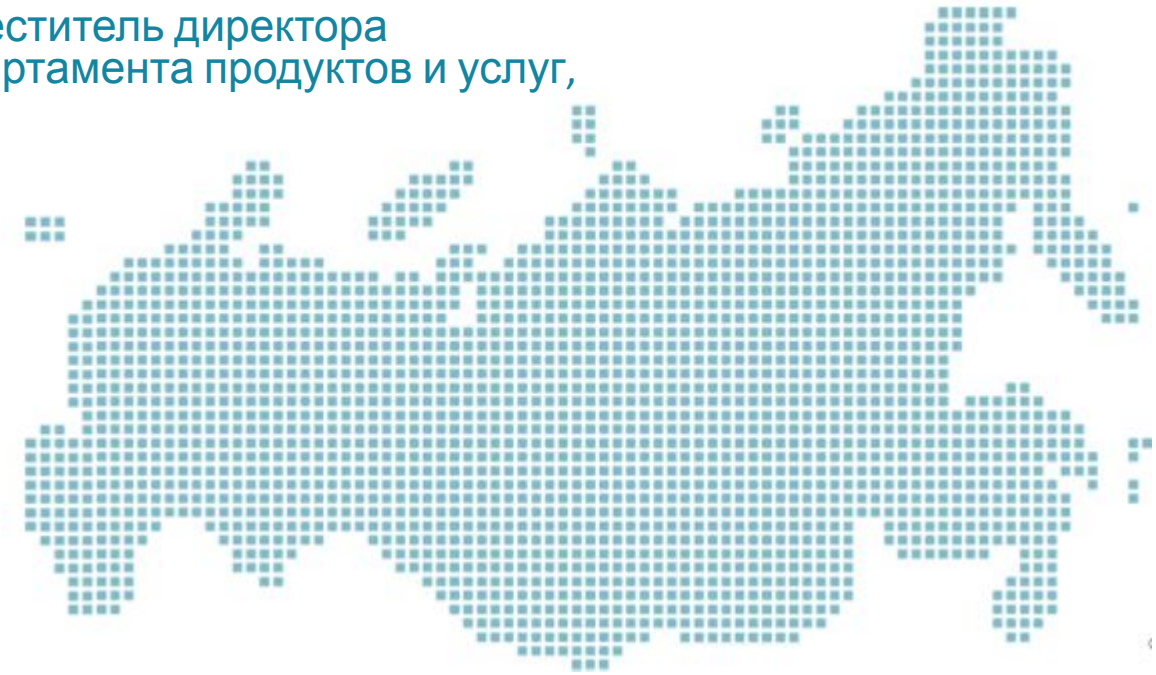
Грани ИБ
Законодательство, процессы, технологии

16-18 января 2011
«Атлас Парк-Отель»

Изменения в правовом поле кредитных организаций(152-ФЗ, СТО БР ИББС, ЭП, НПС)

Царев Евгений
Заместитель директора
Департамента продуктов и услуг,
MBA



152-ФЗ. ИЗМЕНЕНИЯ В…

1. **Терминологии**
2. Условиях обработки ПДн
3. **Разделение на «Операторов ПДн» и «Лиц, осуществляющих обработку ПДн по поручению оператора ПДн»**
4. **Порядке организации обработки и защиты ПДн**
5. **Форме получения согласия на обработку ПДн**
6. Взаимодействия с субъектом ПДн
7. Трансграничной передаче ПДн
8. Порядке уведомления Роскомнадзора
9. **Мерах по защите ПДн**
10. Ответственности за неисполнение требований закона

ИЗМЕНЕНИЯ В ТЕРМИНОЛОГИИ

ИЗМЕНЕНИЯ В ТЕРМИНОЛОГИИ

- Добавился термин **«автоматизированная обработка»**, в котором четко определено, что использование любых средств вычислительной техники автоматически делает обработку автоматизированной.
- Термин **«обезличивание ПДн»** был дополнен уточнением, что обезличенной считается любая информация, которая сама по себе (без дополнительных источников информации) не позволяет определить принадлежность ее конкретному субъекту

ИЗМЕНЕНИЯ В ТЕРМИНОЛОГИИ

- Из термина **«ИСПДн»** исчезли фразы про обработку без средств автоматизации. Соответственно, исчезает и понятие смешанной обработки в ИСПДн.
- В термине **«трансграничная передача ПДн»** вместо «передачи через Государственную границу Российской Федерации», появилась **«передача на территорию иностранного государства»**

ИТОГО. ИЗМЕНЕНИЯ В ТЕРМИНОЛОГИИ

- ПДн - все, что относится к физическому лицу.
- Автоматизированная обработка – обработка только с использованием СВТ.
- ИСПДн – только те компоненты, которые участвуют в автоматизированной обработке (базы данных, технические средства, информационные технологии).
- Обезличивание ПДн – действия, в результате которых невозможно утверждать, что ПДн относятся к конкретному субъекту ПДн, т.е. ПДн могут относиться к нескольким субъектам ПДн.

