



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(дипломная работа)

На тему "Разработка защищенной информационно-аналитической системы для торговли на Forex"

Исполнитель Базарнов Илья Борисович
(фамилия, имя, отчество)

Руководитель д.т.н., профессор
Фомин Владимир Владимирович
(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой (подпись)

профессор, доктор технических наук
(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«17» февраля 2017г.

Санкт-Петербург
2017



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(дипломная работа)

На тему "Разработка защищенной информационно-аналитической системы для торговли на Forex"

Исполнитель Базарнов Илья Борисович
(фамилия, имя, отчество)

Руководитель д.т.н., профессор
Фомин Владимир Владимирович
(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой _____
(подпись)

профессор, доктор технических наук
(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«__» _____ 20__ г.

Санкт–Петербург
2017

ГОУ ВПО РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Факультет Информационных систем и геотехнологий

Кафедра ИТ-СБ

Специальность 090106-Информационная безопасность

телекоммуникационных систем

ЗАДАНИЕ

на дипломное проектирование

Студент

Базарнов Илья Борисович ОИБ-С11-1

1. Тема дипломного проектирования (работы)

Разработка защищенной информационно-аналитической системы для торговли на Forex (на основе данных анализа опционов CME Group)

2. Исходные данные

Протоколы pdf-формата CME Group, ПО веб-сервер IIS или Apache, ПО терминал MT4, стартовый комплект разработчика программно-аппаратных средств защиты HASP SRM, ключи защиты HASP SL/HL (Hasp HL Pro), аппаратный ключ Рутокен Web, ПО API плагина для Рутокен WEB, PHP, MySQL. Среда визуальной разработки программ Delphi.

3. Перечень подлежащих разработке разделов по теме

Загрузка pdf файлов протоколов с ftp-сервера CME Group. Конвертация из формата pdf в txt. Выбор торговой стратегии. Разработка web-сайта, позволяющего отображать результаты обработки txt файлов с данными от CME Group для выбранной торговой стратегии. Поддержка регистрации пользователей на разработанном сайте. Усиление защиты доступа пользователей к сайту использованием двухфакторной аутентификации на основе аппаратного ключа Рутокен WEB. Разработка программы-клиента для подключения пользователей к web-порталу (альтернативный web-браузер только для подключения к разработанному сайту). Защита написанной на Delphi программы-клиента с использованием аппаратного или программного ключа HASP. Тестирование разработанной защищенной информационно-аналитической системы для торговли на Forex (на основе данных анализа опционов CME Group), оценка эффективности реализованных вариантов защиты.

4. Состав технической документации проекта

Инструкция по установке и использованию разработанной защищенной системы. Дипломная записка. DVD диск с разработанными системами защиты, документация в электронном виде (pdf и doc формат). Тестовые программы с установленной защитой.

Задание утверждено на заседании кафедры ИТ-СБ «__» _____ 20__ г.,

Дата выдачи задания «__» _____ 20__ г.

Зав. кафедрой ИТ-СБ _____ (В.Г. Бурлов)

Руководитель _____ (В.В. Фомин)

Студент _____ (Базарнов И.Б.)

Содержание

| | |
|--|----|
| ВВЕДЕНИЕ | 5 |
| 1 Разработка математико-алгоритмической модели информационно-аналитической системы информирования трейдеров | 9 |
| 1.1 Рассмотрение торговых стратегий, использующих данные CME Group | 9 |
| 1.2 Алгоритм открытия ордеров по валютной паре EUR/USD на рынке Forex на основе данных опционных уровней первого порядка | 12 |
| 1.3 Обработка бюллетеней биржи CME Group по паре EUR/USD | 16 |
| 1.4 Формализованные алгоритм информационно-аналитической системы – нахождение границ рынка, открытие ордеров | 19 |
| 2 Программная реализация модулей информационно-аналитической системы | 22 |
| 2.1 Получение бюллетеней с ftp сервера CME Group..... | 22 |
| 2.2 Выбор СУБД. Структура базы данных информационно-аналитической системы..... | 23 |
| 2.3 Организация доступа к web-сайту, аутентификация пользователей | 29 |
| 3 Организация двухфакторной аутентификации пользователей с помощью аппаратных ключей Рутокен Web. Разработка специализированного клиента для доступа к сайту системы и защита его ключами HASP | 36 |
| 3.1 Разработка и тестирование php модуля двухфакторной аутентификации с использованием аппаратных ключей Рутокен Web..... | 36 |
| 3.2 Разработка специализированной программы-клиента для подключения к информационно-аналитической системе..... | 41 |
| 3.3 Защита специализированной программы-клиента для подключения к информационно-аналитической системе ключами серии Hasp | 48 |
| Установка навесной защиты при помощи аппаратного ключа HASP HL. | 59 |
| 4 Безопасность жизнедеятельности..... | 63 |
| 4.1 Характеристика вредных факторов при работе с ПК..... | 63 |
| 4.2 Организация рабочего места с ПК. Требования к помещениям с ПК | 64 |
| 4.3 Требования к размещению и оборудованию рабочего места с ПК | 65 |
| 4.4 Требования к санитарно-гигиеническим параметрам рабочего места с ПК | 67 |
| Выводы | 71 |
| Приложения | 75 |
| Приложение А. DVD диск с исходными текстами программ и документацией | 75 |

