ЗАЩИТА ДАННЫХ В БАНКОВСКОЙ СИСТЕМЕ РАСЧЕТА ФИНАНСОВЫХ РИСКОВ

С. П. Бондаренко[1], М. А. Акинфина[2]

[1]*Белорусский государственный университет*
[2]*Белорусский государственный экономический университет*
Минск, Республика Беларусь
e-mail: BondarenkoSP@bsu.by

Приводятся результаты разработки необходимых компонент безопасности для многопользовательской системы расчета финансовых рисков. Описаны реализация и внедрение необходимых компонентов безопасности.

Ключевые слова: финансовые риски; защита информации; модель безопасности.

THE PROTECTION OF THE DATA IN THE BANKING SYSTEM OF CALCULATION FINANCIAL RISKS

S. P. Bondarenko[1], M. A. Akinfina[2]

[1]*Belarusian State University*
[2]*Belarus State Economic University*
Minsk, Belarus

In this work the results of developing the necessary components of safety for the multi-user system of the calculation of financial risks are given. Realization and introduction of the necessary components of safety are described.

Keywords: financial risks; the protection of information; the model of safety.

В настоящее время, в век высоких технологий, хранение и обработка информации неразрывно связаны с компьютерными технологиями, системами и сетями связи, поэтому становится очевидной важность решения вопроса разграничения доступа к информации в них. Угрозы информационной безопасности существуют в любой информационной системе, которая предполагает некоторое взаимодействие пользователей, передачу данных по сети или работу с внешними системами. Но особенно подвержена таким угрозам финансовая сфера, в которой почти все программные продукты включают в себя работу с конфиденциальной информацией или требуют особого контроля качества. Поэтому при разработке любой такой системы необходимо особое внимание уделить требованиям информационной безопасности.

Система расчета финансовых рисков представляет собой программный комплекс для расчета и анализа различных показателей финансовых рисков, которые банки должны предоставлять в соответствии с международными стандартами, а именно в соответствии с международными требованиями стандартов Базеля. Система предназначена для использования только в банках. Пользователи системы – финансовые ана-

литики, риск-менеджеры и другие банковские работники. Как правило, система используется специальным отделом банка, отвечающим за расчет и оценку финансовых рисков клиентов банка и самого банка. Количество пользователей системы может колебаться от 10 до 500 человек. Система работает с набором сделок и дополнительной информацией, которые попадают в нее из различных источников данных. Источники данных в общем случае могут быть абсолютно любыми, начиная от ручного ввода всех данных и заканчивая импортированием из сложных хранилищ данных. Основная функция системы, помимо самих математических расчетов, – возможность создания различных отчетов с рассчитанными показателями риска для поданных на вход данных. Также система позволяет экспортировать эти результаты в различные форматы данных и строить их различные графические представления.

Актуальной задачей для данной системы является противодействие несанкционированному доступу к ресурсам компьютерных сетей, а именно безопасное управление доступом и информационными потоками по памяти и по времени между сущностями компьютерной системы [1]. Из-за нарушения правил доступа, а также действий со стороны лиц, не имеющих прав доступа к ресурсам компьютерных сетей, основная проблема – это разработка эффективных моделей разграничения прав доступа и их программная реализация.

Некоторые технологии и методы, направленные на защиту информации, уже встроены в современные операционные системы, но таких мер зачастую оказывается недостаточно. Поэтому создаются дополнительные программные или программно-аппаратные средства защиты информации от несанкционированного доступа к информации.

Концепция хранения данных такова, что все постоянные данные в системе расчета финансовых рисков хранятся в файловой системе в виде XML-файлов и имеют базовую структуру. Это позволяет реализовать простые механизмы доступа к ним, передачи их между процессами и пользователями по сети и локально, сохранения в различном виде. Все данные имеют уникальные идентификаторы, по которым можно определить тип данных и получить к ним доступ.

Изначально все данные хранятся на сервере, на этапе конфигурации системы необходимые пользователю данные попадают в специальное хранилище, расположенное также на сервере, и сохраняются в бинарном виде для ускорения работы с ними. Эти данные используются только для промежуточных расчетов и после их окончания удаляются. Те данные, которые необходимо редактировать, переносятся на машину пользователя. Там с ними выполняются необходимые операции, и они сохраняются. При необходимости их можно синхронизировать с данными, расположенными на сервере.

Был выполнен анализ системы расчета финансовых рисков на уязвимости, которые являются значимыми в области ее применения. Также были учтены пожелания и замечания конечных пользователей системы, так как ее имеющиеся компоненты уже находятся в опытной эксплуатации. При этом были обнаружены следующие недостатки:

- отсутствие механизмов идентификации и аутентификации и всех связанных с ними механизмов защиты информации;
- отсутствие контроля и анализа прав доступа пользователей;
- отсутствие разделения обязанностей;
- отсутствие доказательств совершения действий;
- отсутствие или проведение в недостаточном объеме тестирования программного обеспечения;

- отсутствие проверки обрабатываемых данных;
- снижение доступности системы при увеличении числа одновременно работающих пользователей.

