Институт информационных технологий БГУИР, Минск,
Республика Беларусь

Волкова А.А.

Пачинин В.И. – зав. кафедрой ИСиТ, канд. техн. наук, доцент

Представлена автоматизированная система управления банковскими операциями и бизнес-процессами, позволяющая организовать работу подразделений банка на основе новых информационных технологий.

В сфере банковских услуг существует потребность, как в квалифицированных кадрах, так и в программном обеспечении, которое, как известно, разрабатывается специально для некоторых организаций либо для всего банковского дела. Данные программные продукты затрагивают множество отраслей и возможностей. Начиная от расчета заработной платы работников банка и заканчивая планированием выплат для погашения кредитов заемщиком. Все эти программы создаются для упрощения деятельности банков, предприятий. Данные программные продукты позволяют усовершенствовать технологический процесс и в результате повысить качество и скорость обслуживания клиентов.

Применение подобной системы подразумевает использование программного комплекса в кредитном и банковском отделе. Для реализации решено реализовать компьютерную сеть, которая позволит автоматизировать работу кредитного отдела, а также отдела банковских операций.

На рисунке 1 приведена структурная схема АСУ банковскими операциями и бизнес-процессами.

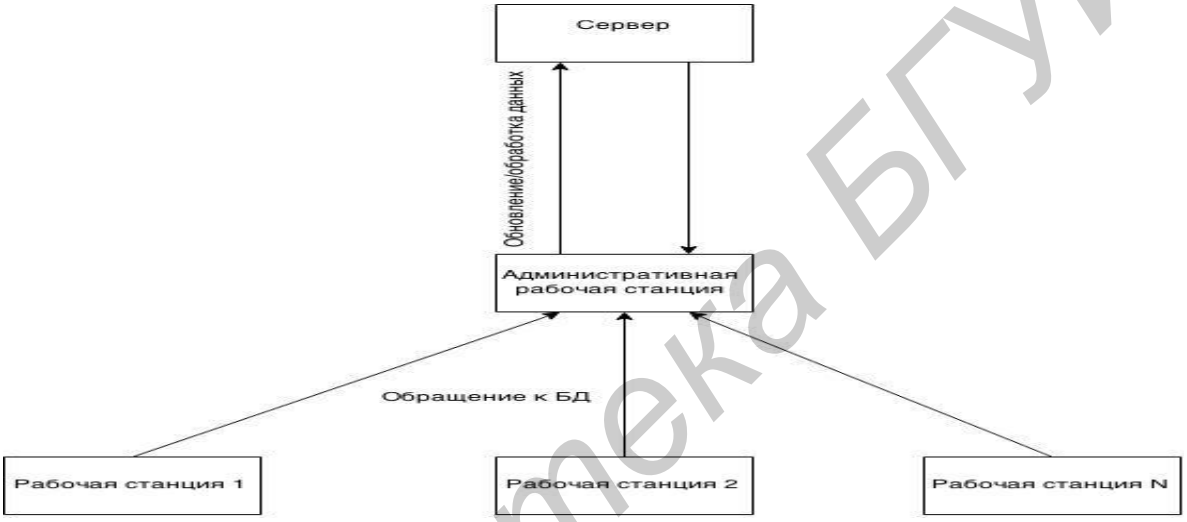

Рисунок 1- структурная схема АСУ банковскими операциями и бизнес-процессами

На рабочих местах сотрудников устанавливаются рабочие станции с соответствующим программным обеспечением. сотрудников. Для сотрудников соответствующих подразделений организуется доступ к сереру в требуемы разделы. Использование такой системы позволило автоматизировать регистрацию новых клиентов, оформление кредитных договоров, хранение информации о клиентах, облегчить поиск информации о типах кредитах и видов платежей, увеличить скорость добавления платежей.

Тип сети – Клиент-серверная. Клиент-серверные сети используют более сложное программное обеспечение, серверная и клиентская части программного кода различаются между собой, устранены основные недостатки файл-серверных сетей, когда единицей обмена между сервером и рабочей станцией является запрос и релевантная запросу выборка, а не целый файл; при редактировании данные доступны для коллективного доступа; уменьшена нагрузка на сетевой трафик. Разновидность клиент-серверной архитектуры - двухуровневый толстый клиент.

Двухуровневый толстый клиент - на рабочей станции находится программное обеспечение в виде пользовательского интерфейса, программ бизнес-приложений. Обработка данных функциональных задач осуществляется на рабочей станции. Сервер обеспечивает хранение файлов и БД, управление сетевыми ресурсами (доступ к файлам и БД, сетевые принтеры);

Построить кабельную систему необходимо на основе оптоволоконного одномодового кабеля.

Таким образом, была разработана автоматизированная система, которая выполняет все функции по управлению банковскими операциями и бизнес-процессами. Она позволяет эффективно организовать работу и деятельность сотрудников банка, не допустить ошибки в их работе, создает удобство работы с документами и клиентами.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гайдамака А. В., Евдокименко М. Н.

Моженкова Е. В. – м - р. техн. наук, ассистент

Рассматриваются основные угрозы безопасности веб-приложений и способы борьбы с ними. Работа представляет собой краткий обзор зарубежных исследований.