75 с., 29 рис., 7 источников, 1 приложение

Объект исследования дипломной работы: защищенной информационно-аналитической системы для торговли на Forex (на основе данных анализа опционов CME Group).

Цель работы:

- выбор и алгоритмизация торговой стратегии для разрабатываемой информационно-аналитической системы торговли на Forex (на основе данных анализа опционов CME Group);
- загрузка pdf-файлов с ftp сервера CME Group, конвертация их в txt-формат, получение на основе их обработки целевой информации (границы рынка), создание защищённого web-сайта для доступа пользователей (двухфакторная аппаратная аутентификация), разработка специализированного клиента для доступа к контенту сайта;
- выбор и установка системы защищенного доступа к web-сайта с использованием аппаратных ключей, защита клиента доступа к контенту сайта с помощью аппаратных или программных ключей.

Представлены практические результаты, полученные на основе выполненных теоретических исследований:

- тексты php модулей для разработанного web-сайта системы;
- методика установки и использования защищенного доступа к web-сайту с использованием РутOKEN WEB;
- методика установки и использования защиты эксперта ключами HASP;
- полученные результаты тестирования установленных систем защит.

ВВЕДЕНИЕ

Торговля на международном рынке Форекс связана с высокими рисками, позволяющими получать высокий доход от спекулятивных операций в случае успеха и не менее серьезные убытки, если неправильно было выполнено прогнозирование изменения рынка. Использование трейдерами информационно-аналитических систем позволяет повысить качество прогнозов и, как следствие, увеличить прибыль от совершения торговых операций.

Разработка защищенного варианта информационной системы видится актуальной по нескольким причинам. Следует отметить, что в настоящее время для трейдеров, торгующих на Forex, доступно относительно немного информационных систем, что объясняется как сложностью собственно подхода к прогнозированию поведения рынка, так и тем, что большое число торговых стратегий достаточно плохо формализованы и основаны не на строгих количественных оценках, а на качественной оценке трейдером той или иной ситуации. Разработка информационной системы, ориентированной на оценку действий крупных игроков рынка (открытые ими позиции можно определить, проанализировав данные бюллетеней CME Group), позволяет трейдерам соотносить свои действия с ожиданиями крупных игроков рынка. Доступ к информационно-аналитической системе пользователей может быть реализован с использованием web-портала (web-сайта), альтернативное или дополнительное решение обеспечения доступа – разработка специализированной программы-клиента. Использование специально разработанного клиента дает определенные преимущества в плане работы трейдерам по сравнению с использованием обычного веб-браузера, который только обеспечивает доступ к системе. Специализированный клиент может включать в себя расширенный дополнительный функционал – модули статистической обработки, модули формирования разного рода отчетов, средства визуализации данных, инструментарий, позволяющий автоматизировать доступ трейдеров к информационной системе и т.д.

Информационные системы, формирующие рекомендации трейдерам, в том числе информационно-управляющие системы, позволяющие выдавать сигналы для выставления, управления и закрытия ордеров, должны быть надежно защищены от несанкционированного доступа и использования. С учетом этого являются практически значимыми вопросы установки и использования современных систем защит, в том числе программно-аппаратных.

После ознакомления с поставленной задачей и рассмотрения подлежащих разработке разделов по теме работы был составлен план работы, включающий в себя следующие этапы:

1 Рассмотрение структуры представления информации в формате pdf-файлов бюллетеней CME Group. Ознакомление с существующими торговыми стратегиями, основанными на результатах обработки данных бюллетеней CME Group. Выбор из перечня возможных стратегии, которая будет положена в основу проектируемой информационно-аналитической системы. Выбранная стратегия с одной стороны должна быть работающей, с другой относительно легко реализуемой с технической точки зрения. Алгоритмизация выбранной стратегии.

