Центр регистрации доменов

Принципы безопасной обработки персональных данных клиентов интернет-магазина

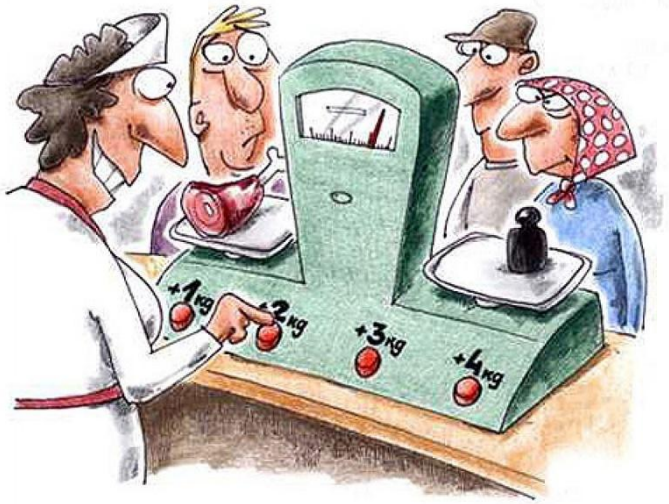
Олег Педько,

Руководитель проектов,
Департамент развития услуг

Москва,
11.10.2012

www.nic.ru

Буква закона



Интернет-магазины – субъект 152-ФЗ «О персональных данных»

С какими ПДн работают интернет-магазины?

- **ФИО**
- **Номера телефонов**
- **Адреса электронной почты**
- **Адреса доставки**

… и не только

Категории ПДн

ОПРЕДЕЛЕНИЯ

Категория 4	Категория 3	Категория 2	Категория 1
Обезличенные и (или) общедоступные ПДн	ПДн, позволяющие определить субъекта ПДн	ПДн позволяют определить субъекта ПДн и получить о нем доп. информацию, за исключением ПДн категории 1	ПДн касаются расовой, нац. принадлежности, политических взглядов, религиозных и философских убеждений, здоровья, интимной жизни

ПРИМЕРЫ

Категория 4	Категория 3	Категория 2	Категория 1
ФИО Email	ФИО Email Серия и номер паспорта	ФИО Email Серия и номер паспорта Почтовый адрес	ФИО Email Серия и номер паспорта Почтовый адрес Вероисповедание Национальность Состояние в браке Наличие детей

Кто контролирует?

ФСБ, ФСТЭК, РОСКОМНАДЗОР

Проверки Роскомнадзора:

- **Плановые (график есть на сайте Роскомнадзора)**
- **Внеплановые (уведомление за сутки до начала проверки)**

Причины: требования прокуратуры, жалобы физических лиц

2011 год

- **Внеплановые проверки > плановые**

Ответственность

- **Штрафы**
  - **до 500 тыс. руб. штрафа для юридического лица**
  - **до 50 тыс. руб. штрафа для руководителя юридического лица**
- **Приостановка деятельности юр. лица на срок до 90 дней**

… и это только начало

Длинный список (1)

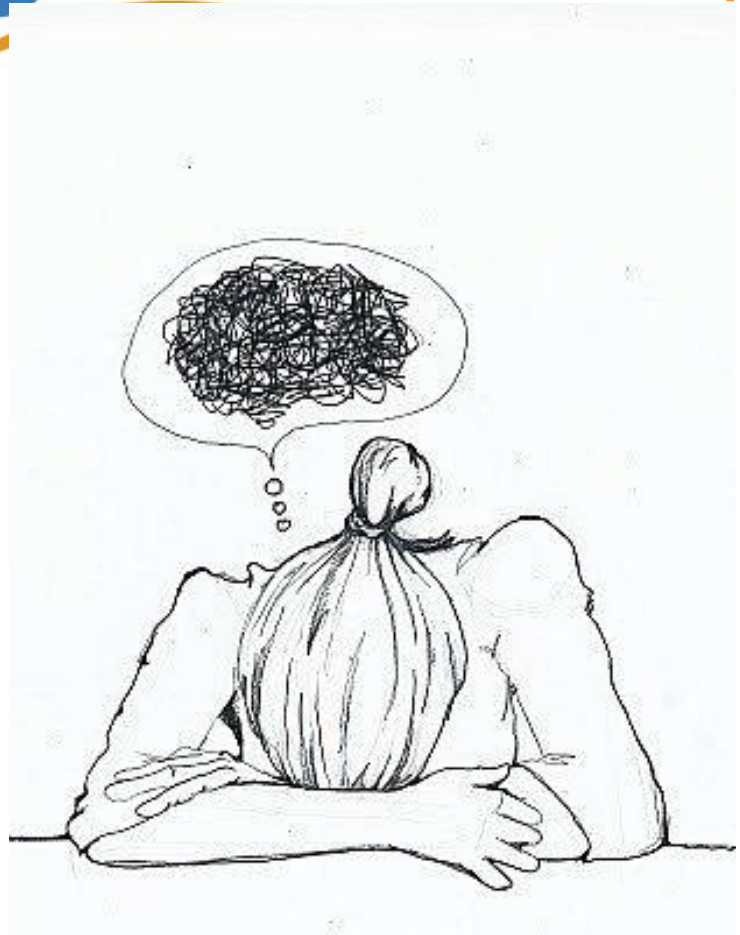
Что необходимо сделать для правильной обработки персональных данных?

