s•terra

# ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

## Глоссарий

**ПДн** – персональные данные

**ИС** – информационная система

**ИСПДн** – информационная система персональных данных

**СКЗИ** – средство криптографической защиты информации

**УЗ** – уровень защищенности

**СПО** – специальное программное обеспечение

**ППО** – прикладное программное обеспечение

## Введение

После множества переносов 1 января 2011 года вступил в силу Федеральный закон от 27.07.2006 года №152 «О персональных данных» и начали действовать санкции за неисполнение требований (административная и уголовная ответственность). Основная цель закона – защитить права и свободы граждан при обработке личной информации, в том числе право на неприкосновенность частной жизни, личную и семейную тайну.

Федеральный закон обязал операторов персональных данных «принимать необходимые организационные и технические меры для защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий». Для обеспечения реализации положений Федерального закона выпущены следующие документы:

- Постановление Правительства РФ от 01.11.2012 г. № 1119[1], которое определяет классификацию ИСПДн, возможных угроз и уровней защищенности ПДн;
- Приказ ФСТЭК России от 18.02.2013 г. № 21[2], определяющий перечень мер защиты, которые должны быть реализованы в зависимости от уровня защищенности ИСПДн для нейтрализации актуальных угроз, а также требования к сертификации применяемых средств защиты информации.
- Приказ ФСБ России от 10.07.2014 г. № 378[3], определяющий состав организационных и технических мер, которые необходимо реализовывать при применении в ИСПДн средств криптографической защиты информации. Документ также содержит требования к классу защиты СКЗИ в зависимости от уровня защищенности ПДн.

[1] Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

[2] 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»

[3] Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

***Определено 4 группы обрабатываемых ПДн:***

1 группа - специальные категории ПДн, к которым относится информация о национальной и расовой принадлежности субъекта, о религиозных, философских, либо политических убеждениях, информация о здоровье и интимной жизни субъекта;

2 группа - биометрические ПДн, данные, характеризующие биологические или физиологические особенности субъекта, например фотография или отпечатки пальцев;

3 группа - общедоступные ПДн, сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

4 группа - иные категории ПДн, не представленные в предыдущих группах.

Под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в ИС, результатом – которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия.

***Угрозы подразделяются на 3 типа:***

1 тип - Актуальны для ИС, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в СПО, используемом в ИС.

2 тип - Актуальны для ИС, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в ППО, используемом в ИС.

3 тип - Актуальны для ИС, если для нее актуальны угрозы, не связанные с наличием НДВ.

Определено 4 уровня защищённости (УЗ) персональных данных (представлены в таблице 1), различающихся перечнем необходимых к выполнению требований и устанавливаемых в зависимости от категории обрабатываемых персональных данных, типа актуальных угроз и числа субъектов персональных данных.

*Таблица 1. Уровни защищенности (УЗ) персональных данных*

| **Тип ИС** | **Сотрудники оператора** | **Кол-во субъектов** | **Тип актуальных угроз** | | |
|---|---|---|---|---|---|
| | | | **1** | **2** | **3** |
| 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 |

## Решение С-Терра по защите ПДн

Продукты компании С-Терра, сертифицированные регуляторами – ФСБ России и ФСТЭК России, позволяют обеспечить защиту персональных данных в ИСПДн любого уровня защищенности.

*Таблица 2. Применение продуктов С-Терра для защиты ПДн разных УЗ*

| Область применения | Продукт | УЗ-1 | УЗ-2 | УЗ-3 | УЗ-4 |
|---|---|---|---|---|---|
| Криптографическая защита удаленного доступа к ресурсам ИС | С-Терра Шлюз, С-Терра Виртуальный Шлюз, МСМ-950, С-Терра «Пост», С-Терра Клиент, С-Терра Клиент-М | - | + | + | + |
| Межсетевое экранирование | С-Терра Шлюз, С-Терра Виртуальный Шлюз, МСМ-950, С-Терра «Пост», С-Терра Клиент | + | + | + | + |
| Защита от вторжений | С-Терра СОА* | + | + | - | - |

*- в процессе сертификации. Срок – 3q2016

## Преимущества решения С-Терра

- Проверенный производитель
- Использование стандартных протоколов
- Поддержка ГОСТ алгоритмов шифрования
- Интеграция в существующую инфраструктуру (в том числе в виртуальную)
- Сертификация ФСБ и ФСТЭК России
- Высокая экономическая эффективность

## Рекомендации по выбору

Рассмотрим несколько типовых вариантов использования продуктов С-Терра для защиты ИСПДн.

### 1. Защита взаимодействия нескольких территориально распределённых компонентов ИСПДн

В центральной точке устанавливается шлюз безопасности – С-Терра Шлюз, который обеспечивает межсетевое экранирование и терминирует защищенные туннели с удаленными объектами. Конкретная модель выбирается из линейки шлюзов, исходя из требований по производительности, параметров аппаратной платформы и необходимого класса защиты. Для повышения отказоустойчивости центрального объекта может быть установлено два шлюза в кластере «горячего» резервирования. Рекомендуем использовать систему централизованного управления С-Терра КП. В удаленных объектах также устанавливается С-Терра Шлюз, но, как правило, более младшей модели. Если количество рабочих мест в удаленном объекте менее 5, то целесообразно рассмотреть С-Терра Клиент или С-Терра «Пост» для каждого рабочего места.