2 Решение практического вопроса автоматического получения новых файлов бюллетеней CME Group в pdf формате и конвертация из данного формата в текстовый формат представления данных (txt).

3 Программная реализация алгоритма обработки информации, получение результатов, которые будут предоставлены пользователям информационной системы.

4 Разработка web-сайта для пользователей информационно-аналитической системы.

5 Усиления системы защиты доступа пользователей к web-сайту, поддержка решения основанного на использовании системы двухфакторной аутентификации для пользователей сайта (программно-аппаратное решение, использующее ключи серии Рутокен WEB).

6 Разработка алгоритма и программная реализация на объектно-ориентированном языке Паскаль (среда разработки Delphi) специализированного клиента, позволяющего трейдерам получать доступ к web-сайту.

7 Защита разработанного специализированного клиента от несанкционированного использования и распространения с помощью программной или программно аппаратной защиты (ключи серии Hasp SI и Hasp HI, соответственно).

8 Заключительный этап работы – тестирование и отладка написанного программного обеспечения, выработка рекомендаций по применению того или иного типа защиты.

Следует отметить, что вопрос выбора оптимального варианта системы защиты не является тривиальным и заслуживает внимательного рассмотрения. В работе не разрабатываются новые системы защиты, но актуальным является вопрос выбора оптимальной для конкретной информационной системы защиты или комплекса защитных средств. Средства защиты должны выбираться с учетом как технических (аппаратная и программная платформа, используемая операционная система, емкость коммуникационных каналов обеспечивающих подключение пользователей по сети и т.д.), так и экономических критериев (стоимость системы защиты, необходимость квалифицированного персонала для обслуживания системы защиты, использование программных или аппаратных средств – вопросы связанные с временем доставки ключей потребителю, необходимость таможенного оформления физических ключей, возможность пересылки программных ключей с использованием сети Интернет с последующей их активацией и т.д.). Выбор оптимальных систем защиты информации от несанкционированного доступа особенно актуально для систем электронной торговли и торговых экспертно-аналитических систем. Целесообразно повысить уровень защищенности торговой экспертно-аналитической системы путем интеграции в нее программно-аппаратных систем защиты. Для защиты модулей трейдеров клиентского доступа к

аналитике может использоваться аппаратный ключ типа Hasp HI Pro, для обеспечения защищенного доступа трейдеров к разработанному web-сайту, используется аппаратный ключ RuToken Web. Например, сайт <http://www.rutoken.ru/> содержит исходные коды для организации защиты <http://www.rutoken.ru/products/all/rutoken-web/> Рутокен Web для PHP. Представлен пример интеграции поддержки Рутокен Web в приложениях, написанные на PHP. <http://demo.rutoken.ru/sites/php>. Плагин для WordPress: Защищенная аутентификация пользователей в CMS WordPress с помощью Рутокен Web <http://demo.rutoken.ru/sites/wordpress>.

1 Разработка математико-алгоритмической модели информационно-аналитической системы информирования трейдеров

1.1 Рассмотрение торговых стратегий, использующих данные CME Group

Торговля на рынке Forex может осуществляться вручную, в полуавтоматизированном или в полностью автоматизированном варианте с использованием специального программного обеспечения – торговых роботов. Во всех случаях ордера на покупку или продажу финансовых инструментов открываются с использованием информации о текущих и предшествующих котировках финансовых инструментов. Для анализа изменения графиков котировок валют могут использоваться различные математические модели, реализованные в виде программного обеспечения, работающего под управлением тех торговых платформ, которые используются для торговли. Выбор платформы чаще всего определяется не желанием трейдера, а возможностью выбора одной или нескольких платформ, которые поддерживаются брокером (фирмой, предоставляющей трейдерам доступ к торговле на рынке). Рынок может находиться в одном из состояний, в наиболее общей классификации можно выделить состояние целенаправленного изменения – падения или увеличение стоимости актива, т.е. можно говорить о том, что имеет место восходящий или нисходящий тренд. Второе состояние рынка, в котором он пребывает значительную часть времени – отсутствие ярко выраженного движения изменения стоимости торгуемого актива, об этом состоянии говорят, как о состоянии без движения, состоянии флэта, когда значение стоимости актива колеблется в относительно небольшом диапазоне.

