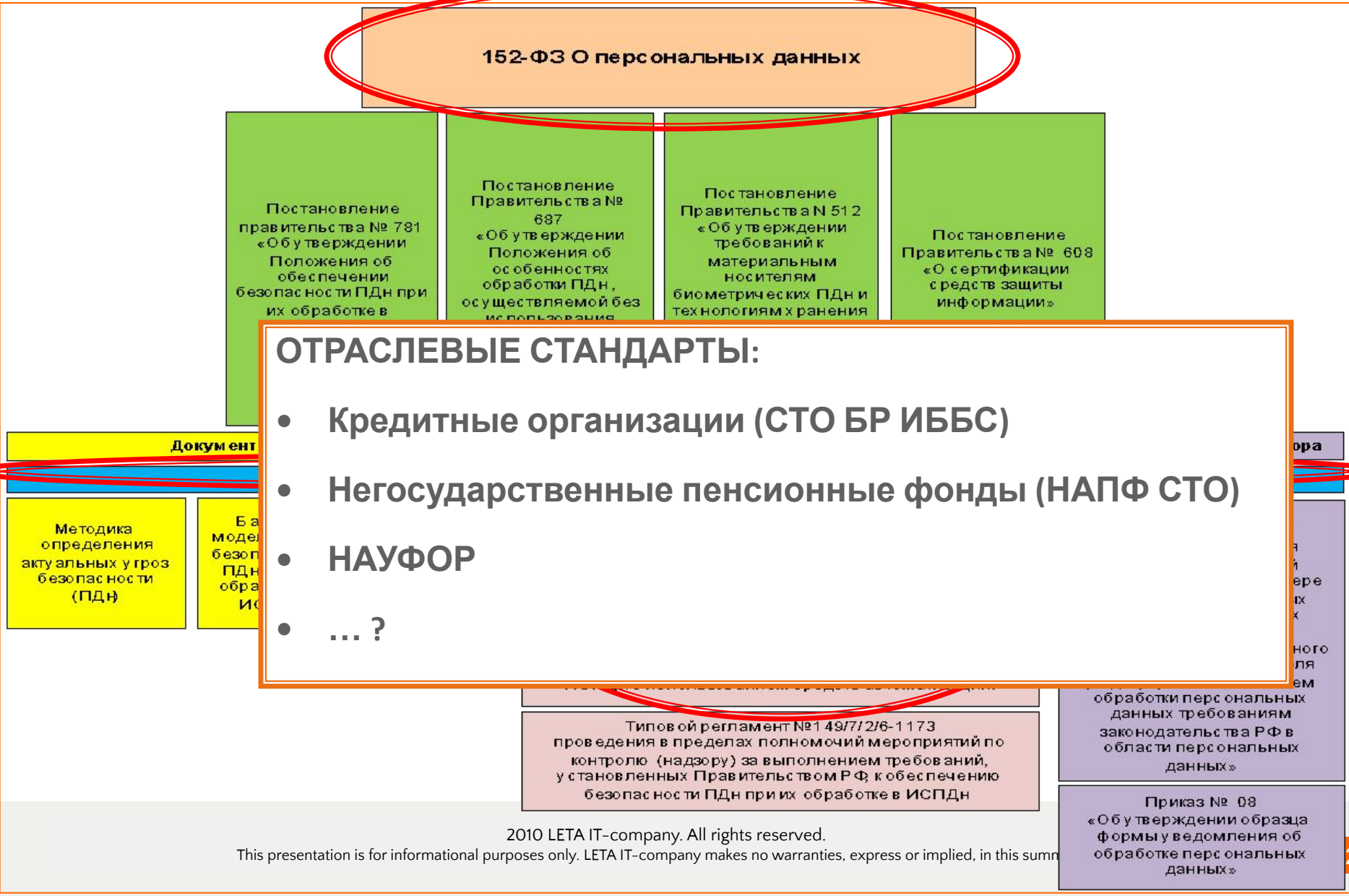
152-ФЗ: прагматичный подход к выполнению требований

Бондаренко Александр
Директор департамента консалтинга, CISA, CISSP

152-ФЗ: ТЕКУЩАЯ НОРМАТИВНАЯ СРЕДА



ПРОВЕРКИ ПО 152-ФЗ

- за 2010 г. проведено **1253** проверки из них **804** плановые
- составлено более **3000** протоколов об административных правонарушениях
- ключевые нарушения: отсутствие уведомления, некорректно составленные уведомления, отсутствие согласия субъекта ПДн
- на 2011 г. запланировано **1415** проверок (http://rsoc.ru/docs/4_Plan_proverok_2011.zip)
- первоочередные документы для проверки:
  - перечень персональных данных
  - образцы заключенных согласий
  - копии договоров, в рамках которых производится получение или передача ПДн
  - образцы документов, содержащих ПДн
  - документы, определяющие порядок обеспечения безопасности ПДн

ОШИБКИ ПРИ РЕЛИЗАЦИИ ПРОЕКТА

- проект по 152-ФЗ это не спринт, а марафон !
- ориентир только на выполнение требований и выполнение работы «в стол»
- минимальное вовлечение в проект (работа от консультанта «под ключ»)
- отсутствие координации внутренних служб (ИТ, ИБ, юридическая, кадровая службы)
- намеренное сокращение области проекта
- игнорирование необходимости обучения пользователей
- «махинации» с выбором и применением средств защиты

ИНТЕГРАЦИЯ 152-ФЗ И МЕЖДУНАРОДНЫЕ ПРАКТИКИ

		ISO 27001
Основные методы и способы защиты информации от несанкционированного доступа	реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;	A.11
	ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;	A.9.1
	разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;	A.11
	регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;	A.10.10
	учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;	A.10.7
	резервирование технических средств, дублирование массивов и носителей информации;	A.10.5
	использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;	-
	использование защищенных каналов связи;	A.10.6.1
	размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;	A.9.2.1
	организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;	A.9.1
	предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.	A.10.4
Методы защиты при взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования)	межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;	A.10.6.1, A.11.4.6 - A.11.4.7
	обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;	A.10.6.1
	анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);	A.12.6.1
	использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;	A.11
	централизованное управление системой защиты персональных данных информационной системы.	4.2, A.13

КОНТАКТНАЯ ИНФОРМАЦИЯ

Бондаренко Александр Валерьевич

Директор департамента консалтинга, CISA,CISSP
Компания LETA

e-mail: abondarenko@leta.ru

109129, Россия, Москва, ул. 8-я Текстильщиков, д.11, стр. 2

Тел./факс: +7 (495) 921-1410
www.leta.ru