s·terra®

Ваш ориентир в мире безопасности

Обзор законодательства по защите персональных данных. Критерии выбора средств защиты информации

Владимир Чернышев

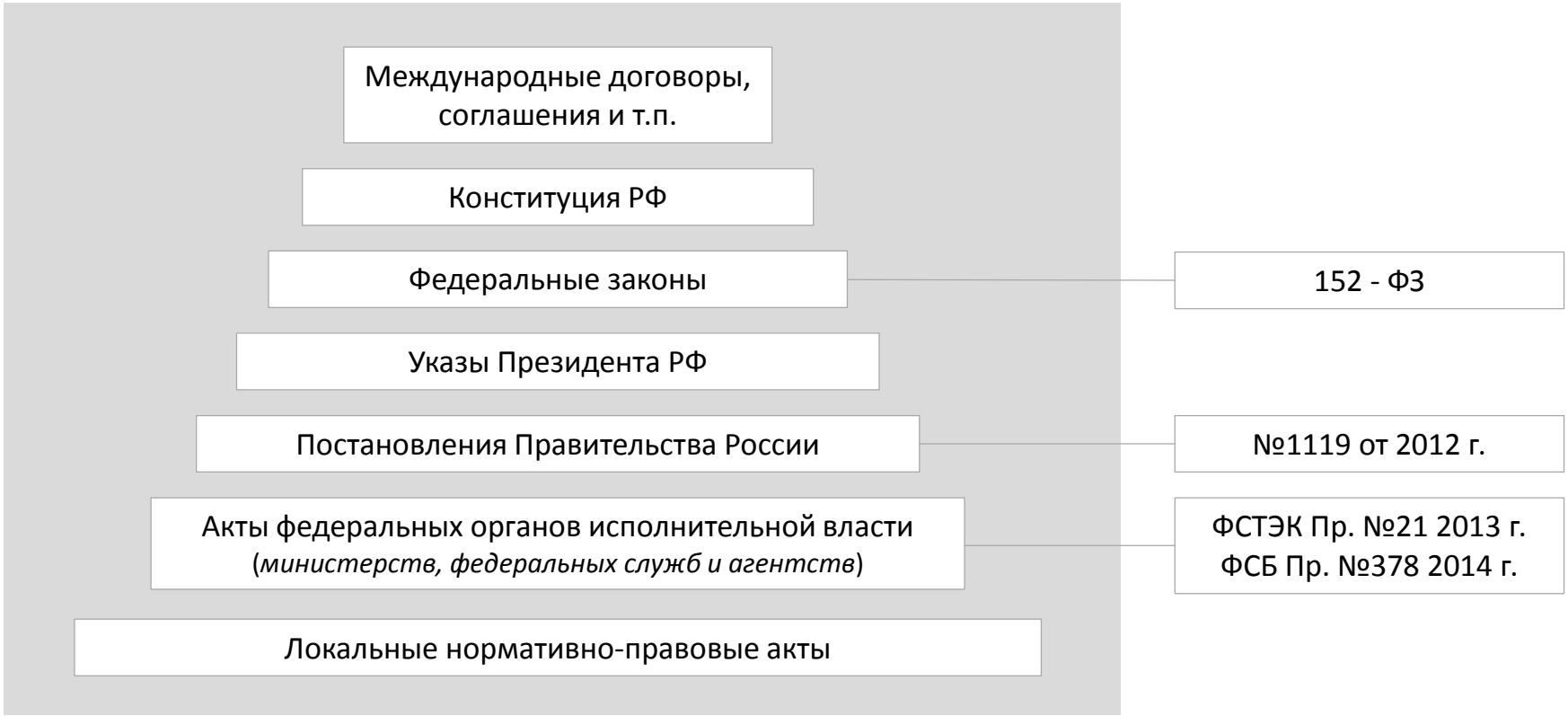
Ведущий менеджер
по работе с заказчиками

www.s-terra.ru

План вебинара

- Структура законодательства по защите ПДн.
  О чем будем говорить.
- Федеральный закон «О персональных данных».
- Постановление Правительства Российской Федерации
  от 1 ноября 2012 г. №1119.
- Приказ ФСТЭК от 18 февраля 2013 г. N 21.
- Приказ ФСБ России от 10 июля 2014 г. N 378.
- Использование продуктов С-Терра в ИСПДн.

Иерархия нормативных правовых актов



Федеральный закон

«О защите персональных данных»

№152-ФЗ, 2006 г.

Что защищаем?

ПДн, ПДн специальные и биометрические.

От чего и как защищаем?

Угрозы безопасности, уровни защищенности и требования к защите ПДн.

Кто устанавливает уровни защищенности и требования к защите ПДн?

Правительство Российской Федерации.

Кто отвечает за обеспечение безопасности ПДн?