Используемая трейдерами торговая система часто строится на основе математической модели, опирающейся на данные технического и/или волнового анализа – анализируются характерные фрагменты графиков финансовых инструментов с целью поиска закономерностей и прогнозирования на их основе будущих движений инструмента. Данные, используемые для

технического и волнового анализа, как правило, в большей или меньшей степени дополняются данными фундаментального анализа, учитывающего мировую экономическую и политическую ситуацию, данные макропоказателей экономик стран, образующих торгуемую пару, например, британский фунт к доллару США. Дополнительную информацию об изменениях финансового инструмента можно получать, анализируя данные контрактов по опционам и фьючерсам на мировых биржах. Например, для анализа могут использоваться данные отчетов крупнейшей товарно-сырьевой Чикагской биржи, а именно, CME Group – информация Daily Bulletin ([http://www.cmegroup.com/daily_bulletin/current/Section39_Euro_FX_And_Cme\\$Index_Options.pdf](http://www.cmegroup.com/daily_bulletin/current/Section39_Euro_FX_And_Cme$Index_Options.pdf) – по ссылке доступен для просмотра последний из выпущенных отчетов по EUR/USD). Анализ учитывает расстановку контрактов крупных игроков. В общем случае наличие крупных объемов контрактов опционов Call и Put, которые можно оценить, как проданные, позволяет найти, так называемые верхнюю и нижнюю границу рынка. Верхняя и нижняя граница рынка для текущего опционного месяца образуют комфортный диапазон, в котором может колебаться цена, не затрагивая интересов крупных игроков. Крупные игроки получают свою прибыль, при условии, что на момент экспирации (момент закрытия месячных опционов) цена осталась в данном ценовом коридоре. Для торговли может использоваться алгоритм достаточно хорошо зарекомендовавшей себя среднесрочной торговой системы, позволяющей торговать EUR/USD. Суть подхода в том, что если цена выходит за верхнюю границу или за нижнюю границу рынка, то крупные игроки-маркетмейкеры приложат все свои усилия, чтобы на момент закрытия опционного месяца цена вернулась в комфортный диапазон, позволяющий этим крупным игрокам получить прибыль. В противном случае крупные игроки – маркетмейкеры, хедж фонды, банки и другие коммерческие организации несут существенные убытки. Так как крупные игроки обладают большим капиталом и информационными возможностями, то манипулируя рынком, они будут стараться хотя бы кратковременно на момент закрытия контрактов вернуть

цену в нужный им диапазон. После успешного закрытия опционов новые контракты будут выставлены с учетом новых сформировавшихся реалий и “естественный ход цены” продолжится. На основе сказанного формируется следующий алгоритм, если цена вышла за верхнюю границу рынка, то надо открывать ордера на продажу, т.к. на цену будут “давить”, чтобы она вернулась назад. Если цена опустилась за нижнюю границу рынка, то надо открывать ордера на покупку, т.к. на цену будут “толкать вверх”, чтобы она вернулась назад в желаемый для игроков диапазон. В настоящее время нет торговых роботов, реализующих работу на основе данной системы. Для трейдеров актуально как получение информации о сигналах для работы с рынком в режиме реального времени, так и создание программы-робота для автоматизированной торговли. Сигналы открытия, сопровождения, закрытия ордеров могут формироваться информационно-аналитической системой (формализация алгоритма, программирование алгоритма, загрузка исторических данных в созданную базу данных, получение и обработка данных в режиме реального времени) и затем доставляться трейдерам с использованием электронной почты, sms, публикацией информации на страницах web-сайта. Сигналы могут непосредственно передаваться терминалам торговой платформы (MT4, MT5) для обработки роботом.

С учетом изложенного выше подхода, трейдерам предлагается возможность использования в торговле нескольких торговых стратегий, которые трейдеры выбирают сами исходя их собственных предпочтений. Все стратегии используют актуальную оперативную информацию значений нижней и верхней границы рынка по торгуемому финансовому инструменту, получаемых на основе обработки данных бюллетеней CME Group.

