ЭЛВИС-ПЛЮС

20 лет
в море информационных
технологий

БУДЕМ ЖИТЬ ПО-НОВОМУ?
Анализ последних документов ФСТЭК и пути наиболее гармоничного приложения их к существующим подходам

X Международная выставка
InfoSecurity Russia'2013

Заместитель Генерального директора
ОАО «ЭЛВИС-ПЛЮС» по развитию
С. В. ВИХОРЕВ

Москва, 2013 г.

ЭЛВИС-ПЛЮС

ВОПРОСЫ ПРЕЗЕНТАЦИИ

- Краткий анализ нормативных документов
- Новый подход к выбору мер защиты
- Парадокс свободы выбора
- В помощь страждущим

КРАТКИЙ АНАЛИЗ НОРМАТИВНЫХ ДОКУМЕНТОВ

О сколько нам открытий чудных готовят просвещенья дух …

(А. С. Пушкин)

ЭЛВИС-ПЛЮС

ЧТО НОВОГО?

Приказ ФСТЭК России от 18.02.2013 г. № 21

Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

вступил в действие со 2 июня 2013 г.

Приказ ФСТЭК России от 11.02.2013 г. № 17

Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

вступил в действие с 1 сентября 2013 г.

ЭЛВИС-ПЛЮС

ЧТО НОВОГО?

Приказ ФСТЭК России № 21:

1. Изменился подход к выбору мер защиты.
2. Существенно изменился перечень мер защиты
3. Появились компенсирующие меры по снижению актуальных угроз
4. Требования к классам СрЗИ увязаны с уровнями защищенности
5. Появилось требование по регулярной оценке эффективности мер
6. Закреплена возможность привлечения лицензиатов
7. Отменен Приказ ФСТЭК № 58

Изменилась парадигма выбора мер обеспечения безопасности информации.

ЭЛВИС-ПЛЮС

ВАЖНОЕ ЗАМЕЧАНИЕ

Приказ ФСТЭК России № 21, п. 4

Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия,
в случаях, когда, применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

Пока есть только один легальный способ оценки соответствия: сертификация по требованиям безопасности.

ЭЛВИС-ПЛЮС

ПОДВОДНЫЙ КАМЕНЬ

Приказ ФСТЭК России № 21, п.6

Оценка эффективности реализованных мер по обеспечению безопасности ПДн проводится оператором самостоятельно.

«Под технической защитой конфиденциальной информации понимается выполнение работ и (или) оказание услуг по ее защите... лицензированию подлежат следующие виды работ и услуг: контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации».

пп. 2 и 4 ПП № 79

Оценивать эффективность можно, но имея лицензию на деятельность по ТЗКИ

ЧТО НОВОГО?

Приказ ФСТЭК России № 17:

1. Изменился подход к выбору мер защиты
2. Существенно изменился перечень мер защиты
3. Появились компенсирующие меры по снижению актуальных угроз
4. Изменен порядок классификации ГИС по защищенности
5. Классы СрЗИ увязаны с классами защищенности ГИС
6. Классы защищенности ГИС увязаны с уровнями защищенности ПДн
7. Введена (подтверждена) обязательная сертификация СрЗИ
8. Определен порядок обязательной аттестации ГИС
9. Определены основные угрозы безопасности информации в ГИС
10. Определено содержание модели угроз

Приказ ФСТЭК № 17 аналогичен Приказу ФСТЭК № 21.

ЭЛВИС-ПЛЮС

ЧТО НОВОГО?

Приказ ФСТЭК России дает классификацию основных угроз безопасности информации при нарушении:

- Конфиденциальности
  - неправомерный доступ
  - копирование
  - предоставление или распространение
- Целостности
  - уничтожение
  - модификация
- Доступности
  - блокирование

Организационные и технические меры защиты, реализуемые в рамках системы защиты информации, должны исключать эти угрозы.

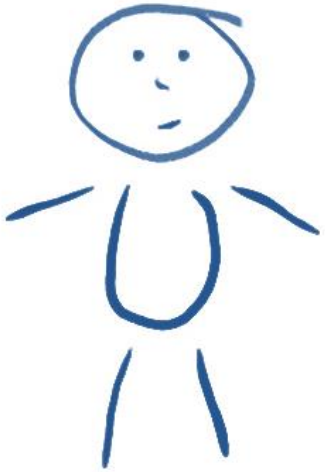
ВАЖНЫЕ ЗАМЕЧАНИЯ

1. СТР-К применяется в качестве методического документа для нейтрализации угроз безопасности информации, связанных с утечками по техническим каналам.

