Learn. Connect.
Collaborate. together.

Основные тенденции законодательства в области защиты данных

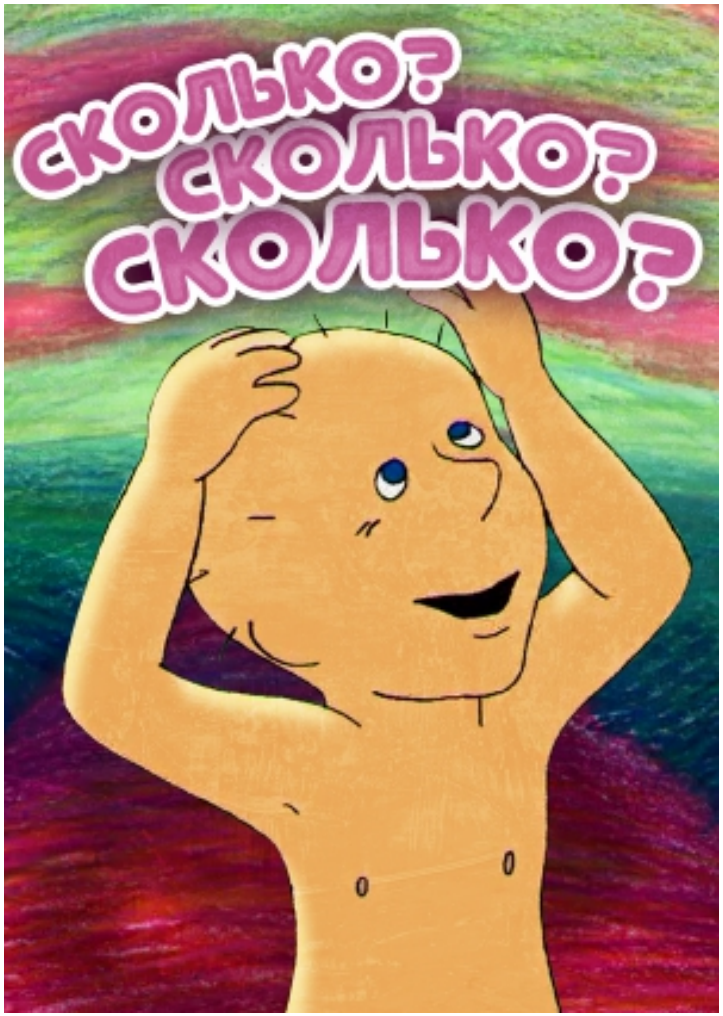
Лукацкий Алексей, консультант по безопасности

Почему Cisco говорит о законодательстве?

ТК22	ТК122	ТК362	РГ ЦБ
«Безопасность ИТ» (ISO SC27 в России)	«Защита информации в кредитных учреждениях»	«Защита информации» при ФСТЭК	Разработка рекомендаций по ПДн, СТО БР ИББС v4 и 382-П/2831-У

ФСБ	МКС	ФСТЭК	РАЭК	РКН
Экспертиза документов	Предложения	Экспертиза и разработка документов	Экспертиза и разработка документов	Консультативный совет

Поиграем в загадки?