Проектируемая информационная система позволяет трейдерам получать информацию в режиме реального времени о текущих значениях нижней и верхней границ рынка для запрашиваемого финансового инструмента, а также исторические архивные данные за предыдущие периоды. Следует отметить, что в работе не ставилась задача разработки математической модели, которую

можно использовать в экспертной системе для всестороннего анализа рынка, т.к. построение такой модели требует специальных знаний из области экономики, изучаемых специалистами, получающими экономическое образование. Задача была ограничена только возможностью выбора одной модели из имеющихся моделей, которая могла бы быть относительно просто реализована в виде программного алгоритма. В перечне используемых валютных пар было принято решение ограничиться только парой евродоллар. Так как для рассматриваемого финансового свойственна высокая волатильность, то для успешной торговли целесообразно дополнить разрабатываемую информационную систему функциональной подсистемой оперативного информирования трейдеров о торговых сигналах. Целесообразно разработать систему рассылки сообщений о сигналах по электронной почте, sms, отображать на страницах web-сайта.

Практическая реализация вышеприведенных пунктов позволяет создать конкурентоспособную информационно-аналитическую систему для торговли на Forex на основе данных анализа опционов CME Group.

1.2 Алгоритм открытия ордеров по валютной паре EUR/USD на рынке Forex на основе данных опционных уровней первого порядка

Рассмотрим варианты открытия ордера на покупку/продажу финансового инструмента EUR/USD на рынке Форекс на основе данных опционных уровней первого порядка. С началом нового опционного месяца (информацию о датах начала и конца опционного месяца, текущую информацию о выставленных контрактах опционов CALL и PUT можно найти в бюллетенях CME Group *“<http://www.cmegroup.com/market-data/daily-bulletin.html> в рассматриваемом контексте практический интерес представляет секция FX, в том числе Euro FX And Cme\$Index Options - PG 39”* [1, с. 5]), определяется верхняя и нижняя граница рынка. В базовом варианте расстояние между нижней и верхней границами составляет не менее 250 пунктов. Для открытия ордера ждем, пока

цена уйдет за пределы границ рынка и закрепится над верхней или под нижней границей. Считаем, что цена закрепились за границей рынка если рынок закрывается, а затем открывается по цене, находящейся вне границ ценового коридора. Время закрытия-открытия рынка оцениваем по среднеевропейскому времени, отстающему на 2 часа от Московского времени. На рынке Форекс торговля на буднях днях ведется круглосуточно – временные суточные отрезки и границы между ними, определяемые, как границы открытия-закрытия, рассматриваются как интервалы анализа. Если цена находится вне границ ценового коридора и закрепились вне его, то сигнал на открытие сделки – закрытие свечи на часовом графике (H1) по торгуемому направлению (если над верхней границей, то следует выставить отложенный ордер на продажу, если под нижней границей – отложенный ордер на покупку на расстоянии 50 пунктов (4-х знак) от цены закрытия свечи) после 10 часов по Москве (после 8 часов по терминальному, среднеевропейскому времени). Уровень закрытия ордера по убытку (стоплосс) устанавливается 130 пунктов, уровень закрытия ордера по достижении прибыли (профит) – за противоположной стороной границы рынка (как возможный вариант – закрытие ордера на самой границе рынка). Использование отложенного ордера позволяет уменьшить число неудачных входов в рынок с одной стороны, но с другой уменьшает на 50 пунктов возможную прибыль. Если отложенный ордер до 10 часов по Москве следующего дня не сработал, то ордер удаляется, процедура анализа подходящего момента для установки ордера повторяется по описанному выше алгоритму.

Рассмотрим другие возможные варианты открытия рынка по торгуемому инструменту EUR/USD в новом опционном месяце. На момент открытия рынка Форекс цена находится выше верхней или ниже нижней границы рынка, расстояние между границами рынка равно или больше 250 пунктов. В этом случае следует выставлять ордер на продажу или покупку сразу, не дожидаясь пересечения графика с опционной линией первого порядка, соблюдая описанное выше правило входа в рынок. Другой возможный случай. Начался

новый опционный месяц, на момент открытия рынка цена находится внутри границ рынка, но расстояние между границами рынка меньше 250 пунктов. В этом случае необходимо откорректировать расположение верхней или нижней границы рынка. Ждем, пока график цены не пересечет одну из границ рынка. Затем находим наибольший ближайший опционный уровень, находящийся за пересеченной границей. Если расстояние от этого уровня больше или равно 250 пунктов до противоположной (которую не пересекал график) границы рынка, то значение данного уровня определяем, как скорректированный верхний или нижний уровень, соответственно. Если расстояние меньше 250 пунктов ищем следующий в направлении движения цены, после пересечения первоначально определенной границы рынка, опционный уровень, снова проверяем, стало ли расстояние между данным уровнем и противоположной границей рынка 250 или более пунктов, если нет, то анализируем следующего за рассматриваемым кандидата на уровень скорректированной границы рынка. Операцию повторяем до выполнения условия. Найденный уровень определяем, как скорректированное значение верхней (нижней) границы рынка. Остальные шаги алгоритма торговли остаются без изменения, с границами рынка (одна из которых является скорректированной) работаем также, как и с обычными границами рынка.

