БЕЗОПАСНОСТЬ ТРАНЗАКЦИЙ В СИСТЕМАХ ЭЛЕКТРОННОГО БИЗНЕСА

БЕЗОПАСНОСТЬ ТРАНЗАКЦИЙ В СИСТЕМАХ ЭЛЕКТРОННОГО БИЗНЕСА

Электронная коммерция (e-commerce) - это любая форма бизнес- процесса, в котором взаимодействие между субъектами происходит электронным образом.

Интернет торговля (e-business) - процесс покупки/продажи товаров или услуг, в котором весь цикл коммерческой/финансовой транзакции или ее часть осуществляется электронным образом с применением Интернет-технологий.

Рис.1. Взаимодействие компонентов в системе

Направления электронной коммерции и торговли

Бизнес-модель — концептуальное описание предпринимательской деятельности

бизнес—бизнес (business-to-business, B2B) - **аутсорсинг**;

бизнес—потребитель (business-to-consumer или business-to-client, B2C)- **интернет-магазины**;

потребитель—потребитель (consumer-to-consumer, C2C) – **интернет-аукционы, интернет-площадки**;

бизнес—администрация (business-to-administration, B2A) – **нп, взаимод с ПВТ**;

потребитель—администрация (consumer-to-administration, C2A)- **взаимодействия государственных структур и потребителей в социальной и налоговой сфере (налог. декларации);**

Компоненты модели электронной торговли

- ЭЛЕКТРОННЫЙ МАГАЗИН,
- КЛИЕНТ (ПОКУПАТЕЛЬ),
- ПЛАТЕЖНАЯ СИСТЕМА,
- БАНК (КРЕДИТНАЯ ОРГАНИЗАЦИЯ),
- ПОСТАВЩИК.

Минимум компонентов программного обеспечения, необходимых для функционирования интернет-магазина:

- **Web-сервер (Apache, Microsoft-IIS, Netscape-Enterprise),**
- **Сервер приложений,**
- **СУБД (MySQL, PostgreSQL, ORACLE, MS SQL)**

Основой для ведения электронной коммерции является Web-сайт.

Во время сканирования web-сайтов наступает обмен заданиями, генерируемыми браузером, а также ответами на эти задания, генерируемыми сетевым сервером.

Такой сервер следует рассматривать как часть Интернет-магазина (рис.2).

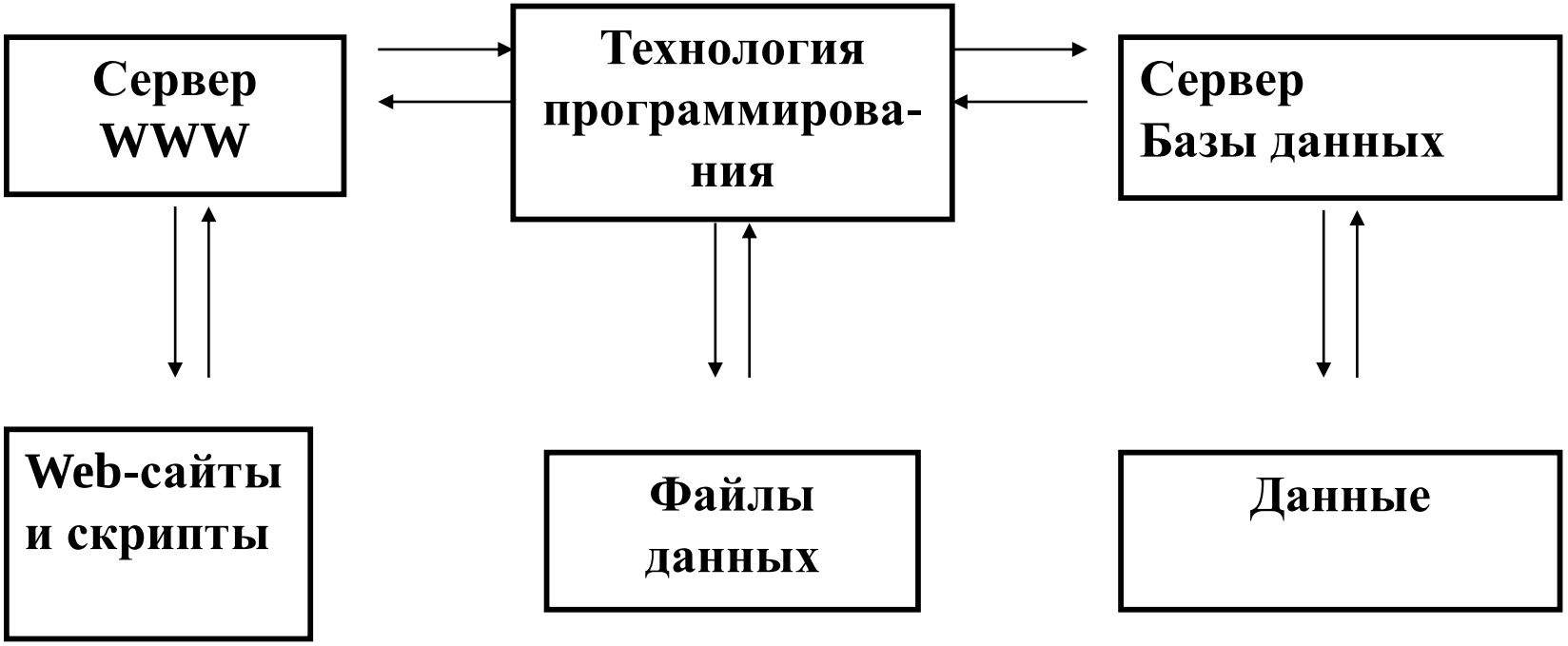
Сервер WWW
Технология программирова-ния
Сервер Базы данных
Web-сайты и скрипты
Файлы данных
Данные

