ЭЛВИС-ПЛЮС

ПРОБЛЕМЫ ОПЕРАТОРОВ ПЕРСОНАЛЬНЫХ ДАННЫХ.
НОРМАТИВЫ ПРИНЯТЫ, ЧТО ДАЛЬШЕ?

(требования и комментарии)

Сергей ВИХОРЕВ
Директор Аналитического Департамента
ОАО «ЭЛВИС-ПЛЮС»

2008 год

ВНИМАНИЕ!

Материалы, изложенные в данной презентации рассматривают только основные аспекты проблемы безопасности информации и не претендуют на полноту анализа изменений российского законодательства

ЭЛВИС-ПЛЮС

Пролог

В соответствии с Законом «О персональных данных» организация или физическое лицо, осуществляющее и/или организующее обработку персональных данных, является оператором персональных данных и обязано обеспечить их защиту.

С 1 января 2008 года деятельность операторов считается легализованной при наличии регистрации этих операторов в реестре.

До 1 января 2010 года все операторы обязаны обеспечить защиту персональных данных.

По оценкам ФСБ России и ФСТЭК России на сегодняшний день требования Закона касаются около 7 млн. организаций.

ЭЛВИС-ПЛЮС

Пролог

В период 2007-2008 годов в соответствии с возложенными полномочиями, ФСТЭК России разработаны и введены в действие ряд нормативных и методических документов в области защиты персональных данных.

Нормативные и методические документы по защите персональных данных разработаны во исполнение Закона 2006 г. № 152-ФЗ «О персональных данных» и Постановления Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в ИС персональных данных»

ЭЛВИС-ПЛЮС

Понятийный аппарат

Федеральный Закон № 152-ФЗ «О персональных данных»

- **Персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация**

- **Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки**

ЭЛВИС-ПЛЮС

Как обеспечить безопасность ПДн

Несогласованность классификации ИС ПДн

Оператор обязан принимать организационные и технические меры, для защиты ПДн от НСД, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий

(ФЗ «О персональных данных» ст. 19, ч. 1)

ИС ПДн делятся на «типовые» (защита только конфиденциальности) и «специальные» (защита конфиденциальности + хотя бы 1 характеристика безопасности дополнительно)

«Порядок проведения классификации ИС ПДн» (Приказ № 55/86/20, п. 14 -16)

То есть, Закон устанавливает необходимость обеспечения для всех ИС не только конфиденциальности, но и других характеристик безопасности, а нормативный документ выделяет ИС, в которых защищается только конфиденциальность

Проблема: проведение корректной классификации ИС ПДн и, следовательно, определения требований по их защите

ЭЛВИС-ПЛЮС

Какие требования выбрать?

Несогласованность требований

Новые документы вводят новые понятия и новые требования не всегда учитывают уже действующие

Категория информации в ИС / Требования к защите	ГТ	КИ	КТ	ПДн	КС
СТР	X				
СТР-К		X	X	X	
РД по АС	X	X	X		
РД по СВТ	X	X	X		
РД по МЭ	X	X	X		
РД по НДВ	X	X	X		
Требования к МЭ с СКЗИ (ФСБ России)	X	X		X	
Требования к СКЗИ (ФСБ России)	X	X	X	X	
Основные мероприятия по защите ПДн				X	
Рекомендации по защите ПДн				X	
Общие требования по защите КС					X
Пособие по организации защиты КТ			X		

Проблема: проведение гармонизации требований по защите с уже используемыми в существующих информационных системах

ЭЛВИС-ПЛЮС

Какие требования выполнять?

Необходимость реализации единого и комплексного подхода к защите ИС

На практике нет «чистых» ИС, только для обработки ПДн.

В реальных ИС организаций могут обрабатываться:

- **сведения, относящиеся к коммерческой тайне**
- **персональные данные**
- **служебная тайна**
- **другая информация**

Для реальных ИС используются требования РД ФСТЭК России по классу 1Г, СТР-К, ГОСТ Р 52448-2005 (для операторов связи), новые требования по защите ПДн

Проблема: отсутствие механизма определения совокупных требований к реальным ИС

ЭЛВИС-ПЛЮС

Какие требования применять?

Неопределенность требований

Новые документы определяют требования к классам ИС, но для ряда параметров требования не определены

Класс ИС ПДн	Режим обработки	Права доступа	Требуемые подсистемы защиты ПДн						
			КД	IAM	СМ	СКЗИ	AVP	ID&P	ПЭМИН
IV	Определяется Оператором ПДн в зависимости от ущерба от НСД								
III	Однопользов.		X	X	X		X	?	
	Многопользов.	Равные	X	X	X		X	?	
		Разные	X	X	X		X	?	
II	Однопользов.		= X	X	= X		= X	?	X
	Многопользов.	Равные	= X	X	= X		= X	?	X
		Разные	= X	= X	= X		?	?	X
I	Однопользов.		= X	= X	= X		= X	?	= X
	Многопользов.	Равные	= X	= X	= X	X	X	?	= X
		Разные	= X	= X	= X	?	X	?	= X

Проблема: уточнение требований по защите ПДн с уже используемыми в существующих информационных системах

ЭЛВИС-ПЛЮС

Какие СЗИ применять?

Отсутствие прошедших оценку соответствия (сертифицированных) СЗИ

Новые документы вводят новые требования к СЗИ ПДн

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия».

Постановление Правительства РФ от 17.11.2007 г. № 781, ст. 5

Проблема: В настоящее время отсутствуют СЗИ, которые формально можно применять для защиты ПДн.

ЭЛВИС-ПЛЮС

Сухой остаток

Или проблемы, требующие решения

- Как провести корректную классификацию ИС ПДн и, следовательно, определить требования по их защите
- Как гармонизировать требования по защите ПДн с уже используемыми в существующих ИС
- Как определить совокупные требования к реальным ИС
- Какие СЗИ, можно применять для защиты ПДн

ЭЛВИС-ПЛЮС

Спасибо за внимание !

124460, МОСКВА, Зеленоград,
Центральный проспект, 11
тел. 531-4633, факс 531-8863
e-mail: vsv@elvis.ru
http://www.elvis.ru