РАЗДЕЛЕНИЕ НА **«ОПЕРАТОРОВ ПДН»** И **«ЛИЦ, ОСУЩЕСТВЛЯЮЩИХ ОБРАБОТКУ ПДН ПО ПОРУЧЕНИЮ ОПЕРАТОРА ПДН»**

РАЗДЕЛЕНИЕ НА «ОПЕРАТОРОВ ПДН» И «ЛООПДНППОПДН»

- Оператор
  - организует/осуществляет обработку;

  и
  - определяет состав персональных данных, подлежащих обработке;

  и
  - определяет цели обработки;

  и
  - определяет действия (операции), совершаемые с персональными данными.

- Если хотя бы один из пунктов не осуществляется, то есть основания утверждать, что данное лицо не является оператором ПДн, а возможно является ЛООПДНППОПДН

РАЗДЕЛЕНИЕ НА «ОПЕРАТОРОВ ПДН» И «ЛООПДНППОПДН»

- **В поручении на обработку ПДн** должны быть в обязательном порядке определены:
  - перечень действий с ПДн, которые будут совершаться ЛООПДНППОПДН;
  - цели обработки;
  - обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке;
  - требования к защите ПДн.

ИЗМЕНЕНИЯ В ПОРЯДКЕ ОРГАНИЗАЦИИ ОБРАБОТКИ И ЗАЩИТЫ ПДН

ИЗМЕНЕНИЯ В ПОРЯДКЕ ОРГАНИЗАЦИИ ОБРАБОТКИ И ЗАЩИТЫ ПДН

- Операторам юридическим лицам необходимо назначить физическое либо юридическое лицо, ответственное за организацию обработки персональных данных.
  - Осуществляет контроль исполнения законодательства по ПДн
  - Доводить до сотрудников положения нормативки по ПДн
  - Организовать работу по обращениям субъектов

ИЗМЕНЕНИЯ В ПОРЯДКЕ ОРГАНИЗАЦИИ ОБРАБОТКИ И ЗАЩИТЫ ПДН

- Необходимо разработать «**Политику Компании в отношении обработки ПДн**» и разместить ее на веб-сайте (либо иным образом предоставить к ней неограниченный доступ).

5. ИЗМЕНЕНИЯ В ФОРМЕ ПОЛУЧЕНИЯ СОГЛАСИЯ НА ОБРАБОТКУ ПДН

ИЗМЕНЕНИЯ В ФОРМЕ ПОЛУЧЕНИЯ СОГЛАСИЯ НА ОБРАБОТКУ ПДН

- Согласие на обработку ПДн можно получать в любой форме (аудио, «галочки» на веб-сайтах и
т. п.), включая конклюдентные действия. Главное – доказать, что согласие было получено,
т. е. не фальсифицировано самим оператором.

- Для письменной формы согласия введено дополнение о необходимости указания в ней данных о ЛООПДНППОПДН, если обработка будет поручена такому лицу.

ИЗМЕНЕНИЯ В МЕРАХ ПО ЗАЩИТЕ ПДН

ИЗМЕНЕНИЯ В МЕРАХ ПО ЗАЩИТЕ ПДН

- Ст. 18.1:
  - ...**Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей**, предусмотренных настоящим ФЗ и принятыми в соответствии с ним нормативными правовыми актами… К таким мерам **могут, в частности, относиться**:
  - …
  - 3) применение правовых, организационных и технических мер по обеспечению безопасности ПДн **в соответствии со статьей 19** настоящего ФЗ;

ИЗМЕНЕНИЯ В МЕРАХ ПО ЗАЩИТЕ ПДН

- 2. Обеспечение безопасности персональных данных достигается, **в частности**:
  - 1) определением угроз безопасности ПДн при их обработке в ИСПДн;
  - 2) применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПДн;
  - 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
  - 4) оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

ИЗМЕНЕНИЯ В МЕРАХ ПО ЗАЩИТЕ ПДН

- 2. Обеспечение безопасности персональных данных достигается, **в частности**:
  - …
  - 5) учетом машинных носителей ПДн;
  - 6) обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
  - 7) восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
  - 8) установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
  - 9) контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

ИЗМЕНЕНИЯ В МЕРАХ ПО ЗАЩИТЕ ПДН

- Теперь на законодательном уровне закреплена **обязанность оператора ПДн оценивать вред**, который может быть причинен субъектам и соотнести указанный вред с принимаемыми оператором мерами, направленными на обеспечение выполнения обязанностей, предусмотренных ФЗ.

