При этом современные системы управления содержанием web-сайта должны удовлетворять следующим требованиям: поддерживать динамическую работу и иметь средства управления содержанием на каждом этапе жизненного цикла web-сайта; поддерживать встроенную политику безопасности web-сайта и управление учетными записями пользователей; предоставлять возможность смены дизайна и содержания сайта; поддерживать максимально дружественный и удобный интерфейс пользователя; поддерживать встроенный механизм поиска; иметь возможность обработки ошибок и средства их анализа; иметь консоли администрирования и модерирования для настройки системы и ее управления; предоставлять механизм стратегического управления проектом; поддерживать интеллектуальную обработку запросов; обеспечивать пользователя полным комплектом пользовательской и технической документации.

Таким образом, выбор системы автоматизированного создания и управления содержанием современного web-сайта представляет собой трудную задачу, которую необходимо решать, опираясь, как минимум, на требования, описанные выше, а также очень важно, учитывать специфику каждого web-сайта и цели его создания.

Литература

1. Вавилов К., Щербина С. Web-интеграция // Открытые Системы. – 2001. – №2.

Вопросы информационной безопасности Интернет-банкинга

Г.В. Грибова

Алтайская академия экономики и права, г. Барнаул

В условиях тесного переплетения информационных технологий с банковскими бизнес-процессами все более актуальным становится использование в управлении банками современных принципов менеджмента качества.

Применительно к банковской терминологии использование процессного подхода понимается нами как принцип «знай свои технологии». К числу таких технологий относится интернет-банкинг – относительно новая технология, получившая распространение лишь в последние годы.

Сегодняшнему клиенту банка важен свободный выбор, он хочет сам решать: как, когда и где вступать в контакт со своим банком. В ответ на эту потребность банки предлагают обслуживание в режиме он-лайн.

В настоящее время на рынке присутствуют несколько систем интернет-банкинга, которые можно условно разделить на три категории:

– системы, возможности которых ограничены предоставлением клиенту информации о состоянии его счетов. Такова, например, система «Интернет-Банк Экспресс», используемая Импэксбанком;

– системы, позволяющие осуществлять удаленное управление счетами: внутри- и межбанковские переводы, оплату мобильной связи, оплату коммунальных услуг, покупку/продажу безналичной валюты и так далее.

Таких, пожалуй, большинство – к ним относится, например, система «Телебанк», используемая МДМ-Банком, Газпромбанком, Внешторгбанком и рядом других банков.

– системы, позволяющие клиенту получить в режиме он-лайн практически весь комплекс банковских услуг, включая кредитование, операции с ценными бумагами и управление личными финансами. В качестве примера такой системы можно назвать «Интернет-Клиент» от «Банк'с софт системс», работающую в таких крупных банках, как «Петрокоммерц», «Альфа-Банке» и рядом других банков.

Особое внимание при организации дистанционного обслуживания уделяется вопросам безопасности. Безопасность систем интернет-банкинга бывает двух уровней: стандартная и повышенная. В первом случае банк предоставляет заемщику лишь логин (имя пользователя) и пароль, которые необходимо ввести для входа в виртуальный офис. Повышенный уровень безопасности предполагает наличие дополнительной защиты, к которой относится электронная цифровая подпись (ЭЦП). Чтобы информация о клиенте не была перехвачена во время сеанса связи, банки используют протокол SSL (Secure Sockets Layer – слой защищенных соединений), обеспечивающий шифровку всей передаваемой информации. SSL обеспечивает шифрование всей передаваемой информации, от компьютера клиента до сервера банка.

Максимальная длина ключа, используемого в данном протоколе, – 128 бит, т.е. существуют 2128 возможных комбинаций «ключей». В России для передачи всех данных в системах интернет-банкинга в соответствии с нормативными документами, сертифицированными средствами ЭЦП и шифрования, могут использоваться дополнительные криптографические модули, помимо стандартного протокола SSL. Существуют и национальные ГОСТы алгоритмов криптографии.