Если на момент открытия рынка в новом опционном месяце цена находится выше верхней (ниже нижней) границы рынка, но расстояние между границами рынка меньше 250 пунктов, то сразу корректируется значение той границы, над которой или под которой находится цена, дожидаться пересечения графика с линией некорректированной границы не нужно. Другой встречающийся случай, когда новый опционный месяц начинается открытием финансового инструмента на рынке Форекс строго на верхней или нижней границе рынка, расстояние между границами рынка 250 или более пунктов. В этом случае необходимо ждать начала следующих суток, и, если цена будет продолжать находиться над верхней (или под нижней) границей рынка, то следует искать точку входа для открытия ордера на покупку (продажу) в по

ранее рассмотренным правилам. Если цена окажется в интервале между верхней и нижней границами, то следует ждать, когда график цены пересечет одну из границ, т.е. дальнейшие действия сводятся к первому (основному) из рассмотренных вариантов.

Следующий вариант, когда на момент открытия опционного месяца торги по финансовому инструменту открываются выше или ниже единой совпадающей границы рынка (наибольшее число опционов PUT и CALL было выставлено на один и тоже ценовой уровень), а цена находится над этим уровнем (или под этим уровнем). Если цена находится над объединённым уровнем, то он будет выступать в качестве сильного уровня поддержки – следует установить на этот уровень отложенный ордер на покупку. Если цена находится под объединённым уровнем, то это уровень сопротивления – на него устанавливаем ордер на продажу. Последний из рассматриваемых вариантов – если на момент открытия опционного месяца имеем объединённый уровень, так же, как и в предыдущем случае, но торги по финансовому инструменту открылись точно на объединённой границе рынка. Из дальнейших возможных вариантов развития ситуации ордер на покупку или продажу открываем только в том случае, если цена два раза подходит к уровню, но не может его пробить и отскакивает от него. В наборах свечей, образующих “дуги” первого и второго касания, должны быть свечи, которые своими теньями не касаются объединённого уровня, то есть отскок от уровня должен быть достаточно большим. После второго отскока цены от уровня можно выставить ордер – в зависимости от того выше уровня или ниже находились “дуги” ордер выставляется на покупку или продажу, соответственно. Для повышения вероятности открытия ордера, который будет закрыт с прибылью, можно при возникновении ситуации на открытие ордера, не открывать сразу ордер по рынку, а ставить отложенный ордер на 50 пунктов в направлении прогнозируемого движения цены. Были перечислены все варианты, при наступлении которых видится целесообразным открытие ордеров, во всех оставшихся случаях в рынок не входим, ордер не открываем. Рассматриваемая

стратегия предлагает открывать не более одного ордера по торгуемому инструменту в опционный месяц. Вопросы, связанные с сопровождением сделки по рассматриваемой стратегии, а также условия закрытия ордера рассматривались в одной из ранее опубликованных работ: “Уровень закрытия ордера по убытку (стоплосс) устанавливаем 130 пунктов, уровень закрытия ордера по достижении прибыли (профит) – за противоположной стороной границы рынка...” [2, с. 98].

1.3 Обработка бюллетеней биржи CME Group по паре EUR/USD

Информацию для прогнозов по торгуемому финансовому инструменту можно получить, анализируя данные контрактов по опционам и фьючерсам. Чикагская товарно-сырьевая биржа относится к крупнейшим мировым биржам, ее портал в сети Интернет – CME Group (<http://www.cmegroup.com>). На бирже торговля осуществляется фьючерсами, опционами на основе процентных ставок, индексов акций, иностранной валюты, энергетических ресурсов, металлов и др. (ru.wikipedia.org/wiki/CME_Group). Для анализа изменений могут использоваться данные суточных отчетов, выпускаемых каждый будний день – информация Daily Bulletin (<http://www.cmegroup.com/market-data/daily-bulletin.html> в рассматриваемом контексте практический интерес представляет секция FX, в том числе Euro FX And Cme\$Index Options - PG 39 [http://www.cmegroup.com/daily_bulletin/current/Section39_Euro_FX_And_Cme\\$Index_Options.pdf](http://www.cmegroup.com/daily_bulletin/current/Section39_Euro_FX_And_Cme$Index_Options.pdf) – доступен для просмотра последний из выпущенных отчетов). Для анализа могут потребоваться данные предыдущих отчетов, доступных для загрузки с ftp сервера биржи <ftp://ftp.cmegroup.com/bulletin> (Рис. 1).