- Введено понятие **уровней защищенности ИСПДн**, которые должны быть определены в соответствующих Постановлениях Правительства РФ. **Пока не изданы.**

ИЗМЕНЕНИЯ В МЕРАХ ПО ЗАЩИТЕ ПДН

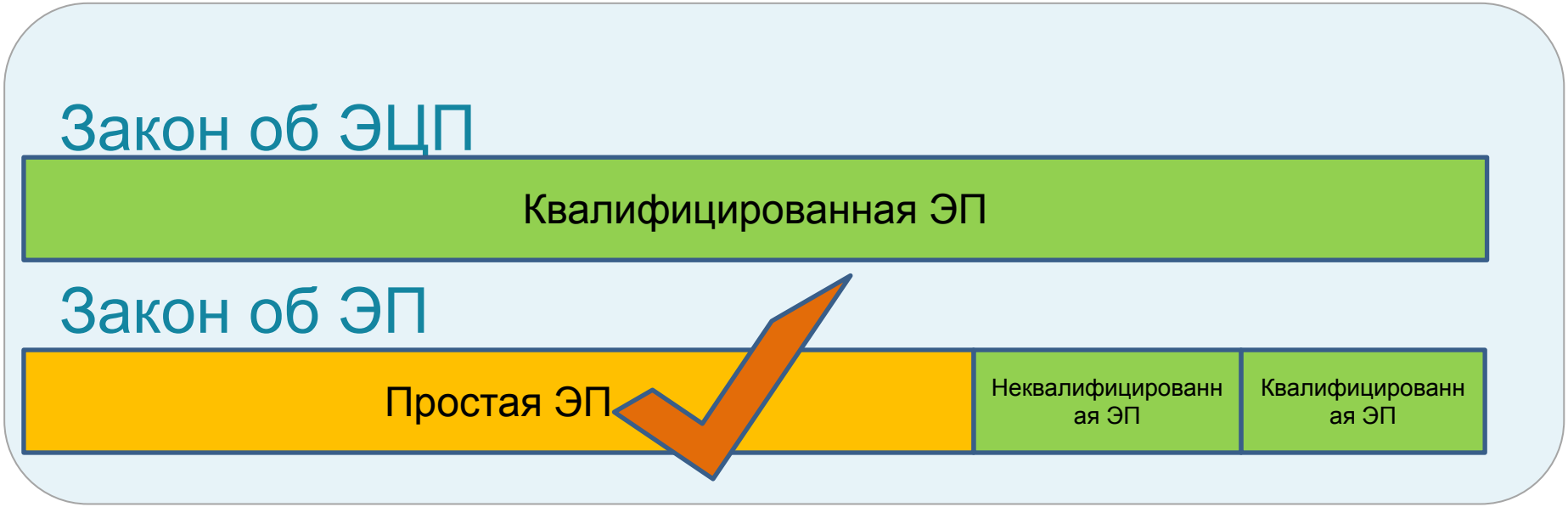
- Оператор ПДн самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ.
- Меры по защите ПДн, перечисленные в ст. 18.1 и 19 являются только типовым набором, а отнюдь не обязательными для исполнения.
- На законодательном уровне четко указана последовательность действий: «Оценка вреда» - «Оценка актуальности угроз» - «Уровень защищенности» - «Оценка реализации требований по ИБ в ИСПДн Компании» - «Модернизация системы защиты ПДн»
- Использование сертифицированных (прошедших в установленном порядке процедуру оценки соответствия) средств защиты информации, в новой редакции 152-ФЗ указано, как одна из мер, но вовсе необязательная, однако требование по использованию сертифицированных СЗИ, пока содержится в документах ФСТЭК России (Приказ № 58).

ЗАКОН ОБ ЭЛЕКТРОННОЙ ПОДПИСИ

ЗАКОН ОБ ЭЛЕКТРОННОЙ ПОДПИСИ

1. Ст.2: «электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию»
2. Ст.3: «…порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней…»

ЗАКОН ОБ ЭЛЕКТРОННОЙ ПОДПИСИ



Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом

СТО БР ИББС

Классификатор
СТО БР ИББС – 0.0

Термины и определения
СТО БР ИББС – 0.1

Общие положения
СТО БР ИББС – 1.0

Аудит информационной безопасности
СТО БР ИББС – 1.1

Методика оценки соответствия
СТО БР ИББС – 1.2

Документы по обеспечению информационной безопасности
РС БР ИББС – 2.0

Методика оценки рисков
РС БР ИББС – 2.2

Руководство по самооценке
РС БР ИББС – 2.1

Требования по обеспечению Безопасности СКЗИ
РС БР ИББС – 2.5

Требования по обеспечению безопасности ПДн в ИСПДн
РС БР ИББС – 2.3

Отраслевая модель угроз
РС БР ИББС – 2.4

Методика классификации активов
РС БР ИББС – Х.Х

Методика назначения и описания ролей
РС БР ИББС – Х.Х

ЗАКОН О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ

1. В случае хищения денежных средств со счета клиента банк обязан возместить полную сумму похищенных средств (Статья 9 пп. 11-16)
2. ЦБ определяет правила платежной системы. Правилами должны определяться требования к защите информации. (Статья 15. пп.4 -5, Статья 20 п. 1)
3. Требования к ЗИ определяет ЦБ и согласовывает со ФСТЭК и ФСБ. Контроль осуществляется ФСТЭК, ФСБ и ЦБ (Статья 27)

КОНТАКТНАЯ ИНФОРМАЦИЯ

Царев Евгений
Заместитель директора Департамента продуктов и услуг, MBA
Моб. тел.: +7 (926) 104-7058
e-mail: ETsarev@leta.ru

LETA
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