Возможные проблемы и особенности применения положений новых документов регуляторов в области защиты персональных данных для финансовой сферы (взгляд интегратора)

Акимов Сергей Леонидович

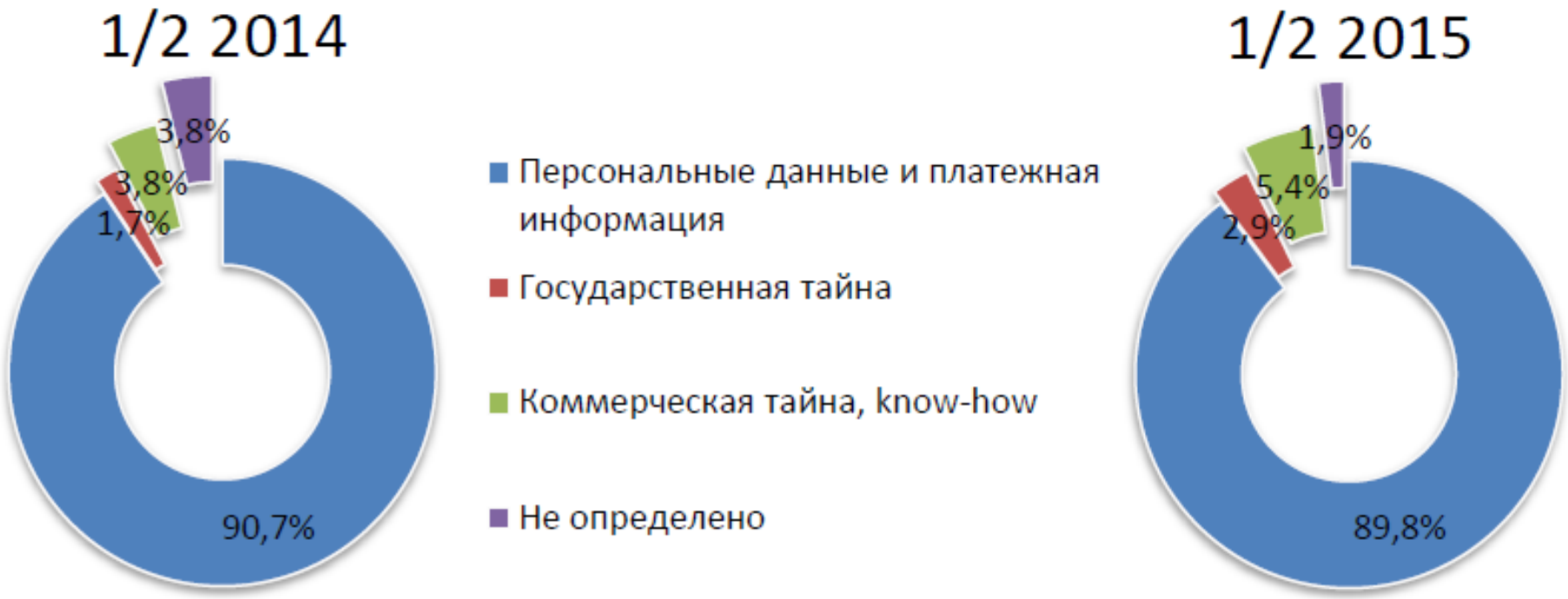
ЭЛВИС-ПЛЮС

Немного статистики (I полугодие 2015 г.)

- 90% утечек связаны с компрометацией ПДн
- Скомпрометированы более 262 млн. записей, в том числе платежная информация
- Россия – 2 место по числу утечек
- 59 случаев утечки конфиденциальной информации из российских компаний и государственных организаций

Источник: Infowatch «Глобальное исследование утечек конфиденциальной информации в I полугодии 2015 года»

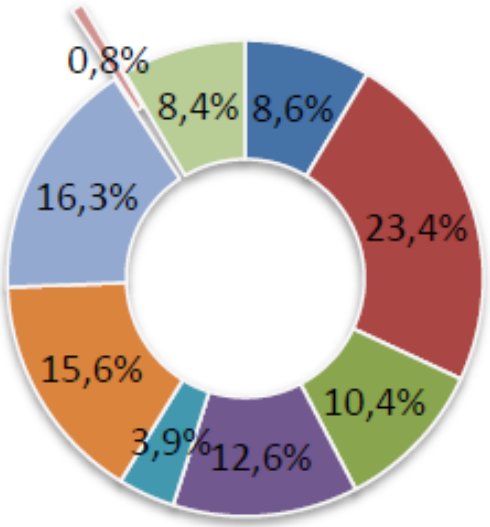
Распределение утечек по типам данных



Источник: Infowatch «Глобальное исследование утечек конфиденциальной информации в I полугодии 2015 года»