Файлы имеют вид *DailyBulletin_pdf_20161010195.zip*, где *20161010* дата в американском формате – год, месяц, день, а **195** – порядковый номер отчета. В отчете по финансовому инструменту EUR/USD находим данные в секции EURO FX CALL по опционам на ближайший месяц (в рассматриваемом примере NOV16 – ноябрь 2016 г., отчет от 10 октября 2016 г.). Следует отметить, что опционные месяцы не совпадают с календарными (Рис. 2).

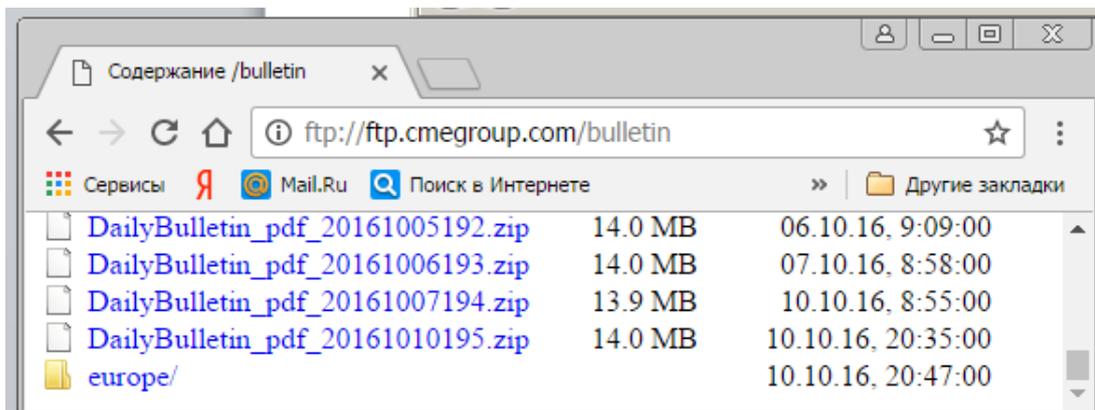


Рисунок 1 – загрузка бюллетеней с ftp сервера

39 Side 01

EURO FX & CME\$INDEX OPTIONS

2016 DAILY INFORMATION BULLETIN - <http://www.cmegroup.com/dailybulletin>
CME Group, Inc.
20 South Wacker Drive, Chicago, Illinois 60606-7499.

39 Side 01

PRELIMINARY

PG39 BULLETIN #195@ EURO FX & CME\$INDEX OPTIONS Mon, Oct 10, 2016 PG39

INDIVIDUAL CONTRACT PRICE DATA FOR OPEN, HIGH, LOW, CLOSE AND SETTLEMENT REFLECT CME REGULAR TRADING HOURS SESSION ONLY. VOLUME CLEARED REFLECTS REGULAR TRADING HOURS (RTH) AND CME GLOBEX® VOLUME FOR FUTURES, AND COMBINED VOLUME FOR OPTIONS. RTH VOLUME REFLECTS PIT TRADING AND CASH-FOR-FUTURES ONLY. VOLUME OR OPEN INTEREST (BOTH BEFORE AND AFTER THE LAST DAY OF TRADING) MAY BE AFFECTED BY: CASH FOR FUTURES, SPREADS, PRIOR DAYS' CLEARED TRADES (OUT-TRADES), POSITION ADJUSTMENTS, OPTIONS EXERCISES, POSITIONS IN DELIVERY, OR POSITIONS IN A CASH SETTLEMENT CYCLE. B=BID A=ASK N=NOMINAL P=POST SETTLEMENT SESSION #=NEW CONTRACT HIGH PRICE *=NEW CONTRACT LOW PRICE R=RECORD VOL OR OPN INT. SETTLEMENT PRICE DETERMINED BY CME RULE 813. B=BID A=ASK N=NOMINAL P=POST SETTLEMENT CAB(CABINET TRANSACTION) 1/2 TICK VALUE EURO FX = \$6.25 CME\$INDEX = \$5.00. PRODUCT LISTINGS REPRESENT CONTRACTS WITH PRICE/VOLUME ACTIVITY AND/OR HAVE ESTABLISHED OPEN INTEREST. PRODUCTS ELIGIBLE TO TRADE BUT ARE INACTIVE DO NOT APPEAR IN THIS REPORT.