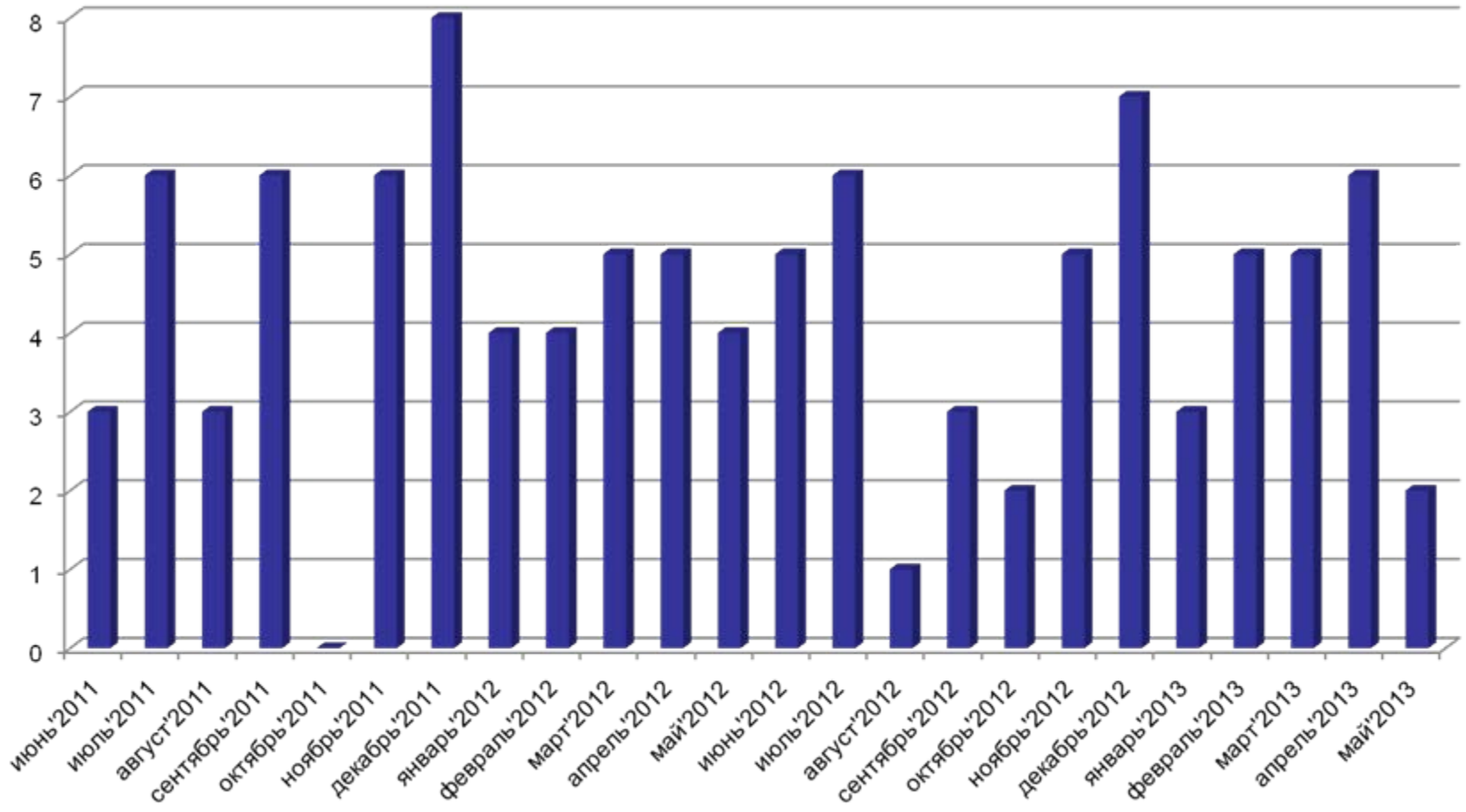


- у нас регуляторов по информационной безопасности?
- у нас появляется нормативных актов по информационной безопасности в месяц?
- у нас планируется выпустить нормативных актов в ближайшие 1-2 года?

Регуляторов в области ИБ у нас 16+

- ФСБ, ФСТЭК, СВР, МинОбороны, ФСО
- Минкомсвязь, Роскомнадзор
- МВД, Банк России
- Совет Безопасности
- PCI Council
- Минэнерго, Минэкономразвития
- Администрация Президента
- Ростехрегулирование
- Минтруд, Рособразование
- Каждый ФОИВ мнит себя регулятором по ИБ…

В среднем появляется 4 нормативных акта в месяц



Вы защищаете открытые данные?

- В последнее время нормативные акты регуляторов стали все больше уделять внимания не только конфиденциальности, но и целостности и доступности данных
  - И не всегда эти данные ограниченного доступа

Один пример : как защитить Web-сайт госоргана с открытыми, конфиденциальными и общедоступными данными?

СТР-К???

Приказ Минкомсвязи от 27.06.2013 №149

Приказ ФСТЭК от 11.02.2013 №17

Приказ МЭР от 16.11.2009 №470

Указ Президента от 17.03.2008 №351

Приказ Минкомсвязи от 25.08.2009 №104

Приказ ФСО от 07.08.2009 №487

Приказ ФСБ/ФСТЭК от 31.08.2010 №416/489

А что с данными ограниченного доступа?

- 65 видов тайн в российском законодательстве
- Персональные данные
- Коммерческая тайна
- Банковская тайна
- Тайна переписки
- Инсайдерская информация
- Служебная тайна
- Тайна кредитной истории
- …

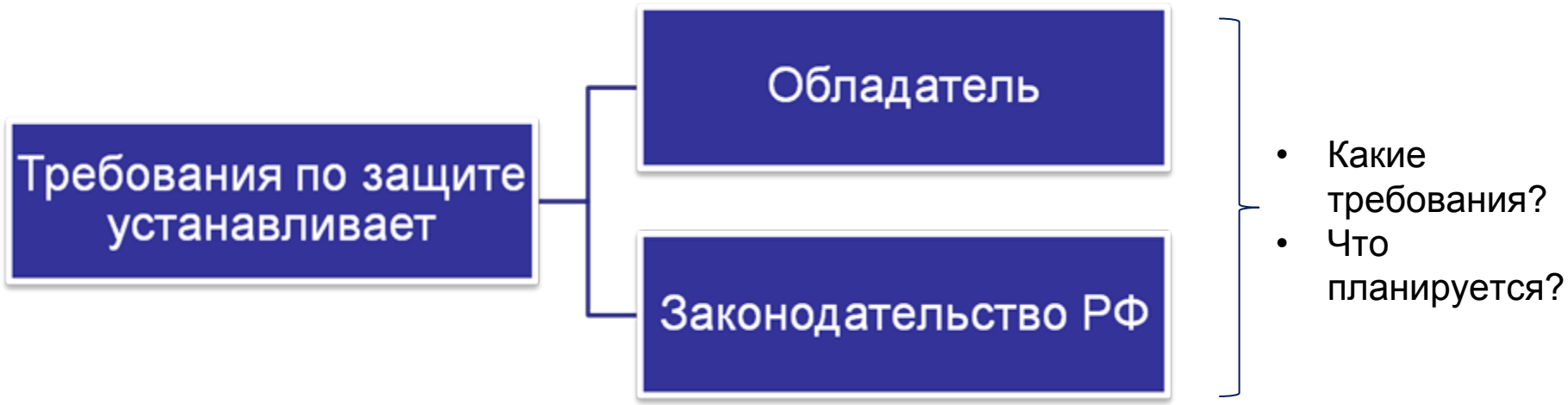
Виды информации ограниченного доступа по российскому законодательству