Оператор ПДн. Лицо, которому оператором поручена обработка ПДн.

Федеральный закон

«О защите персональных данных»

№152-ФЗ, 2006 г.

Что необходимо делать оператору?

Принимать необходимые и достаточные меры:

- Определение угроз безопасности ПДн
- Применение технических и организационных мер для обеспечения требуемого уровня защищенности (*состав и содержание мер определяют ФСТЭК и ФСБ*)
- Выбор СЗИ в соответствии с нормативными правовыми актами ФСТЭК и ФСБ
- Применение СЗИ, прошедших процедуру оценки соответствия
- Оценка эффективности принимаемых мер
- и ряд других

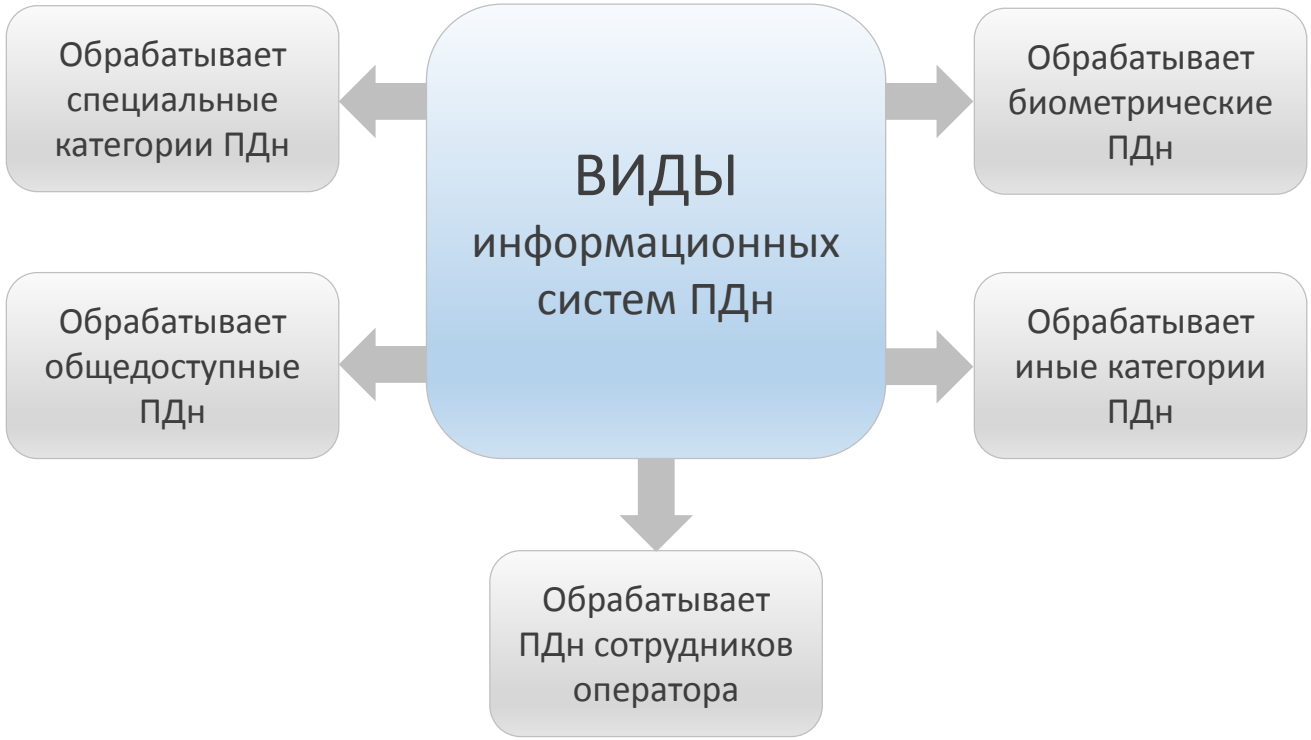
Постановление Правительства РФ №1119, 2012 г.

Утверждены «Требования к защите персональных данных при их обработке в информационных системах персональных данных».

Система защиты ПДн должна:

- нейтрализовать актуальные угрозы
- включать в себя организационные и/или технические меры
- использовать СЗИ, выбранные оператором в соответствии с нормативными правовыми актами ФСБ и ФСТЭК

Постановление Правительства РФ №1119, 2012 г.



Постановление
Правительства РФ
№1119, 2012 г.

ТИПЫ
актуальных угроз

1-го типа. Связаны с наличием НДВ в системном ПО

2-го типа. Связаны с наличием НДВ в прикладном ПО

3-го типа. Не связаны с НДВ в системном и прикладном ПО

Постановление Правительства РФ №1119, 2012 г.