Рис.2

- Каждая транзакция между приложением WWW и Пользователем начинается с обращения, сгенерированного поисковой системой в адрес сервера сети Web.
- Если искомым объектом будет скрипт, то сервер передает его обработку соответствующему механизму, который обслуживает скрипты (нпр, на основе PHP).
- Скрипт может быть предназначен для считывания информации с диска либо записи информации на диск; скрипт может содержать инструкции для считывания внешних фрагментов кода (функции include(); или require()), а также – присоединения кода либо активизации БД.

ИНФОРМАЦИОННЫЕ УЯЗВИМОСТИ ИНТЕРНЕТ-ПРОЕКТОВ ЭЛЕКТРОННОЙ ТОРГОВЛИ

- возможность доступа к информационным ресурсам извне;
- нападения хакеров;
- вредоносные программы — вирусы и троянские кони;
- частое использование электронной почты может помочь злоумышленникам скомпрометировать имена пользователей торгующей организации;
- специальные программы могут быть использованы для поиска слабых мест в системах хранения пользовательских данных;
- «отказы в обслуживании» (DoS).

Основные методы обеспечения безопасности систем e-commerce

- коммуникационные протоколы,
- средства криптографии,
- механизмы авторизации и аутентификации.

Коммуникационные протоколы

Универсальным решением является размещение средств обеспечения безопасности

над протоколом TCP.

Примером подхода является стандарт ***SSL*** *(Secure Socket Layer — протокол защищенных сокетов).*

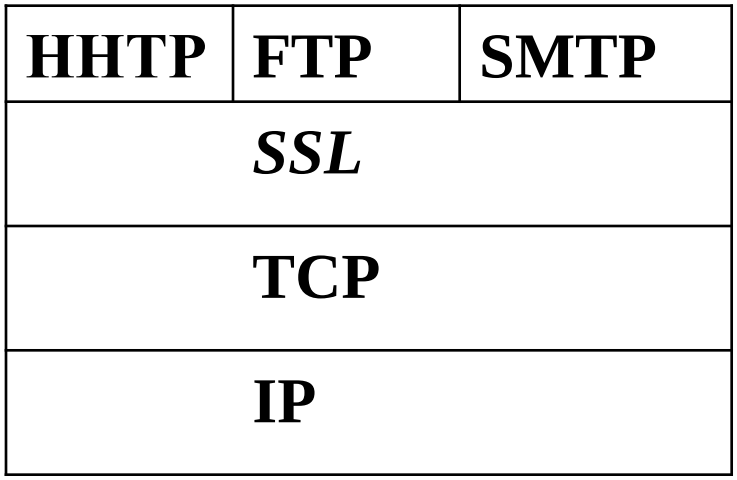

Рис. 3. Размещение средств защиты в стек протоколов TCP/IP

***Протокол SSL**:*

• предложен компанией Netscape,

• призван обеспечить возможность надежной защиты сквозной передачи данных **с** использованием протокола TCP,

• его архитектура состоит из двух уровней протоколов:

а) *протокол записи SSL*,

б) три протокола более высокого уровня:

Протокол квитирования (Handshake Protocol),

Протокол изменения параметров шифрования (Change Cipher Spec Protocol),

Протокол извещения (Alert Protocol)

Протокол квитирования SSL	**Протокол изменения параметров шифрования SSL**	**Протокол извещения SSL**	**HTTP**
	Протокол записи SSL		
	TCP		
	IP		

Рис. 4. Архитектура SSL. Стек протоколов SSL

Работа протокола SSL описывается в терминах двух важных понятий:

Соединение (connection); в SSL соединения представляют отношения между узлами системы;

Сеанс (session). Сеанс SSL — это связь между клиентом и сервером. Сеансы создаются протоколом квитирования SSL

- ***Протокол квитирования*** позволяет серверу и клиенту выполнить взаимную аутентификацию, согласовать алгоритмы шифрования , и криптографические ключи («рукопожатие»).
- ***Протокол изменения параметров шифрования*** генерирует однобайтовое сообщение, которое дает указание начать копирование параметров состояния ожидания в текущее состояние, что приводит к обновлению комплекта шифров, используемых для данного соединения.
- ***Протокол извещения*** предназначен для передачи другой участвующей в обмене данными стороне извещений, касающихся работы SSL.

