Опыт реализации требований PCI DSS в электронной коммерции

2016 г.

Wildberries — один из крупнейших интернет-магазинов России

Более
4 тыс.
брендов
на сайте

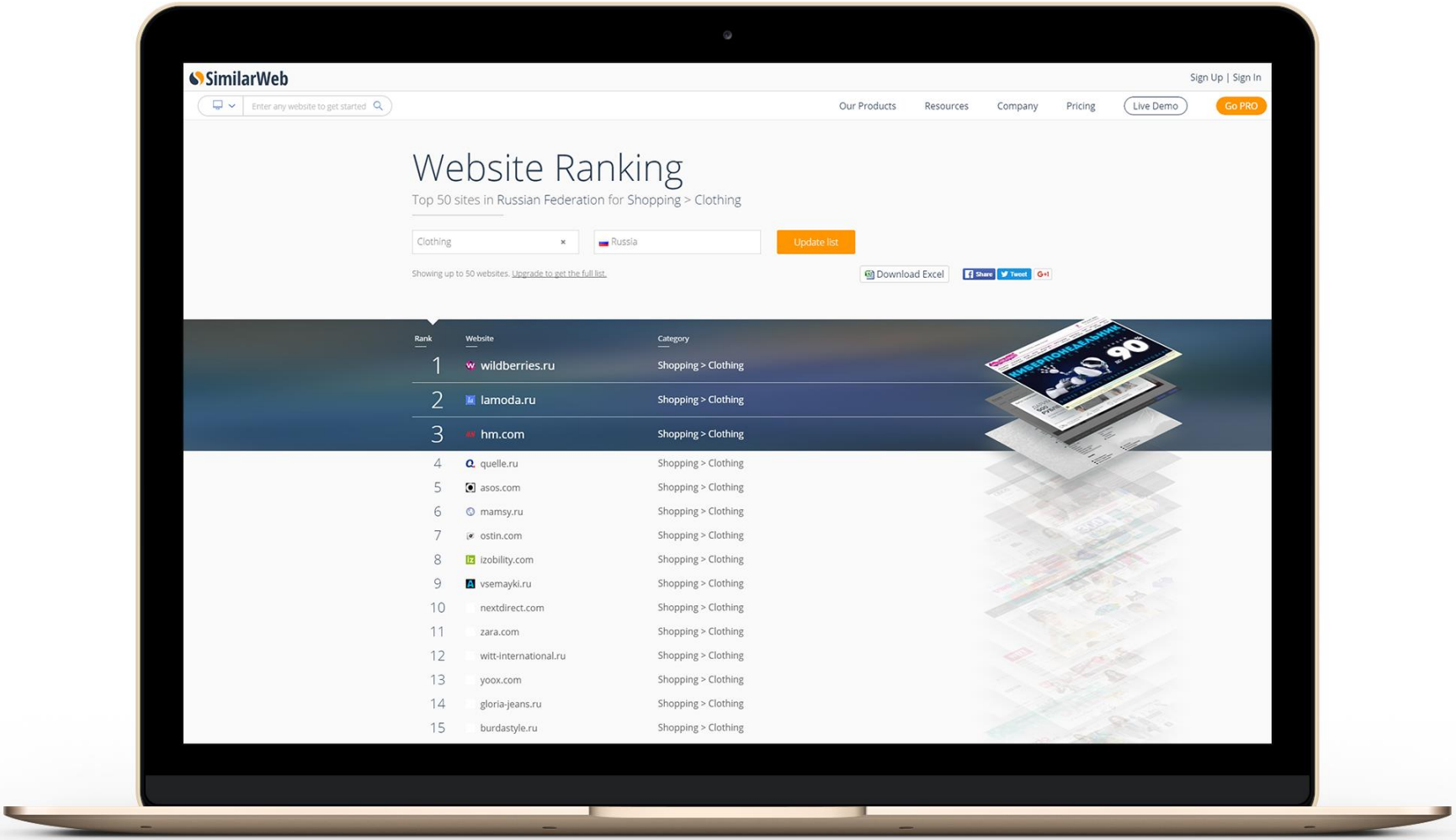
Более
100 тыс.
заказов
в день

Более
1 млн.
посетителей
в день

Более
8 млн.
товаров
на складе

2. Наши клиенты

3. Самый посещаемый интернет-магазин России*



* Согласно международному online-сервису исследования интернет-трафика Similar Web: www.goo.gl/cqzEpf

4. Что предлагает рынок QSA-аудита?

- В 2015 году 10 компаниям из перечня QSA-аудиторов с сайта PCI SSC был направлен запрос коммерческих предложений.
- В 2016 году 3 компании из 10 претендентов отсутствуют в списках QSA-аудиторов.