Интернет прочно вошел в жизнь любого жителя на Земле. Поскольку основным инструментом для взаимодействия пользователя и бизнеса в сети Интернет является веб-приложение или веб-сервис, в данном докладе рассмотрены самые распространенные способы защиты веб-приложений от посягательств со стороны недобросовестных пользователей и других категорий злоумышленников.

Все угрозы информационной безопасности веб-приложений можно разделить на несколько категорий [1-6]:

1. Инъекция вредоносного пользовательского кода в веб-приложение. Включает подкатегории:
   - Межсайтовый скриптинг – XSS (атака на пользователя, направленная на выполнение в его браузере произвольного сценария) – внедрение вредоносного JavaScript-кода на страницу атакуемой веб-системы [1]. При загрузке страницы браузер автоматически исполняет JavaScript-код, собирая данные аутентификации и отправляя их на сайт злоумышленника. Способы предотвращения XSS-атак: запрет на вложение HTML-страниц, экранирование спецсимволов “<“, “>”, передача всех куки с флагом HttpOnly.
   - SQL-инъекция – внедрение вредоносного SQL-кода в тело HTTP-запроса к веб-приложению [5]. Способы предотвращения SQL-инъекций: повсеместное использование ORM в веб-приложении, клиентская и серверная валидация данных, тестирование веб-приложения, экранирование «очищенных» параметров, поступающих в сырые SQL-запросы, тестирование приложения инструментами на нахождение потенциальных SQL-инъекций.
2. CRLF-атака – техника модификации HTTP-заголовков запроса [2]. Можно выделить 2 её вида:
   - CRLF-инъекция – использование ASCII-представления комбинации CR + LF (перенос каретки + новая строка) для формирования «вредных» URL.
   - Расслоение HTTP-запроса. С его помощью злоумышленник может сформировать URL, который подменит собой ответ сервера, а также, инициировав внутреннюю ошибку веб-приложения, увидеть как информацию о сервере веб-приложений, так и служебную информацию.

   Способы предотвращения CRLF-атак: обязательное кодирование CRLF-последовательности до передачи в HTTP-заголовки, а также полное кодирование передаваемых данных.

   2. XXE (XML eXternal Entity) -атака [3]. При валидации XML-документа парсером (объектно-ориентированным скриптовым языком программирования, созданным для генерации HTML-страниц на веб-сервере с поддержкой CGI) с помощью схемы DTD, все ее директивы обязательно должны быть выполнены. Если правилами определено, что во входном документе допускаются спецсимволы XML, – риск быть атакованным очень велик. Способы предотвращения XXE: тщательная настройка XML-парсеров, использование XML Schema вместо DTD для валидирующего парсера.

   3. CSRF (Cross Site Request Forgery) – межсайтовая подделка запросов [5]. Дает возможность злоумышленнику воспользоваться аутентификационными данными жертвы (cookies) и провести от ее имени какую-либо зловредную операцию. Способы предотвращения CSRF: установка HttpOnly-флага передачи cookie, использование одноразовых сессионных token и отправка скрытой формы, чтобы token нельзя было подделать, проверка рефереров при HTTP-запросах к веб-приложению.

   4. Атаки со стороны пользовательского интерфейса. Используя клиентские JavaScript-библиотеки веб-приложения, злоумышленник может «разблокировать» его элементы управления, таким образом скомпрометировав функциональность сайта. Предотвращение атак через пользовательский интерфейс осуществляется путем сверки данных, отправляемых от пользователя, с теми, что хранит веб-приложение.

В докладе подробно рассматриваются все вышеперечисленные угрозы информационной безопасности и методы их парирования.

Список использованных источников:

1.Cross-Site Scripting – Wikipedia [Электронный ресурс] – Режим доступа: http://en.wikipedia.org/wiki/Cross-site_scripting. – Дата доступа: 15.03.2015.

2.CRLF Injection – Open Web Application Security Project [Электронный ресурс] – Режим доступа: https://www.owasp.org/index.php/CRLF_Injection. – Дата доступа: 15.03.2015.

3.Testing for XML Injection – Open Web Application Security Project [Электронный ресурс] – Режим доступа: https://www.owasp.org/index.php/Testing_for_XML_Injection_(OTG-INPVAL-008). – Дата доступа: 15.03.2015.

4.XML Validation – Wikipedia [Электронный ресурс] – Режим доступа: http://en.wikipedia.org/wiki/XML_validation. – Дата доступа: 15.03.2015.

5.Paco Hope, Paco, Walter, Ben. Web Security Testing Cookbook. – Sebastopol (USA): O'Reilly Media, 2008. – 314 p.

6.Types of Attacks for Web Applications – University Of California, San Francisco [Электронный ресурс] – Режим доступа: https://it.ucsf.edu/services/application-and-website-security/types-attacks-web-applications. – Дата доступа: 15.03.2015.

АВТОМАТИЧЕСКАЯ СИСТЕМА УПРАВЛЕНИЯ БИЗНЕС-ПРОЦЕССАМИ

Институт информационных технологий БГУИР, Минск, Республика Беларусь

Ганчарук М А.