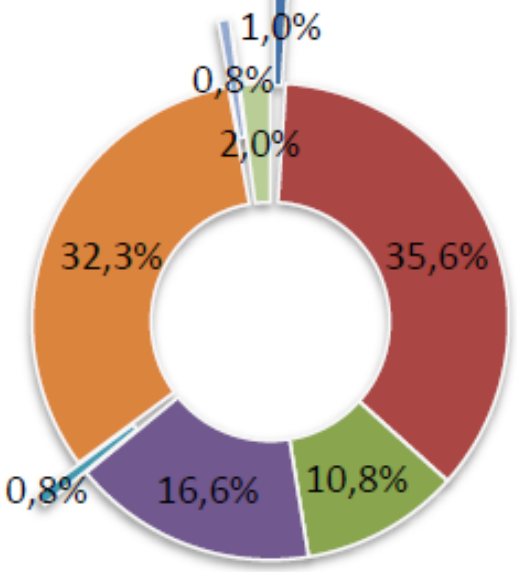
Распределение утечек по отраслям

Число утечек



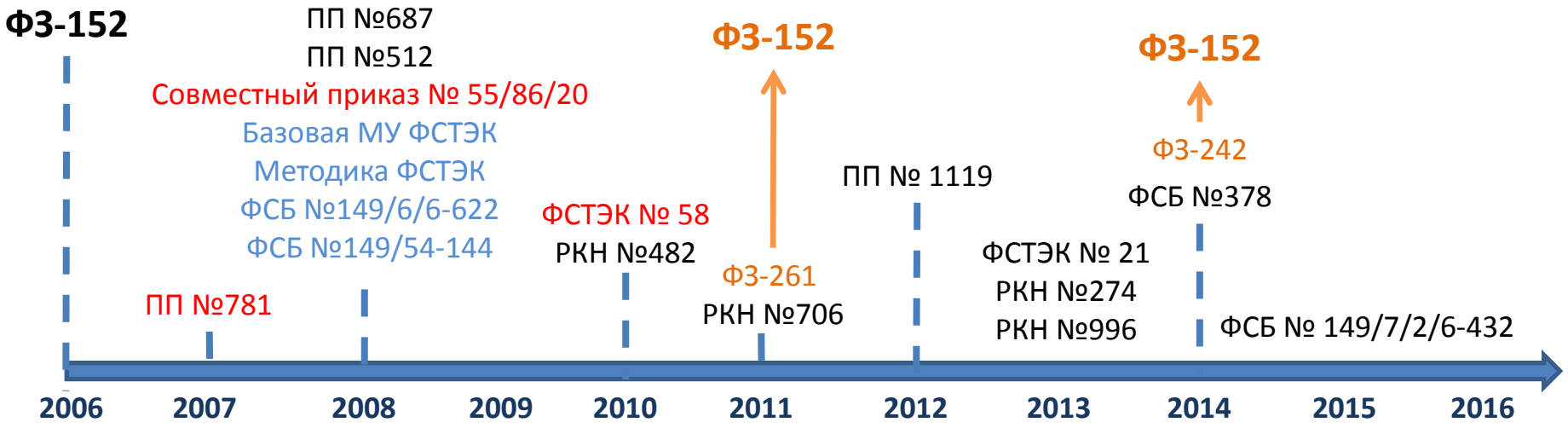
- Банки и финансы
- Медицина
- Торговля, HoReCa
- Высокие технологии
- Промышленность и транспорт
- Госорганы и силовые структуры
- Образование
- Муниципальные учреждения
- Другое/не определено

К-во записей



Источник: Infowatch «Глобальное исследование утечек конфиденциальной информации в I полугодии 2015 года»