5. Организационные и технические особенности при реализации требований стандарта PCI DSS

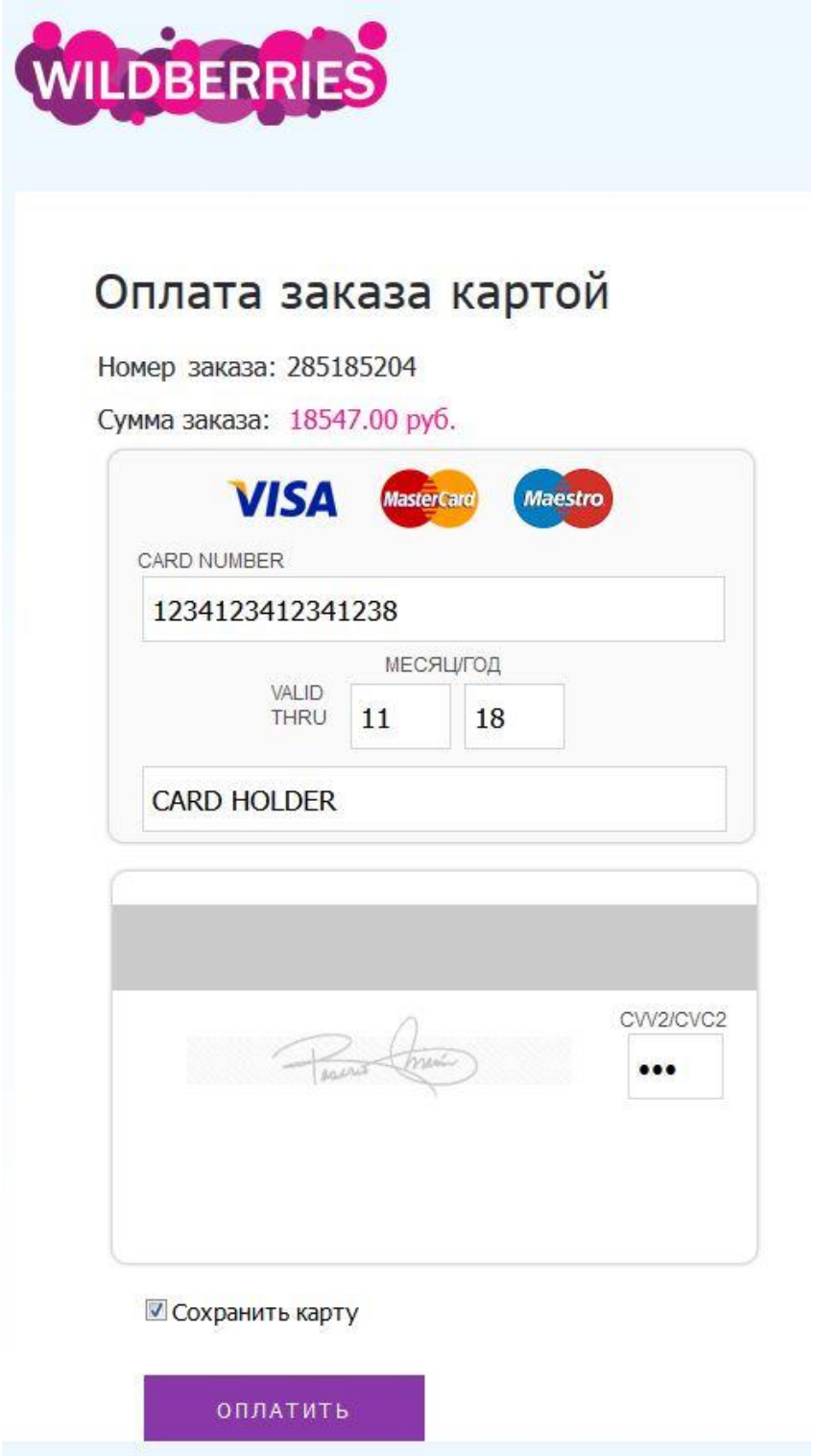
- А банки понимают требования стандарта?! Матрица ответственности и служба безопасности банка.

- Беспечность клиентов или обработка инцидентов по обнаружению карточных данных:
  - Постоянный анализ и чистка почтовых серверов;
  - Постоянный анализ и чистка сервисов обработки обращений клиентов;
  - Информирование клиентов о недопустимости пересылки карточных данных.

- Не отказывайтесь от технической поддержки при реализации проекта и предварительного QSA-аудита. Первый поможет разобраться в деталях, а второй увидеть все недосмотры, что в сумме значительно приблизит вас к достичь положительного результата при сертификационном QSA-аудите

- При реализации проекта силами собственных специалистов, необходимо учитывать внешние и внутренние факторы влияющие на сроки:
  - Выбор, поставка и настройка импортного оборудования;
  - Подписание матриц ответственности с третьими лицами;
  - Большой объем организационной информации, обучение кадров и мотивация;
  - Разработка собственного платежного приложения.