Именно по этой "подписи" система аутентифицирует пользователя и позволяет совершить необходимую операцию. ЭЦП – последовательность байтов, формируемая путем преобразования подписываемого электронного документа специальным программным средством по криптографическому алгоритму и предназначенная для подтверждения подлинности, целостности и авторства электронного документа. ЭЦП признается аналогом собственноручной подписи (пункт 2 статьи 160 Гражданского Кодекса РФ). В статье 3 Федерального Закона № 1-ФЗ от 10.01.2002 «Об электронной цифровой подписи дано следующее понятие:

– электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

Для обеспечения информационной безопасности в системе «Телебанк» используются следующие механизмы:

1) электронная цифровая подпись – обеспечивает гарантию подлинности подписанных документов и удостоверяет, что сообщение не подвергалось модификации в процессе его пересылки, а также используется для аутентификации личности пользователя системы «Телебанк»;

2) механизм криптографической аутентификации сторон – используется для взаимного подтверждения подлинности сервера приложения «Телебанка» и личности клиента;

3) шифрование информации – обеспечивает защиту данных, которыми обмениваются клиентский Java-апплет и сервер приложения «Телебанк», от несанкционированного доступа;

4) персонализация лиц, работающих с системой «Телебанк».

Как показывает практика, наибольшая доля рисков в структуре операционных рисков «Интернет-клиента» приходится на компрометацию ЭЦП по вине самого клиента. Если ЭЦП скомпрометирована, и пароль с логином для входа в систему «Телебанк» стал известен, то у клиента есть возможность оперативно аннулировать электронную подпись и получить новую.

Перечисленные выше механизмы безопасности при оказании услуг интернет-банкинга гарантирует клиенту следующее:

– при установлении соединения с web-сайтом банка, информация направляется конкретному банку, а не мошеннику, организовавшему перенаправление данных;

– данные, направленные в банк не подлежат изменениям в процессе пересылки;

– информация о клиенте и его операциях не будет раскрыта третьим лицам;

– отправитель данных с адреса клиента однозначно идентифицируется.

Распознавание видового состава зерновых культур на многовременных радарных космоснимках ERS-2

А.В. Евтюшкин, Н.В. Рычкова

ЮНИИ ИТ, г. Ханты-Мансийск, БЮИ МВД, г. Барнаул

С июня 2005 г. в Центре ДЗЗ ЮНИИ ИТ ведется создание архива радарных космоснимков ERS-2\SAR на территорию юга Западной Сибири. Полоса захвата сканера 100 км, разрешение 12.5 м, длина волны С (5.6 см), поляризация VV, временной интервал повторения подспутниковых трасс – 35 суток, временной интервал витков с перекрытием в половину кадра – 17 суток, интервал между полосами перекрытия 3-е суток. Период планирования витков ERS-2 Европейским космическим агентством для съемки сельскохозяйственной зоны Западной Сибири – с мая по октябрь. Космоснимки оперативно принимаются универсальным антенным комплексом ТНА-9 с диаметром зеркала 9 м разработки РНИИ КП.

Компьютерный сегмент, называемый системой непосредственного ввода и обработки данных, разработанный фирмой ACS, Италия, является ядром приемной станции ERS установленной в Центре ДЗЗ ЮНИИ ИТ. Его назначение – ввод данных радара с синтезированной апертурой ERS со скоростью 105 Мбит/с, первичная обработка и архивирование данных. Сегмент состоит из высокоскоростного демодулятора HR ERS-1, 4-х процессорного сервера SGI «Challenge» и управляющей рабочей станции SGI «O2». Дальнейшая обработка данных ERS-2\SAR проводится на суперкомпьютере SUN FIRE 15K. Разработано программное обеспечение на языке IDL-6.2 для пакетного геотрансформирования стандартных кадров ERS-2 в формате PRI размером 100*100 км в проекцию UTM. Для построения полного многовременного покрытия территории выполняются следующие виды обработки каждого кадра: калибровка в шкалу dB и коррекция яркости