Основные документы - хронология



СТО БР ИББС-1.0-2006

СТО БР ИББС-1.1-2007
СТО БР ИББС-1.2-2007
РС БР ИББС-2.0-2007
РС БР ИББС-2.1-2007

СТО БР ИББС-1.0-2008
СТО БР ИББС-1.2-2009

СТО БР ИББС-1.0-2010
СТО БР ИББС-1.2-2010
РС БР ИББС-2.2-2009
РС БР ИББС-2.3-2010 Требования
РС БР ИББС-2.4-2010 Отраслевая МУ
Методические рекомендации

161-ФЗ

382-П

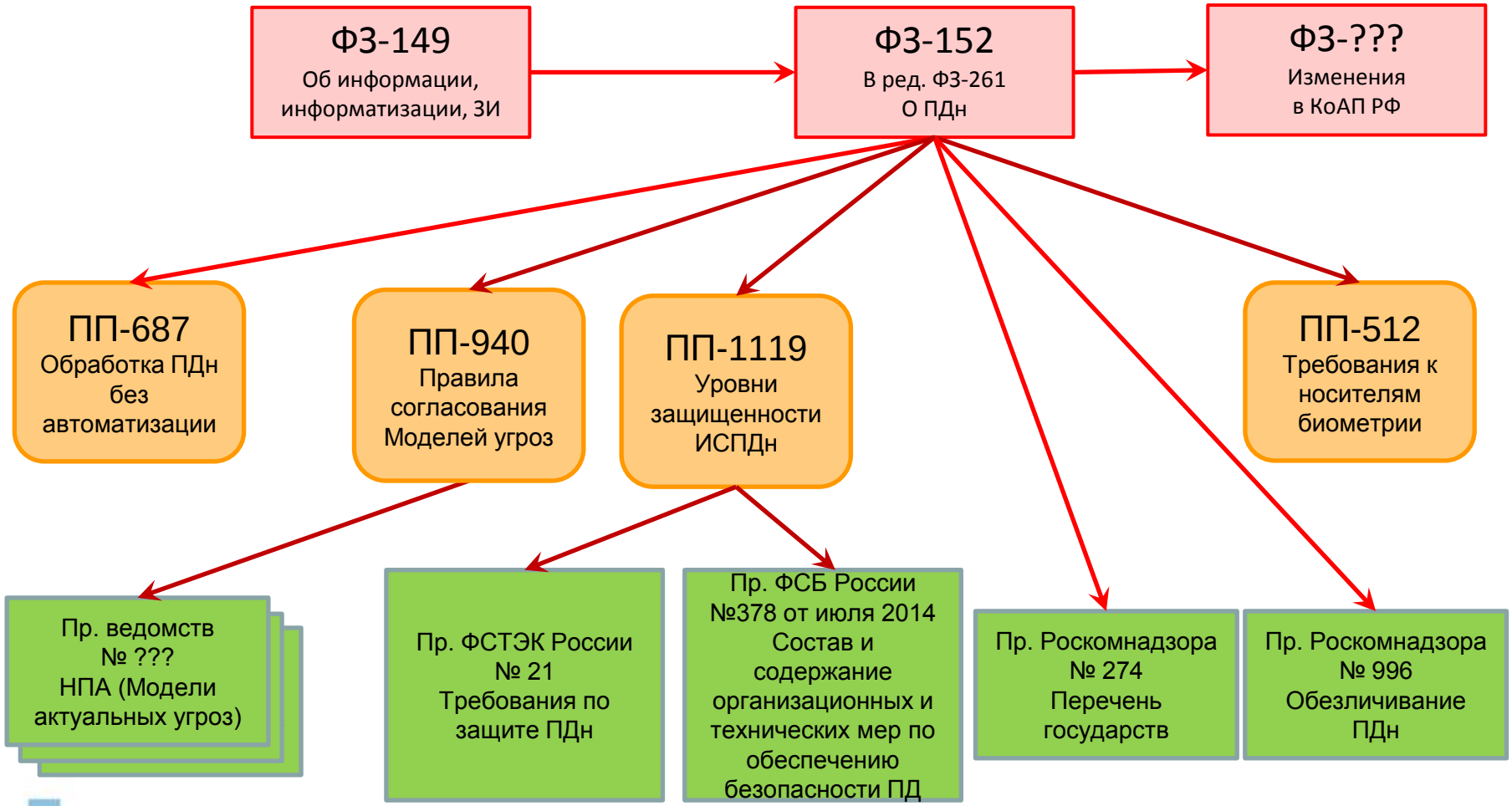
3361-У
СТО БР ИББС-1.0-2014
СТО БР ИББС-1.2-2014
РС БР ИББС-2.6-2014
РС БР ИББС-2.5-2014

