ЭЛВИС-ПЛЮС

ТРИ СТАНДАРТА. ЕДИНСТВО И БОРЬБА ПРОТИВОПОЛОЖНОСТЕЙ

(Триединство требований)

Сергей ВИХОРЕВ, Роман КОБЦЕВ

ОАО «ЭЛВИС-ПЛЮС»

2011 год

© ОАО «ЭЛВИС-ПЛЮС», 2010 г.,

ЭЛВИС-ПЛЮС

© Авторские права защищаются
в соответствии с законодательством
Российской Федерации

При использовании ссылка на
первоисточник обязательна

ЭЛВИС-ПЛЮС

ВНИМАНИЕ!

В этой презентации не будет детального анализа требований, предъявляемых различными стандартами. Они, как правило, достаточно схожи и будут рассмотрены в последующих выступлениях.

Целью этого выступления является необходимость разъяснения того факта, что не надо строить три разные системы защиты, надо строить одну и она будет справедлива для всех требований.

ЭЛВИС-ПЛЮС

ВОПРОСЫ ПРЕЗЕНТАЦИИ

ЭЛВИС-ПЛЮС

ВОПРОСЫ ПРЕЗЕНТАЦИИ

- Триединство нормативных документов
- Краткий анализ нормативных документов
- Основные факторы единства требований
- Краткие выводы
- Инструкции к исполнению

ЭЛВИС-ПЛЮС

ПРОЛОГ

С целью выполнения в организациях БС РФ требований ФЗ «О персональных данных», ЦБ РФ при участии АРБ и Ассоциации «Россия» разработал отраслевые документы по приведению деятельности организаций БС РФ в соответствие с требованиями законодательства в области персональных данных.

«Письмо шести» от 28.06.2010 № 01-23/3148

В комплект отраслевых документов входят:

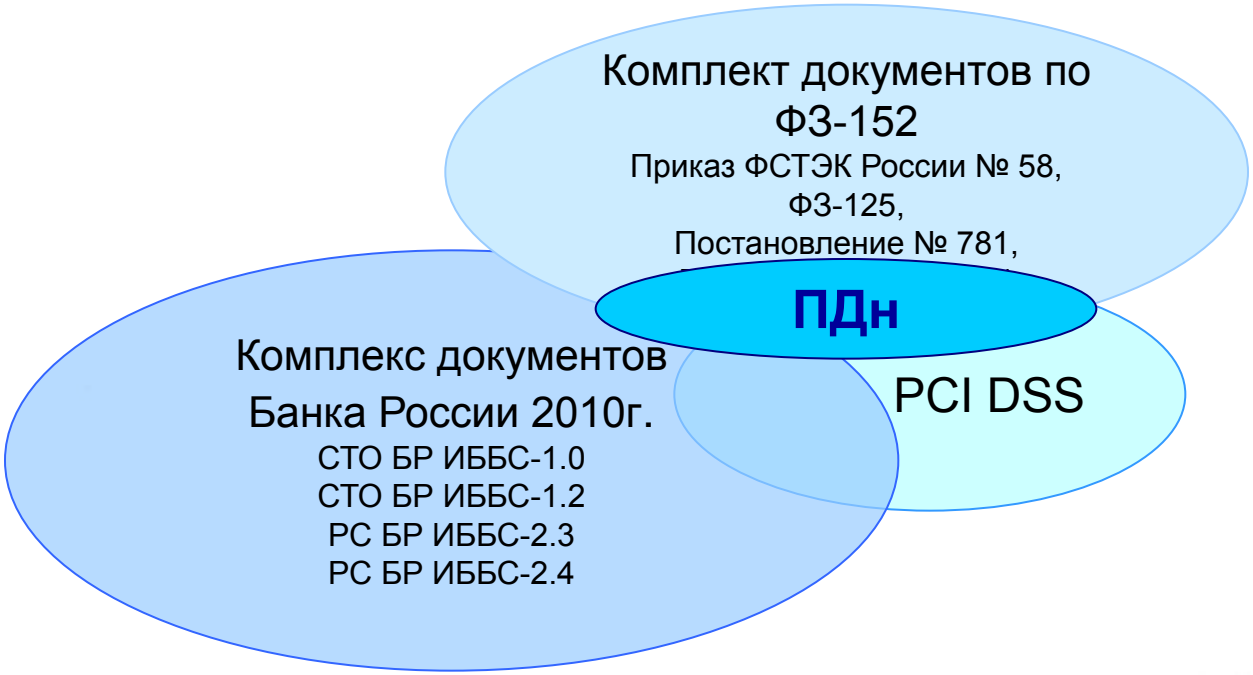
СТО БР ИББС-1.0-2010 (Общие положения)
СТО БР ИББС-1.2-2010 (Методика оценки)
РС БР ИББС-2.3 (Требования по защите ПДн)
РС БР ИББС-2.4 (Частная модель угроз)

Но есть и другие требования, которые необходимо выполнить для защиты ПДн. Что делать? Как поступать?