- **Сформировать рабочую группу по приведению порядка обработки ПДн в соответствие с законом**
- **Проанализировать ПДн, обрабатываемые в ИС**
- **Провести аудит бизнес-процессов и ИС**
- **Разработать модели угроз**
- **Классифицировать ИСПДн**
- **Разработать ТЗ на ИСПДн**

Длинный список (2)

- Разграничить доступ к ПДн
- Спроектировать и внедрить систему защиты ПДн
- Зарегистрироваться в Роскомнадзоре в качестве оператора ПДн
- Получить от клиентов и сотрудников согласие на обработку их ПДн
- Осуществлять рекламную рассылку или продвигать товары клиентам только с их согласия
- Ограничить передачу ПДн третьим лицам

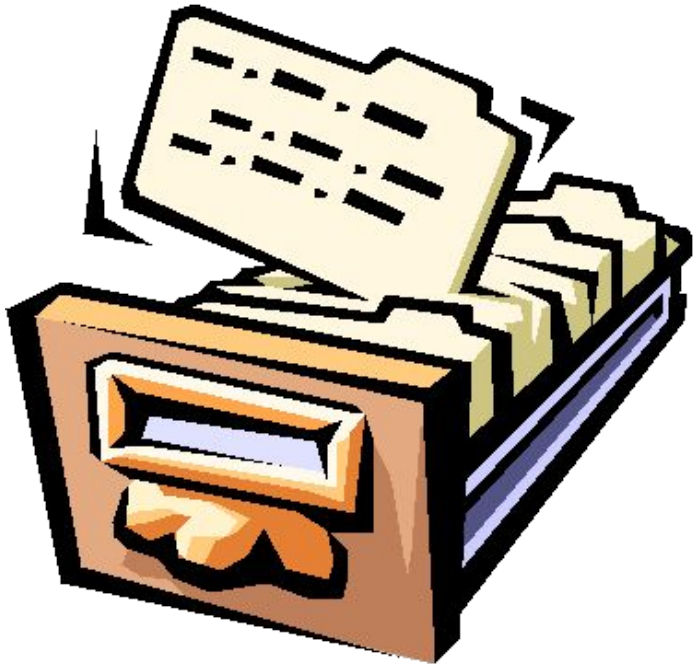
Длинный список (3)



- Правильно взаимодействовать с клиентом по вопросам ПДн
- Составить пакет инструкций и регламентов по ПДн
- Назначить ответственных лиц за организацию обработки ПДн
- Обучить сотрудников правильной обработке ПДн
- Разработать и опубликовать в общем доступе политику обработки ПДн

Что еще?

Договор с курьерской службой о безопасной обработке ПДн



Средства защиты ПДн

- Межсетевой экран
- Антивирус
- Средства защиты от несанкционированного доступа
- Системы обнаружения вторжений и анализа защищенности
- Средства криптографической защиты

Сертифицировано ФСТЭК, ФСБ РФ

Рецепты успеха

- *ИСПДн своими силами*
- *ИСПДн на заказ*

Крупные компании с большим бюджетом

- *Комбинированный подход*

Малый и средний бизнес

Комплексный подход: преимущества

Использование универсальных готовых решений, имеющихся на рынке

=

Экономия средств и времени

Автоматизированные сервисы по подготовке документов для обработки ПДн

- Гибкость
- Подготовка к проверкам
- Финансовые гарантии

+

Хостинг конфиденциальной информации

- Размещение оборудования в специальной зоне дата-центра
- Оборудование, межсетевой экран и антивирус сертифицированы ФСТЭК
- Ведение учета носителей информации
- Ежедневное резервное копирование данных (две копии)

SSL-сертификат – компонент защиты ПДн клиентов магазина

Где рекомендуется устанавливать сертификаты?

- **В тех разделах сайта, где пользователи вводят и хранят ПДн и другие конфиденциальные данные**

  Личные кабинеты, страницы оплаты товара и др.