2. Учитывая, что меры по обеспечению безопасности ПДн, установленные Приказом ФСТЭК № 21, аналогичны мерам, Приказа ФСТЭК № 17, для обеспечения безопасности ПДн в ГИС, достаточно руководствоваться только Приказом ФСТЭК № 17.

Издание Приказа ФСТЭК России № 17 не отменяет действие СТР-К и РД по АС.

САМОЕ ВАЖНОЕ – АЛГОРИТМ ВЫБОРА МЕР ЗАЩИТЫ



Точка, точка, запятая, вышла рожица кривая…

(Юлий Ким)

ЭЛВИС-ПЛЮС

САМОЕ ВАЖНОЕ – АЛГОРИТМ ВЫБОРА МЕР ЗАЩИТЫ

Алгоритм выбора мер защиты аналогичен в обоих приказах:

1. Определение перечня актуальных угроз и их типа
2. Выбор уровня защищенности ПДн (класса ГИС)
3. Определение базового набора мер
4. Адаптация набора мер
5. Уточнение перечня мер
6. Дополнение требований

Приказ позволяет довольно гибко подходить к выбору мер защиты.

ЭЛВИС-ПЛЮС

Алгоритм выбора мер защиты

I. Определение базового набора мер осуществляется в соответствии с перечнем мер приведенном в Приказах ФСТЭК России.

II. Адаптация проводится с учетом характеристик ИС и ИТ, особенностей функционирования ИС. (*На этом этапе исключается все то, чего быть не может, потому что не может быть вообще*)

III. Уточнение предполагает выбор компенсирующих мер нейтрализации актуальных угроз для ИС при невозможности технической реализации выбранных мер, экономической не целесообразности их применения или использования новых ИТ *(Каждая компенсирующая мера должна быть обоснована и доказана возможность нейтрализации угрозы)*.

IV. Дополнение предполагает включение мер, обеспечивающих выполнение требований к защите информации, установленных иными нормативными правовыми актами в области обеспечения безопасности информации.

В результате всех действий можно получить ОПТИМАЛЬНЫЙ НАБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ.

ЭЛВИС-ПЛЮС

ВАЖНОЕ ЗАМЕЧАНИЕ

Базовый набор мер определяется с учетом актуальных угроз, определяемых уполномоченными государственными органами (ст. 19, п. 5, ФЗ-152).

Согласно Постановления Правительства РФ2012 г., № 1119, оператор самостоятельно не определяет состав актуальных угроз.
Оператор определяет только тип угроз на основании отраслевой модели (п.7).

Quod licet Jovi, non licet bovi!

ПАРАДОКС СВОБОДЫ ВЫБОРА

Хотели как лучше, а получили как всегда…

(В. С. Черномырдин)

ЭЛВИС-ПЛЮС

ПАРАДОКС СВОБОДЫ ВЫБОРА

Чем больше свободы выбора у оператора при определении состава мер (требований) по защите информации, тем сложнее (дороже) выполнить требования регулятора

ИЛИ

ПОСТРОИТЬ ОПТИМАЛЬНУЮ ЗАЩИТУ ИНФОРМАЦИИ НЕЛЬЗЯ!

Одно из двух:
либо оптимальная, но не соответствующая,
либо не оптимальная, но соответствующая.

ЭЛВИС-ПЛЮС

ПАРАДОКС СВОБОДЫ ВЫБОРА

Потому, что:

X Базовый набор мер защиты
X Адаптируется
X Уточняется
X Дополняется

Уникальный набор мер защиты

Двух одинаковых ИС – нет, каждая уникальна по-своему!
СрЗИ, покрывающих уникальный набор требований защиты – нет!

ЭЛВИС-ПЛЮС

ПАРАДОКС СВОБОДЫ ВЫБОРА

При отсутствии необходимых сертифицированных СрЗИ, в ходе проектирования организуется разработка (доработка) необходимых СрЗИ и их сертификация (*Приказ ФСТЭК № 17, п. 15.1*).

Оператор стоит перед выбором:

либо сертифицировать СрЗИ под свой уникальный (оптимальный) набор мер защиты,

либо «набирать» необходимые функции безопасности из СрЗИ, имеющихся на рынке, но тогда набор не будет оптимальным!

Костюмчик-то от Бриони обойдется гораздо дороже, чем от «Москвашвея»!

ЭЛВИС-ПЛЮС

ПАРАДОКС СВОБОДЫ ВЫБОРА

Берегись, как бы тебе не стать
столь смиренным, чтобы смирение твое
превратилось в глупость.
(Игнатий Лойла)

Что делать?