6. Форма оплаты

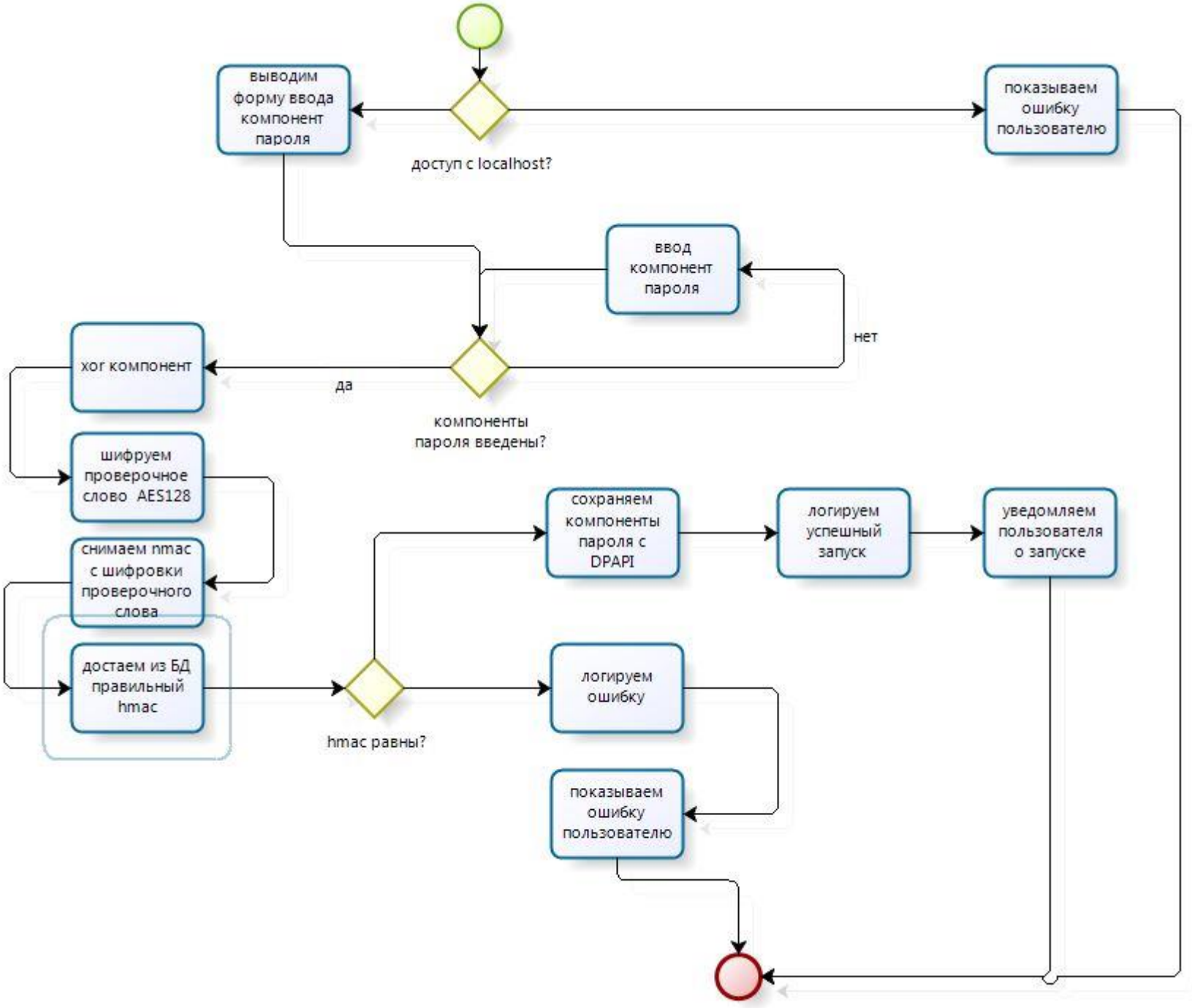


алгоритм Луна
ограничение рамок для года
скрытие CCV
расширенный CH
сверка IP

7. Смена пароля шифрования

1. Три ответственных лица – по одному на каждую компоненту
2. Приложение для смены паролей обеспечивает сложность пароля (спец. знаки, цифры, заглавные и строчные буквы, длина пароля)
3. Бумажные копии паролей находятся в разных сейфах и доступны конкретным лицам.
4. Периодическая проверка целостности конвертов инженером по ИБ
5. hmac от шифровки проверочного слова на постоянной основе хранится в БД под UNIQUE индексом – исключаем повторение
6. После проверки старого пароля начинаем перешифровку данных пачками – по 200 штук (включая маски карт и exp.date)
7. Пароль для перешифровки собирается для каждой итерации и удаляется из памяти за ненадобностью
8. Прерывание процесса перешифровки не критично в целом, так как есть связка “шифрованные данные” – “hmac от проверочной шифровки“. Есть возможность продолжить перешифровку только оставшейся информации.

8. Запуск приложения



для каждой операции (вернуть список карт, сохранение карты в БД) собираем пароль и уничтожаем сразу после операции

Мы с удовольствием ответим на все Ваши вопросы

Ревяшко Андрей Сергеевич

Технический директор

Тел.: +7 495 775-55-05 доб. 1150
E-mail: reviashko@wildberries.ru

Федотов Олег Валерьевич

Специалист по информационной безопасности

Тел.: +7 495 775-55-05 доб. 1201
E-mail: fedotov.oleg@wildberries.ru

Вопросы?

www.wildberries.ru