СТО БР ИБНФО Б-1.0
СТО БР ИБНФО М-1.0
Проект указания БР

РС БР ИББС-2.8-2015
РС БР ИББС-2.7-2015

СТРУКТУРА НОРМАТИВНОЙ БАЗЫ

Вопросы обработки персональных данных



Ранее ← ФЗ-152 → Сейчас

Совместный приказ № 55/86/20
Базовая МУ ФСТЭК
Методика ФСТЭК
ФСТЭК № 58
ФСБ №149/6/6-622
ФСБ №149/54-144

- *СТО БР ИББС-1.0-2010*
- *Отраслевая частная модель угроз (РС БР ИББС-2.4)*
- *Требования по обеспечению безопасности ПДн в ИСПДн организаций БС РФ (РС БР ИББС-2.3)*

ФЗ-242
ПП № 1119
ФСТЭК № 21
ФСБ №378
ФСБ № 149/7/2/6-432

- *СТО БР ИББС-1.0-2014*
- *Проект указания БР об определении угроз безопасности ПДн (СТО БР ИБНФО Б-1.0)*
- *Обеспечение ИБ некредитных финансовых организаций – малых и микропредприятий (СТО БР ИБНФО М-1.0)*

ФЗ-152

- **(ст. 19 п. 5)** ФОИВ, ОГВ субъектов РФ, Банк России, органы государственных внебюджетных фондов, иные государственные органы принимают нормативные правовые акты, в которых определяют угрозы безопасности ПДн

- **(ст. 19 п.6)** ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности ПДн

Проект указания БАНКА РОССИИ «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных»

Некредитные финансовые организации:

- профессиональные участники рынка ценных бумаг;
- управляющие компании инвестиционного фонда;
- специализированные депозитарии инвестиционного фонда;
- клиринговая деятельность;
- деятельность центрального депозитария;
- деятельность субъектов страхового дела;
- негосударственные пенсионные фонды;
- микрофинансовые организации;
- кредитные потребительские кооперативы;
- жилищные накопительные кооперативы;
- бюро кредитных историй;
- актуарная деятельность;
- ломбарды

Проблемные вопросы

- НПА: организация работ по использованию НПА разными организациями финансовой сферы, регулируемой ЦБ РФ?

- НПА: устанавливает перечень всего из 10 угроз, сформулированных в обобщённом виде
  (Банк данных угроз безопасности информации ФСТЭК России - детальное описание 182 угроз)

«Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности ПДн, актуальные при обработке ПДн в ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности»

- Утвержден руководством 8 Центра ФСБ России 31 марта 2015 года

Основные разделы

- Рекомендации по описанию ИСПДн при осуществлении соответствующих видов деятельности
- Определение актуальности использования СКЗИ для обеспечения безопасности ПДн
- Определение актуальных угроз (Рекомендации по определению актуальности угроз в зависимости от типа информационной системы, анализ компенсирующих мер, позволяющих снизить класс защищенности СКЗИ, описание объектов защиты и т.д)

И главное, примеры обоснований и выбора актуальных угроз, с заполнением соответствующих таблиц…

Для ФОИВ, органов государственной власти, ЦБ РФ… (требует согласования с ФСБ России):

- При подготовке перечня актуальных угроз для операторов (организаций), находящихся в сфере регулирования ФОИВ, на который возложены функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности;
- При защите ведомственных ИСПДн (центральный, региональных, территориальных и т.д.)

Для операторов персональных данных… (не требует согласования с ФСБ России)

- При подготовке частных моделей угроз

Проблемы и вопросы

- НПА: организация работ по использованию НПА разными организациями финансовой сферы, регулируемой ЦБ РФ?

- НПА: подготовка модели угроз?

- Потребуется ли корректировка существующих действующих Моделей угроз;
- А как действовать в отношении ИСПДн, обрабатывающих биометрические ПДн, общедоступные ПДн;
- Как использовать НПА ЦОДами, предоставляющими услуги по обработке ПДн организациям финансовой сферы;
- Порядок проведения работ, дорожная карта, контроль, надзор?

Ваши вопросы?