SSL = ДОВЕРИЕ

Категории SSL-сертификатов

DV

Domain validation

- Удостоверяет только домен
- Шифрование соединения
- Выпускается в течение 1 дня
- Иконка замка в браузере

OV

Organisation validation

- Удостоверяет домен и организацию, которой он принадлежит
- Данные о компании отображаются в сертификате
- Голубая строка браузера (Firefox)
- Выпускается в течение 3-5 дней

WILDCARD SAN

Мультидоменные сертификаты

- Сертификаты защищают несколько доменов
- Принадлежность каждого домена организации, запрашивающей сертификат, проверяется отдельно
- Выпускается в течение 7-10 дней

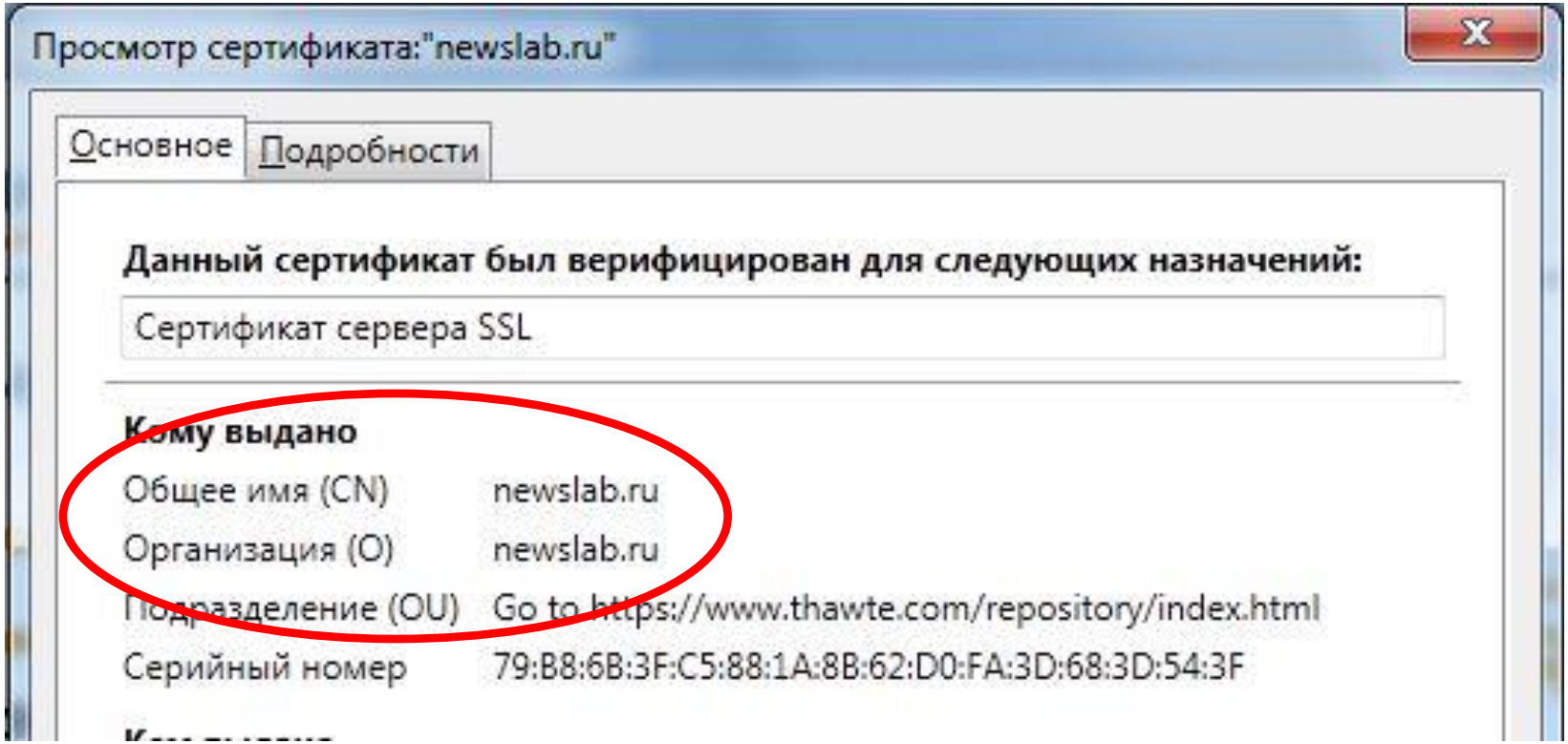
EV

Extended validation

- Расширенная проверка данных для выпуска сертификата (устав, свидетельство о регистрации в налоговом органе и пр.)
- Зеленая строка браузера (все браузеры)
- Выпускается в течение 7-14 дней