Составитель: Алексей Лукацкий, Cisco

п/п	Тайна	Содержимое	Нормативный акт	Наказание за
1	Информация, составляющая коммерческую тайну	Научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны	98-ФЗ "О коммерческой тайне", ст.1465 ГК РФ	183 УК РФ, 81 ТК РФ
2	Банковская тайна (тайна банковских вкладов)	Сведения об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией	ФЗ 395-1 "О банках и банковской деятельности", 857 ГК РФ, Таможенный кодекс РФ, ФЗ "О реструктуризации кредитных организаций"	183 УК РФ, 81 ТК РФ
3	Служебная тайна	Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами	Указ Президента от 6.03.1997 №188, 139 ГК РФ, ФЗ "Об основах государственной службы Российской Федерации", Постановление Правительства РФ от 3.11.94г. № 1233	81 ТК РФ
4	Тайна кредитной истории		218-ФЗ "О кредитных историях"	81 ТК РФ

Обязанность защиты

- Обладатель информации обязан принимать меры по защите информации
  - Ст.6 ФЗ-149
- Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить…
  - Ст.16 ФЗ-149



Какие требования по защите установлены законодательством РФ?

Требования носят рекомендательный характер

Планов по активному развитию пока нет

Требований пока нет (исключая КСИИ)

Планируемые изменения по направлению ПДн

- Приказ РКН по обезличиванию
- Приказ ФСБ по использованию СКЗИ для защиты ПДн
- Законопроект «О внесении изменений в статью 857 части второй ГК РФ, статью 26 ФЗ «О банках и банковской деятельности» и ФЗ «О персональных данных»
- Большая порция изменений в ФЗ-152
- Законопроект по внесению изменений в КоАП (в части увеличения штрафов по ст.13.11)
- Проект Постановления Правительства по надзору в сфере ПДн
- Указание Банка России с отраслевой моделью угроз ПДн
- СТО БР ИББС и новая версия «письма шести» (?)
- Реформа Евроконвенции

Планируемые изменения по направлению ГИС

- Меры защиты информации в государственных информационных системах
- Порядок моделирования угроз безопасности информации в информационных системах
- Методические документы, регламентирующие
  - Порядок аттестации распределенных информационных систем
  - Порядок обновления программного обеспечения в аттестованных информационных системах
  - Порядок выявления и устранения уязвимостей в информационных системах
  - Порядок реагирования на инциденты, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации

Планируемые изменения по направлению банковской тайны

- Новая редакция СТО БР ИББС 1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»
- Новая редакция СТО БР ИББС 1.2 «Методика оценка соответствия СТО БР ИББС 1.0»
- РС «Ресурсное обеспечение информационной безопасности»
- РС «Требования по к обеспечению информационной безопасности на стадиях жизненного цикла банковских приложений»
- РС «Менеджмент инцидентов информационной безопасности»
- Единое пространство доверия с операторами связи

Планируемые изменения по направлению НПС

- Изменения в 382-П (3007-У)
- Отчетность по инцидентам (3024-У)
- Защита банкоматов и платежных терминалов (34-Т и др.)
- Защита электронных средств платежа
- Защита дистанционного банковского обслуживания
- Защита мобильного банкинга
- Рекомендации по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети «Интернет» (146-Т)
- Изменение ст.9 ФЗ-161
- Обязательные нормативы управления операционными рисками
- Национальная система фрод-мониторинга
- Официальный перевод и признание PCI DSS и PA DSS 2.0 и 3.0

Как защищать данные?

- ФСТЭК (2013-2015)
  - Требования к средствам доверенной загрузки
  - Требования к средствам контроля съемных носителей
  - Требования к средствам контроля утечек информации (DLP)
  - Требования к средствам аутентификации
  - Требования к средствам разграничения доступа
  - Требования к средствам контроля целостности
  - Требования к средствам очистки памяти
  - Требования к средствам ограничения программной среды
  - Требования к средствам управления потоками информации (МСЭ, однонаправленные МСЭ, коммутаторы…)
  - ГОСТы по защите виртуализации и облачных вычислений
- ФСБ
  - Виртуализация, снижение числа классов СКЗИ

Что делать при таком обилии новых и планируемых НПА?

- У вас всегда есть выход ☺

security-request@cisco.com

Благодарю вас за внимание