**Пример**

- *Условия:* Организация состоит из головного офиса и 20 филиалов. Связь филиалов с головным офисом осуществляется через недоверенную сеть - интернет. В головном офисе развернута база данных, содержащая ПДн, к которой необходим доступ из филиалов. Канал в головном офисе 100 Мбит/с, в филиалах – по 10 Мбит/с. В каждом филиале более 10 сотрудников со стационарными рабочими местами на ОС Windows.
- *Требуется:* защитить ПДн при их передаче через недоверенную сеть в соответствии с законодательством. В головном офисе требуется резервирование оборудования. Класс защиты по линии ФСБ России – КС2.
- *Решение:*

  В центре рекомендуется использовать:
  - Кластер из шлюзов безопасности С-Терра Шлюз 1000: *2x G-1000M-D-4120-4-ST-KC2*
  - Систему управления С-Терра КП на 100 лицензий: *1x KP-100-D*

  В филиалах рекомендуется установить:
  - Шлюзы безопасности С-Терра Шлюз 100: *20x G-100-D-4107-2-ST-KC2*

  Актуальные цены доступны в прайс-листе, размещенном на сайте компании.

### 2. Защита удаленного доступа к ресурсам ИСПДн

В центральной точке устанавливается шлюз безопасности – С-Терра Шлюз, который обеспечивает межсетевое экранирование и терминирует защищенные туннели с удаленными объектами. Конкретная модель выбирается исходя из требований по производительности, параметров аппаратной платформы и необходимого класса защиты. Для повышения отказоустойчивости центрального объекта может быть установлено два шлюза в кластере «горячего» резервирования. Опционально может использоваться система централизованного управления. Для защиты доступа удаленных пользователей на их рабочие станции устанавливается С-Терра Клиент или С-Терра «Пост», а также С-Терра Клиент-М для мобильных устройств.

**Пример**

- *Условия:* В организации развернута база данных, содержащая ПДн, к которой необходим доступ удаленных сотрудников, работающих вне офиса. Сотрудники используют ноутбуки с ОС Windows – 20 человек и планшеты с ОС Android – 10 человек. Канал в головном офисе 100 Мбит/с.
- *Требуется:* защитить ПДн при их передаче через недоверенную сеть в соответствии с законодательством. Резервирование не требуется. Класс защиты по линии ФСБ России – КС1.
- *Решение:*

  В центре рекомендуется использовать:
  - Шлюз безопасности С-Терра Шлюз 1000: *1x G-1000M-D-4120-4-ST-KC1*
    или С-Терра Виртуальный Шлюз: *1x VG-C4-ST-KC1*
  - Систему управления С-Терра КП на 100 лицензий: *1x KP-100-D*

  Удаленным пользователям рекомендуется установить:
  - Клиент безопасности С-Терра Клиент: *10x C-X-WIN-D-ST-KC1*
  - Клиент безопасности С-Терра Клиент-М: *20x C-M-AND-KC1*

Актуальные цены доступны в прайс-листе, размещенном на сайте компании.

### 3. Другие варианты

Возможны различные комбинации предыдущих случаев и изменение параметров в них, по всем вопросам обращайтесь в отдел технического консалтинга presale@s-terra.com

## О компании «С-Терра СиЭсПи»

ООО «С-Терра СиЭсПи» основано в 2003 году и является ведущим российским разработчиком и производителем средств сетевой информационной безопасности.

Компания «С-Терра СиЭсПи» предлагает органично входящие в сетевую инфраструктуру решения, которые используют протокол IPsec и российские сертифицированные криптографические алгоритмы. Решения характеризуются отличной масштабируемостью, надежностью и рекордной производительностью, что обеспечивает высокую экономическую эффективность.

Продукты и решения С-Терра обеспечивают защиту каналов связи любой производительности (как на сетевом, так и на канальном уровне), безопасный удаленный доступ, в том числе с мобильных платформ, а также предоставляет эффективное управление VPN-инфраструктурой С-Терра.

Продукты С-Терра сертифицированы ФСТЭК России и ФСБ России, в том числе как средства криптографической защиты информации (СКЗИ) по классу КС1, КС2, КС3.

Компания является первым российским технологическим партнером Cisco (Cisco Solution Technology Integrator), Серебряным партнером Samsung и Авторизованным партнером Huawei.

Партнерская сеть компании "С-Терра СиЭсПи" состоит из более чем 300 компаний, включая всех крупнейших российских системных интеграторов. Имеется представительство компании в Республике Беларусь.

Более подробную информацию о компании можно получить на сайте: http://www.s-terra.com/about/