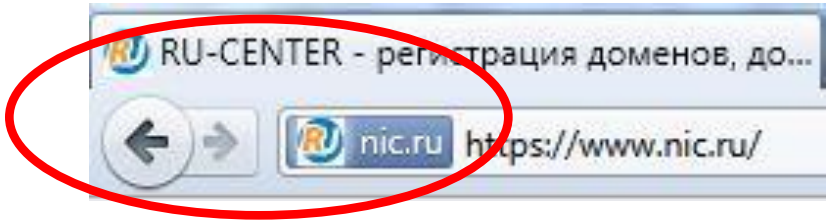
Как выглядит сертификат в браузере? (1)

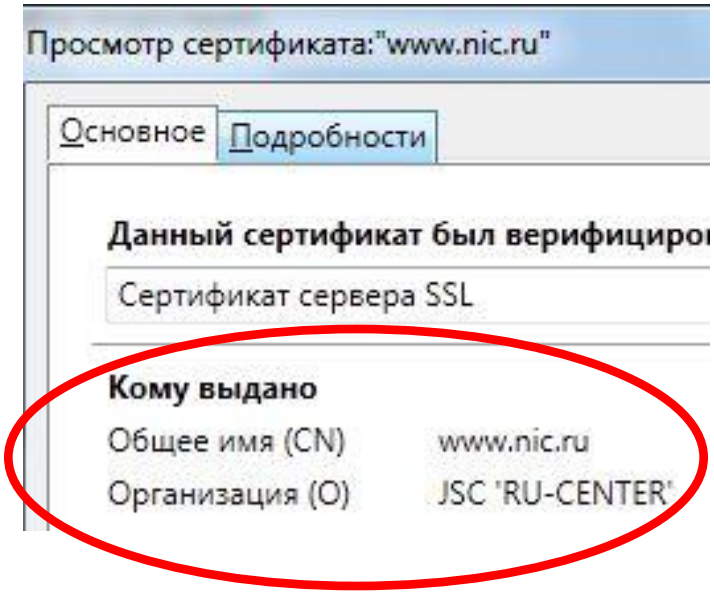
Сертификаты категории DV



Как выглядит сертификат в браузере? (2)

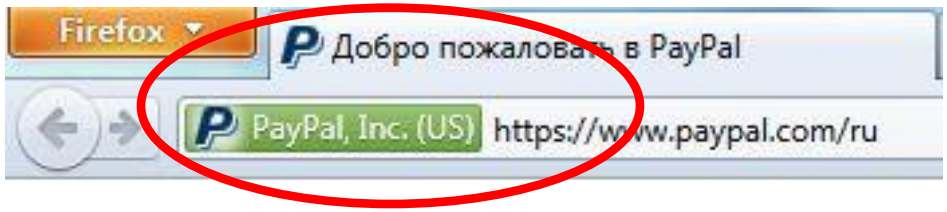
Сертификаты категорий OV, SAN, WILDCARD

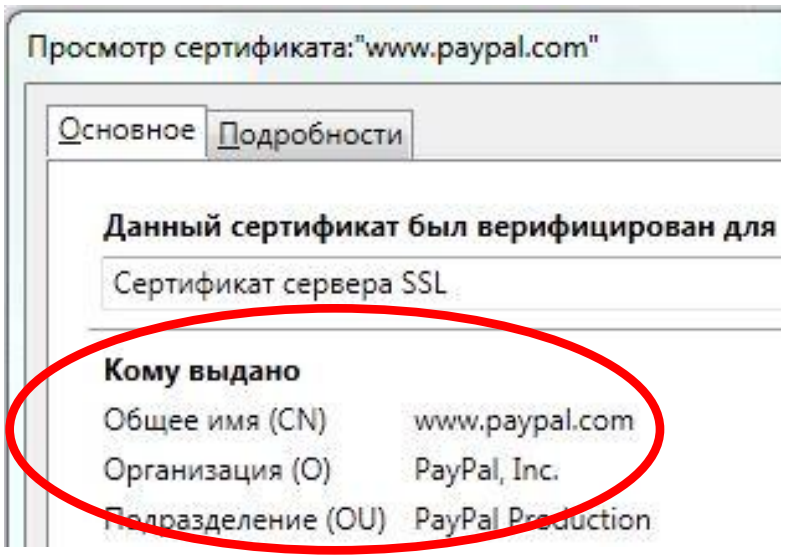




Как выглядит сертификат в браузере? (3)

Сертификаты категории EV





Спасибо за внимание!

Вопросы?

e-mail: pr@nic.ru
web: www.nic.ru
ник.рф
www.ssl.ru