В результате анализа обнаруженных уязвимостей системы было решено вначале разработать и внедрить в систему основные подсистемы идентификации, аутентификации и авторизации, что позволило устранить первые из трех недостатков вышеприведенного списка.

Для реализации идентификации и аутентификации был разработан отдельный сервис нижнего уровня системы. Поскольку система работает в операционной системе Windows, было решено использовать встроенные функции этой операционной системы и платформы .NET. При этом был разработан еще один сервис, который выполнял идентификацию и аутентификацию, используя собственную проверку пользовательского пароля.

Таким образом, результатом разработки стала настраиваемая подсистема аутентификации, которая может функционировать в двух режимах: как встроенная аутентификация системы Windows и как собственная аутентификация на основе логина и пароля.

В качестве модели безопасности для подсистемы авторизации решено было использовать ролевую модель [2, 3], добавив в нее некоторые особенности, необходимые для данной системы. Выбор этой модели обусловлен простотой ее логического устройства и реализации. Также данная модель хорошо отражает разделение на классы пользователей системы.

Проанализировав требования к подсистеме авторизации, было решено реализовать ее отдельным сервисом нижнего уровня системы. Этот сервис был встроен в сервис вызова методов объектов системы, поэтому все операции над ними проходят авторизацию. Изначально были выделены две основные роли: администратор и пользователь, которые были добавлены в систему по умолчанию. Администратор при этом имеет полный доступ, т. е. может создавать новые роли и назначать им права доступа. Также администратор может добавлять пользователей в систему и назначать им роли либо роли могут объединять в себе права доступа других ролей, тем самым объединяя несколько ролей в одну общую роль.

Реализация подсистемы аудита действий пользователей и изменения данных осуществлялась в рамках следующих требований: обработка всех видов ошибок и запись их в журнал, который можно просмотреть, отслеживание всех событий аутентификации и авторизации и событий изменения, удаления или добавления данных. Подсистема работает на нижнем уровне системы и встроена в основные сервисы работы с данными.

Выполнение этих требований и успешное встраивание этой подсистемы устранило такие уязвимости, как: отсутствие доказательств совершения действий, отсутствие информации об использовании ресурсов системы и отсутствие мониторинга действий пользователей.

В ходе разработки системы расчета финансовых рисков появилась необходимость контроля правильности внесенных изменений в алгоритмы расчетов и данные. В итоге была построена подсистема автоматического запуска тестов. В этой подсистеме были реализованы механизмы, которые работают по следующему алгоритму:

- В определенный момент времени, когда система находится в устойчивом состоянии, формируются эталонные данные о ее работе, такие как производительность, результаты расчетов и состояние данных в системе.

- После этого каждый определенный промежуток времени (например, час, день, неделя) на машине с таким же окружением происходит запуск следующих тестов.
- Запускаются основные вычислительные задачи и их результаты, такие как время выполнения и использованные ресурсы, результаты расчетов сравниваются с эталонными данными.
- Запускается сравнение текущих данных системы с эталонными данными.
- Если обнаружены какие-либо различия, то формируется подробный отчет о них и высылается на электронную почту.
- Если возникшие отличия правильные, т. е. возникли не в результате ошибок разработчиков и пользователей системы либо в результате отказа каких-либо ее компонентов, то эталонные данные обновляются текущими данными.

Реализация данной подсистемы позволила устранить следующие недостатки: отсутствие или проведение в недостаточном объеме тестирования программного обеспечения, ошибки при разработке системы. С ее помощью были выявлены множество ошибок разработки и использования системы. Также на основе дополнительной информации, которую легко получить на сервере, подсистема позволяет анализировать изменение производительности системы со временем, использование системой дополнительных ресурсов сервера и его загруженность.

Исследование поведения системы при пиковых нагрузках обнаружило снижение степени доступности при увеличении числа одновременно работающих пользователей. Была проведена работа по установлению причины этого отказа, которая показала, что сервис получения рыночных данных не справляется с большим количеством одновременных запросов. В итоге была разработана подсистема кэширования запросов рыночных данных, которая позволила устранить эту проблему.

Таким образом, все найденные уязвимости в системе расчета финансовых рисков были устранены разработкой и внедрением упомянутых подсистем.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Афанасьев А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. М., 2009.
2. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М. : ДМК, 2008.
3. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М., 2009.
4. Ховард М., Леблан Д. Защищенный код. 2-е изд. М. : Русская редакция, 2005.