ЭЛВИС-ПЛЮС

КРАТКИЙ АНАЛИЗ

Триединство требований



В разных нормативах имеются требования по защите информации, но все они защищают еще и ПДн

ЭЛВИС-ПЛЮС

СХОЖЕСТЬ И РАЗЛИЧИЕ

Что защищаем (область применения)

Комплекс документов ЦБ РФ-2010	1. Банковские платежные технологические процессы (**банковская тайна**) 2. Банковские информационные технологические процессы (**коммерческая тайна, банковская тайна**) 3. Информационные системы обработки персональных данных (**банковская тайна, персональные данные**)
Комплект нормативов, в развитие ФЗ-152	1. Информационные системы обработки персональных данных (**персональные данные**)
Стандарт PCI DSS	1. Сетевую инфраструктуру, в которой циркулируют данные о держателях карт, критичные аутентификационные данные (**персональные данные, банковская тайна**)

Наиболее широкая область применения у документов ЦБ РФ

ЭЛВИС-ПЛЮС

СХОЖЕСТЬ И РАЗЛИЧИЕ

Правовой статус

Комплекс документов ЦБ РФ-2010	Отраслевой стандарт
Комплект нормативов, в развитие ФЗ-152	Законодательный акт
Стандарт PCI DSS	Международный стандарт

Все документы имеют разный правовой статус.
Наиболее высокий статус имеют требования ФЗ-152

ЭЛВИС-ПЛЮС

СХОЖЕСТЬ И РАЗЛИЧИЕ

Обязательность исполнения

Комплекс документов ЦБ РФ-2010	Добровольный
Комплект нормативов, в развитие ФЗ-152	Принудительный
Стандарт PCI DSS	Добровольно-принудительный

Все документы по разному обязательны к исполнению.
Ясно одно: Требования ФЗ-152 надо исполнять!

ЭЛВИС-ПЛЮС

СХОЖЕСТЬ И РАЗЛИЧИЕ

«Суровость» санкций

Комплекс документов ЦБ РФ-2010	Не предусмотрены
Комплект нормативов, в развитие ФЗ-152	Административные штрафы (до 20 000 руб.), административная приостановка деятельности на 90 дней
Стандарт PCI DSS	Штрафные санкции от платежной системы (до $ 25 000), отключение от платежной системы Visa

Наиболее «суровые» санкции со стороны международных платежных ситем, хотя и наш КоАП не слаб.

ЭЛВИС-ПЛЮС

СХОЖЕСТЬ И РАЗЛИЧИЕ

Направленность требований

Комплекс документов ЦБ РФ-2010	Организационные (общие), технические конкретно для ПДн
Комплект нормативов, в развитие ФЗ-152	Организационные и технические конкретно для ПДн
Стандарт PCI DSS	В основном технические конкретно для ПДн на пластиковых картах

Во всех нормативах присутствуют конкретные технические требования по защите ПДн

ЭЛВИС-ПЛЮС

СХОЖЕСТЬ И РАЗЛИЧИЕ

Способ подтверждения соответствия

СТО БР ИББС-1.0 РС БР ИББС-2.3	1. Оценка соответствия, организацией с опытом аудита ИБ (ABISS) 2. Самооценка собственными силами
Пр. ФСТЭК № 58	1. Проверка готовности СЗИ к использованию с составлением заключения о возможности их эксплуатации (организации, имеющие лицензию на ТЗКИ)
Стандарт PCI DSS	1. Аудит, выполняемый QSA-аудитором 2. Сканирование от сертифицированного поставщика услуг (ASV) 3. Самооценка с заполнением опросного листа

Наиболее сложная процедура – по стандарту ЦБ РФ,
Наиболее затратная процедура – по стандарту PCI DSS

ЭЛВИС-ПЛЮС

ВАЖНОЕ ЗАМЕЧАНИЕ

I фактор единства

«… Оператор при обработке ПДн обязан принимать необходимые организационные и технические меры для защиты ПДн»

ФЗ-152, ст. 19, ч.1

«… Требования по обеспечению ПДн в общем случае реализуются комплексом организационных, технологических, технических и программных мер…»

РС БР ИББС-2.3-2010, п. 6.1.1

«… Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика безопасности. Политика безопасности должна учитывать все требования стандарта »

PCI DSS, п. 12.1

Все три норматива признают, что защита должна объединять организационные и технические меры.