A. Типизировать объекты с ИС по набору мер защиты.

B. «Привязать» классы защищенности ИС к классам СрЗИ и требованиям к ним.

Первое позволит сформулировать типовой набор мер (требований к СрЗИ) и организовать сертификацию партии или производства СрЗИ по этим требованиям.

Второе позволит существующий набор требований к классам СрЗИ «разложить» по уровням защищенности ИС.

В принципе, именно второе и сделано …

ЭЛВИС-ПЛЮС

В ПОМОЩЬ СТРАЖДУЩИМ

Сам погибай – товарища выручай…

(А В. Суворов)

ЭЛВИС-ПЛЮС

Приказ ФСТЭК России № 21

Соотношение требований к классам СЗИ с уровнями защищенности

Уровень защищённости ПДн	Класс защиты СЗИ								Уровень контроля ПО СЗИ на отсутствие НДВ
	СВТ	САВЗ		СОВ		МЭ			
		Угрозы 2 типа или взаимодействие с сетями МИО	Угрозы 3 типа и отсутствие взаимодействия с сетями МИО	Угрозы 2 типа или взаимодействие с сетями МИО	Угрозы 3 типа и отсутствие взаимодействия с сетями МИО	Угрозы 1 и 2 типа или взаимодействие с сетями МИО	Угрозы 3 типа и отсутствие взаимодействия с сетями МИО		
УЗ-1	Не ниже 5 класса	Не ниже 4 класса		Не ниже 4 класса		Не ниже 3 класса	Не ниже 4 класса		4 уровень
УЗ-2									
УЗ-3									4 уровень (в случае актуальности угроз 2 типа)
УЗ-4	Не ниже 6 класса	Не ниже 5 класса		Не ниже 5 класса		5 класс			-

ЭЛВИС-ПЛЮС

Приказ ФСТЭК России № 17

Соотношение требований к классам СЗИ с классами защищенности ГИС

<table>
<tr><th rowspan="3">Класс защищённости ГИС</th><th colspan="6">Класс защиты СЗИ</th><th rowspan="3">Уровень контроля ПО СЗИ на отсутствие НДВ</th></tr>
<tr><th rowspan="2">СВТ</th><th colspan="2">САВЗ</th><th colspan="2">СОВ</th><th colspan="2">МЭ</th></tr>
<tr><th>Взаимодействие с сетями МИО</th><th>Отсутствие взаимодействия с сетями МИО</th><th>Взаимодействие с сетями МИО</th><th>Отсутствие взаимодействия с сетями МИО</th><th>Взаимодействие с сетями МИО</th><th>Отсутствие взаимодействия с сетями МИО</th></tr>
<tr><td>К1</td><td rowspan="4">Не ниже 5 класса</td><td colspan="2" rowspan="2">Не ниже 4 класса</td><td colspan="2" rowspan="2">Не ниже 4 класса</td><td rowspan="2">Не ниже 3 класса</td><td rowspan="3">Не ниже 4 класса</td><td rowspan="2">Не ниже 4 уровня</td></tr>
<tr><td>К2</td></tr>
<tr><td>К3</td><td colspan="2" rowspan="2">Не ниже 5 класса</td><td colspan="2" rowspan="2">Не ниже 5 класса</td><td rowspan="2">Не требуется</td></tr>
<tr><td>К4</td><td colspan="2">Не ниже 4 класса</td></tr>
</table>

ЭЛВИС-ПЛЮС

Приказ ФСТЭК России № 17

Соотношение классов защищенности ГИС (приказ № 17) с уровнями защищенности ПДн (ПП-1119)

Классы защищенности ГИС (Приказ ФСТЭК № 17)	Уровни защищенности ПДн (ПП-1119)			
	УЗ-1	УЗ-2	УЗ-3	УЗ-4
К1	X	X	X	X
К2		X	X	X
К3			X	X
К4				X

ЭЛВИС-ПЛЮС

ВАЖНОЕ ЗАМЕЧАНИЕ

Требования, введённые Приказами № 17 и № 21, будут применяться к ИС, для которых решение о создании системы защиты будет принято после вступления в силу этих нормативных правовых актов.

ИС, аттестованные (прошедшие оценку эффективности) по требованиям защиты информации до вступления в действие Требований, утвержденных приказами ФСТЭК России N 17 и N 21, повторной аттестации (оценке эффективности) не подлежат.

СПАСИБО ЗА ВНИМАНИЕ!

vsv@elvis.ru

@vsv_elvis