Тип ИС, обрабатываемые ПДн	ПДн сотрудников оператора	Кол-во субъектов ПДн	Требуемый уровень защищенности		
			для 1 типа актуальных угроз	для 2 типа актуальных угроз	для 3 типа актуальных угроз
ИСПДн-С Специальные	нет	>100 000	УЗ-1	УЗ-1	УЗ-2
	нет	<100 000	УЗ-1	УЗ-2	УЗ-3
	да	Любое			
ИСПДн-Б Биометрические	да/нет	Любое	УЗ-1	УЗ-2	УЗ-3
ИСПДн-И Иные	нет	>100 000	УЗ-1	УЗ-2	УЗ-3
	нет	<100 000	УЗ-2	УЗ-3	УЗ-4
	да	Любое			
ИСПДн-О Общедоступные	нет	>100 000	УЗ-2	УЗ-2	УЗ-4
	нет	<100 000	УЗ-2	УЗ-3	УЗ-4
	да	Любое	УЗ-2	УЗ-3	УЗ-4

Постановление Правительства РФ №1119, 2012 г.

УЗ-4

- Организация режима обеспечения безопасности помещений, в которых размещена ИСПДн
- Обеспечение сохранности носителей ПДн
- Утверждение документа, определяющего перечень допущенных к ПДн лиц
- Использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства в области ИБ, если их применение необходимо для нейтрализации актуальных угроз

УЗ-3

+ назначение должностного лица, ответственного за обеспечение безопасности ПДн в ИСПДн

УЗ-2

+ ограничение доступа к электронному журналу сообщений (*исключительно работниками, которым сведения из этого журнала необходимы для выполнения служебных обязанностей*)

УЗ-1

+ автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн в ИСПДн;

+ создание структурного подразделения, ответственного за обеспечение безопасности ПДн в ИСПДн

Приказ ФСТЭК
№21, 2013 г.

Содержит состав мер по обеспечению безопасности ПДн

Выбор мер включает :

- Определение базового набора мер;
- Адаптацию базового набора мер;
- Уточнение адаптированного базового набора мер;
- Дополнение уточненного адаптированного базового набора мер;
- Разработка иных (компенсирующих) мер.

Состав и содержание мер для каждого из уровней защищенности приведены в приложении к приказу.

Требования по классам защиты и уровням контроля

s•terra

	УЗ-4	УЗ-3	УЗ-2	УЗ-1
СОВ и средства антивирусной защиты (*класс, не ниже*)	6 5	5 4 акт. угрозы 2 типа или есть МИО*	5 4 4	
		5 акт. угрозы 3 типа и нет МИО		
МЭ (*класс, не ниже*)	6 5	6 3 акт. угрозы 2 типа или есть МИО	5 3 4 акт. угрозы 1 или 2 типов, или есть МИО	
		4 акт. угрозы 3 типа и нет МИО	4 акт. угрозы 3 типа и нет МИО	
ПО СЗИ (*уровень контроля НДВ, не ниже*)	–	4 акт. угрозы 2 типа	4	

– требования приказа ФСТЭК №21, 2013 г.

– требования по проекту нового приказа ФСТЭК

– требования приказа ФСТЭК №9 от 09.02.2016 г.

* МИО – международный информационный обмен

Приказ ФСБ

№378, 2014 г.

Утвердил состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ.

Для каждого из УЗ ПДн должны применяться СКЗИ соответствующего класса.

Класс СКЗИ определяется исходя из совокупности предположений о возможностях для создания способов, подготовке и проведении атак, и типа актуальных угроз безопасности ПДн.

Приказ ФСБ

№378, 2014 г.

Требуемый уровень защищенности								Требуемый класс СКЗИ
4	**3**		**2**			**1**		
+)	+) угрозы **3** типа	+) угрозы **2** типа	+) угрозы **3** типа	+) угрозы **2** типа	угрозы **1** типа	+) угрозы **2** типа	угрозы **1** типа	КА
+)	+) угрозы **3** типа	+) угрозы **2** типа	+) угрозы **3** типа	+) угрозы **2** типа	–	+) угрозы **2** типа	–	КВ
+)	+) угрозы **3** типа	–	+) угрозы **3** типа	–	–	–	–	КС3
+)	+) угрозы **3** типа	–	+) угрозы **3** типа	–	–	–	–	КС2
+)	+) угрозы **3** типа	–	+) угрозы **3** типа	–	–	–	–	КС1

+) — исходя из возможностей нарушителя при создании способов, подготовке и проведении атаки

Выбор СЗИ/СКЗИ для защиты ПДн

по критерию необходимого класса/уровня сертификации

- Определить, какие ПДн/в каком количестве обрабатываются в ИС
- Определить тип актуальных угроз
- На основании этих данных определить требуемый уровень защищенности ПДн

- По требуемому уровню защищенности определить требуемые классы/уровни сертификации СЗИ
- Выбрать СЗИ

- Сформировать и утвердить совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак

- По требуемому уровню защищенности, типу актуальных угроз и предположениях о возможностях при создании способов, подготовке и проведении атак определить требуемые класс СКЗИ
- Выбрать СКЗИ соответствующего класса

VPN C-Терра

s•terra

- IPsec VPN с ГОСТ-алгоритмами
- Встроенный межсетевой экран
- СОВ (с версии 4.2)
- Централизованное удаленное управление
- Большой выбор аппаратных платформ

ФСБ России:	КС1, КС2, КС3, МЭ4
ФСТЭК России:	НДВ3, МЭ3, ОУД4+

Применение для защиты ПДн продуктов С-Терра

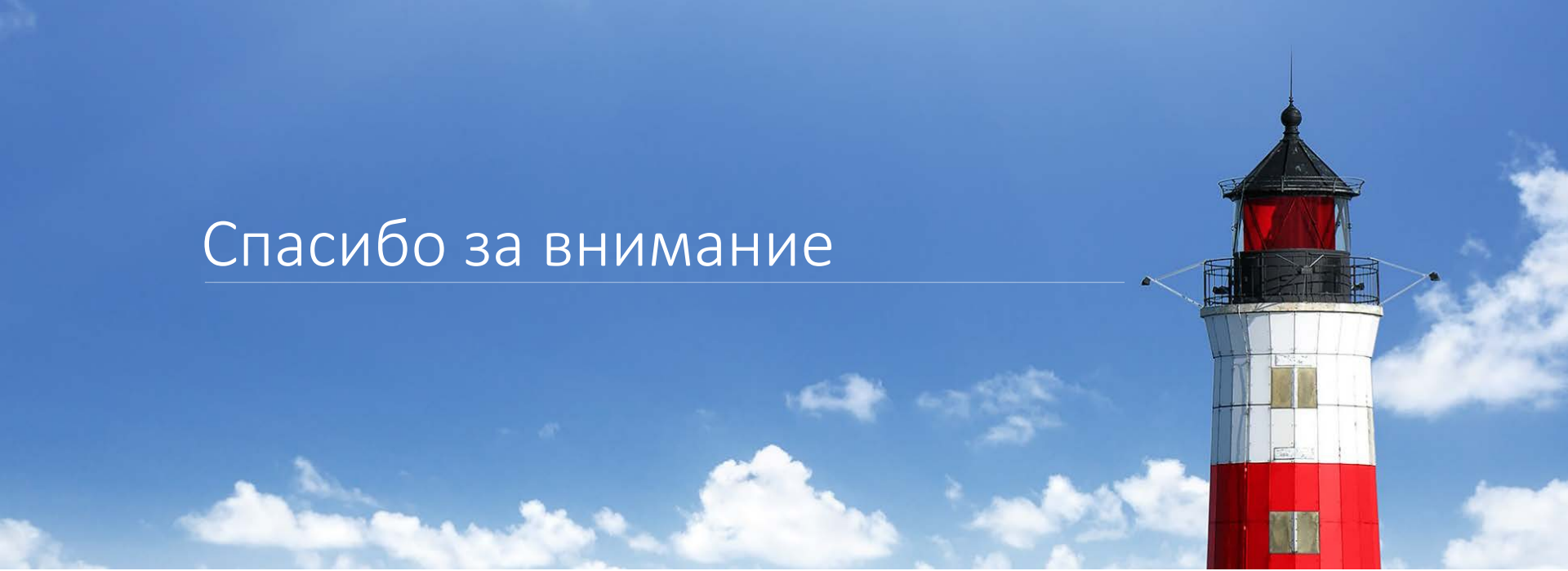
Область применения	Продукт С-Терра	Уровни защищенности
Криптозащита удаленного доступа к ресурсам ИС	С-Терра Шлюз, С-Терра Виртуальный Шлюз, С-Терра «Пост», С-Терра Клиент, С-Терра Клиент-М	УЗ-2 — УЗ-4
Межсетевое экранирование	С-Терра Шлюз, С-Терра Виртуальный Шлюз, С-Терра «Пост», С-Терра Клиент	УЗ-1 — УЗ-4
Защита от вторжений	СОВ (с версии 4.2)	УЗ-1 — УЗ-4

Продукт С-Терра VPN Е для трансграничной передачи ПДн

Область применения	Исполнения
Эксплуатация за пределами Российской Федерации	- С-Терра Шлюз Е, С-Терра Виртуальный Шлюз Е - С-Терра Клиент Е

Сертификаты ФСБ России:

- №СФ/114-3074 от 06.03.2017
- №СФ/114-3075 от 06.03.2017



Спасибо за внимание

Владимир Чернышев,
ведущий менеджер по работе с заказчиками

+7 (499) 940 9001, доб.177
vch@s-terra.ru

s•terra®