Протокол записи SSL обеспечивает поддержку двух сервисов для соединения SSL:

****Конфиденциальность;***

****Целостность сообщений.***

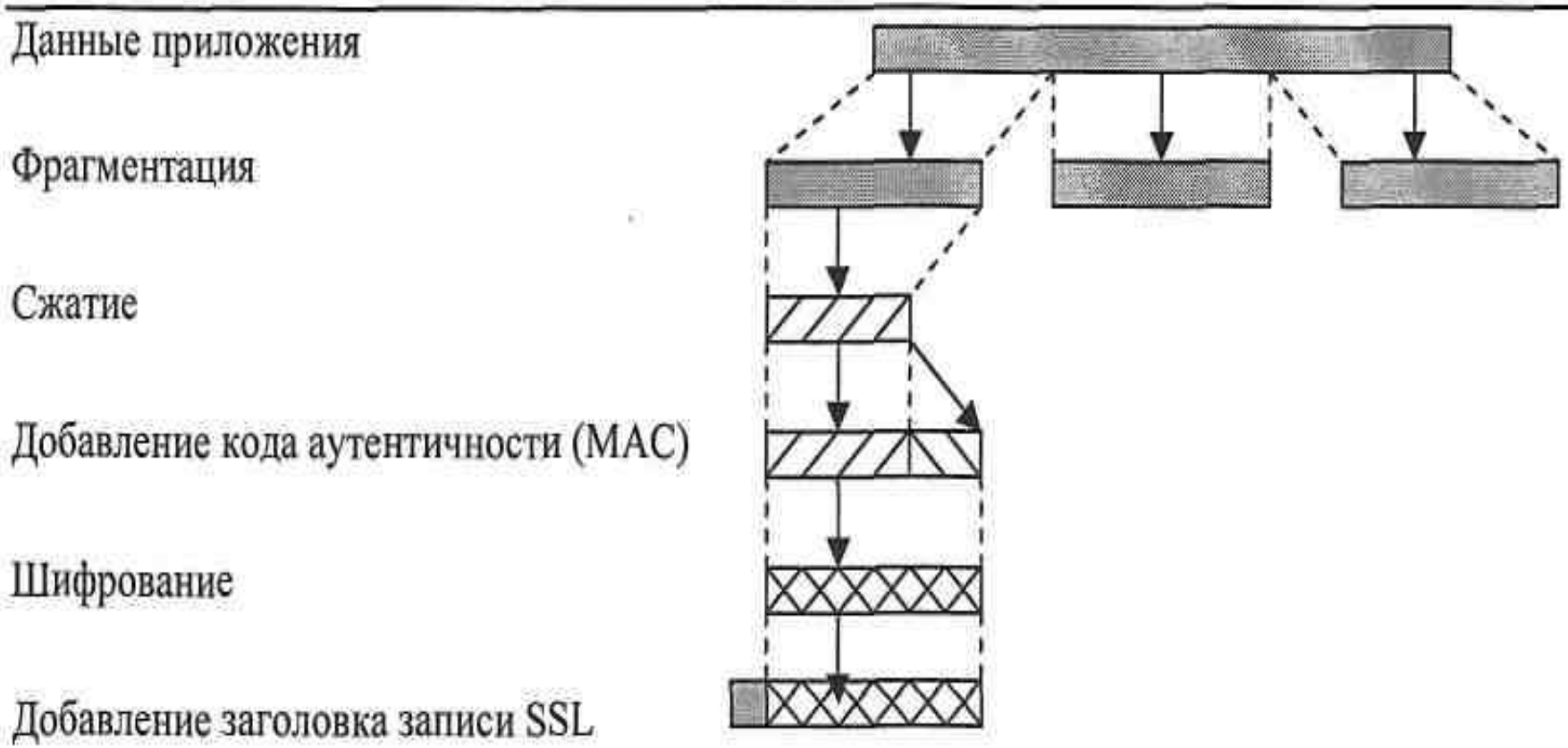

Рис. 5. Схема работы протокола записи SSL

Общие рекомендации

- В случае использования PHP следует иметь в виду, что больший уровень безопасности системы и также более высокая производительность будут достигнуты, если в качестве отдельного модуля (а не отдельного скрипта CGI) будет инсталлирован SAPI (*Server Application Programming Interface*) сервера WWW,
- хорошим решением является инсталлирование сервера БД на том же компьютере, что и сервера WWW. В противном случае – механизм PHP, подсоединяясь к такому серверу, пользуется протоколом TCP/IP, и, как следствие – передает данные в незакодированном виде,
- протокол SSL может быть использован в механизме идентификации (пароль и идентификатор), а также в конечной фазе реализации покупки (во время инициализации скрипта, «отвечающего» за генерацию протокола покупки (накладной)); большинство серверов WWW имеют встроенные функции обслуживания этого протокола.