ЭЛВИС-ПЛЮС

ВАЖНОЕ ЗАМЕЧАНИЕ

II фактор единства

«… Мероприятия по обеспечению безопасности ПДн при их обработке в ИС включают в себя … определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз…»

Постановление Правительства РФ от 17.11.2007 г. № 781, п.12.а

«… Модели угроз и нарушителей должны быть основным инструментом организации БС РФ при развертывании, поддержании и совершенствовании СОИБ…»

РС БР ИББС-1.0-2010, п. 6.1

«… Политика безопасности должна описывать ежегодно выполняемый процесс идентификации угроз, уязвимостей и результатов их реализации, в рамках формальной оценки рисков…»

PCI DSS, п. 12.1.2

Процедура моделирования угроз (оценки рисков) лежит в основе выбора требований к системе защиты ПДн

ЭЛВИС-ПЛЮС

КРАТКИЙ АНАЛИЗ ТРЕБОВАНИЙ

Состав предъявляемых технических требований

СТО БР ИББС-1.0 РС БР ИББС-2.3	1. Функции идентификации и аутентификации субъектов 2. Функции регистрации и учета 3. Функции разграничения доступа и защиты от НСД 4. Функции обеспечения целостности и безопасности ПО и СЗИ 5. Функции межсетевого экранирования 6. Функции антивирусной защиты 7. Функции шифрования (СКЗИ)
Пр. ФСТЭК № 58	1. Функции управления доступом (идентификация, аутентификация) 2. Функции регистрации и учета 3. Функции обеспечения целостности СЗИ 4. Функции анализа защищенности и обнаружения вторжений 5. Функции межсетевого экранирования 6. Функции антивирусной защиты 7. Функции шифрования
Стандарт PCI DSS	1. Функции идентификации и аутентификации субъектов 2. Функции регистрации и контроля 3. Функции разграничения доступа 4. Функции обеспечения безопасности ПО 5. Функции межсетевого экранирования 6. Функции антивирусной защиты 7. Функции шифрования

ЭЛВИС-ПЛЮС

СХОЖЕСТЬ И РАЗЛИЧИЕ

III фактор единства

СТО БР ИББС-1.0 РС БР ИББС-2.3	Технические требования **полностью совпадают** с требованиями Пр. ФСТЭК № 58
Пр. ФСТЭК № 58	Технические требования **полностью совпадают** с требованиями РС БР ИББС-2.3
Стандарт PCI DSS	Технические требования во многом **совпадают** с требованиями СТО БР ИББС-1.0, но **ограничены в применении** только пластиковыми картами

Таким образом, выполнив технические требования хотя бы по одному стандарту, можно с уверенностью сказать. Что они будут выполнены и для остальных стандартов

ЭЛВИС-ПЛЮС

ВАЖНОЕ ЗАМЕЧАНИЕ

Дополнительные преимущества для организаций БС РФ

Исходя из анализа, приведенного в Приложении к Рекомендациям Центрального Банка России РС БР ИББС-2.3-2010, видно, что выполнение этих рекомендаций гарантирует соответствие Вашей системы обеспечения информационной безопасности требованиям международных стандартов ISO/IEC 17799-2005 и ISO/IEC 27002-2005

В случае, если Комплекс БР ИББС вводится в организации БС РФ официально (решением) и система обеспечения информационной безопасности организации соответствует СТО БР ИББС-1.0, гарантировано, что и защита ПДн соответствует требованиям Регуляторов.

«Одним махом семерых побивахом!»

ЭЛВИС-ПЛЮС

ПРИВЕДЕНИЕ В СООТВЕТСТВИЕ ОРГАНИЗАЦИЙ БС РФ

Последовательность действий

- Принять решение о введении Комплекса БР ИББС
- Уведомить ЦБ РФ о принятом решении
- Привести систему в соответствие СТО БР ИББС-1,0
- Выполнить рекомендации РС БР ИББС-2.3
- Провести оценку соответствия требованиям СТО БР ИББС-1,0
- Документ о подтверждении соответствия направить Регуляторам

«Письмо шести» от 28.06.2010 г. № 23/3/3148

И все это надо сделать не позже 1 июля 2011 года

ЭЛВИС-ПЛЮС

Спасибо за внимание !

124460, МОСКВА, Зеленоград,
Центральный проспект, 11
тел. 777-42-92, факс 531-8863
e-mail: vsv@elvis.ru
http://www.elvis.ru