EURO FX AMERICAN & EURO & CME\$INDEX CONTRACTS LAST TRADE DATES

| EXPIRATION: | OCT16 | NOV16 | DEC16 | JAN17 | FEB17 | MAR17 | JUN17 | SEP17 |
|-------------------|-------|-------|-------|-------|-------|-------|-------|-------|
| EURO FX FUT | | | 12/19 | | | 03/13 | 06/19 | 09/18 |
| EURO FX OPT | 10/07 | 11/04 | 12/09 | | | 03/03 | 06/09 | |
| EURO FX OPT (EUR) | 10/07 | 11/04 | 12/09 | 01/06 | 02/03 | 03/03 | 06/09 | 09/08 |
| EPX WK2 (EUR) | 10/14 | 11/11 | | | | | | |
| EPX WK3 (EUR) | 10/21 | | | | | | | |
| EPX WK4 (EUR) | 10/28 | | | | | | | |

Рисунок 2 – опционные месяца не совпадают с календарными.

Опционный месяц ноябрь 2016 г. – NOV16, но отчет от 10 октября 2016г.

Анализируем данные в колонке OPEN INTEREST (4-я справа) и находим наибольшее число (Рис. 3): 3780 +. Затем смотрим число в данной строке в первой (самой левой) колонке – это 1130. Делим 1130 на 1000. Получаем значение верхней границы (уровня) рынка – 1.1300. Затем находим нижнюю границу (уровня) рынка (Рис. 4). Секция EURO FX PUT для NOV16: в 4-й колонке справа находим наибольшее число 4567 – смотрим информацию в данной строке в первой колонке. Находим 1095. Делим 1095 на 1000 и получаем значение нижней границы ценового уровня – 1.095. Расстояние между верхней и нижней границей составляет 350 пунктов (четырёхзнак) – $1.1300 - 1.0951 = 0.035$, т.е. 350 пунктов. Значения верхней и нижней границы могут меняться от отчета к отчету, что обусловлено торговой деятельностью крупных игроков, продающих и покупающих опционы, поэтому с выходом очередного отчета следует уточнять значения уровней границ рынка. На основе

анализа построенных и оперативно обновляемых с каждым новым отчетом границ рынка, называемых также уровнями первого порядка (<http://www.forexlife.pro>), могут быть разработаны различные системы для торговли на Форекс. Следует отметить, что значения текущей цены фьючерса по данным отчета CME Group и текущей цены финансового инструмента EUR/USD на Форекс могут отличаться на несколько пунктов (Forward points),

| 39 | | EURO FX & CME\$INDEX OPTIONS | | | | | | | | | | | | 39 | |
|---|--------------|---|------|--------|--------|----|------|------|-----|--------|------|--------|--------|---|--|
| Side 02 | | 2016 DAILY INFORMATION BULLETIN - http://www.cmegroup.com/dailybulletin | | | | | | | | | | | | Side 02 | |
|  | | CME Group, Inc. 20 South Wacker Drive, Chicago, Illinois 60606-7499. | | | | | | | | | | | |  | |
| | | PRELIMINARY | | | | | | | | | | | | | |
| PG39 BULLETIN #195@ | | EURO FX & CME\$INDEX OPTIONS | | | | | | | | | | | | Mon, Oct 10, 2016 PG39 | |
| EURO FX CALL | EURO FX CALL | ---- | ---- | 16.00N | 12.60- | 34 | .629 | ---- | 79 | 722 - | 13 | 38.10B | 12.20A | | |
| 1110 | ---- | ---- | ---- | 12.70N | 9.50- | 32 | .538 | ---- | 8 | 2056 + | UNCH | 34.10B | 9.20A | | |
| 1120 | ---- | ---- | ---- | 9.70N | 6.90- | 28 | .443 | ---- | 274 | 2404 - | 80 | 30.40B | 6.80A | | |
| 1125 | ---- | ---- | ---- | 7.20N | 4.90- | 23 | .349 | ---- | 187 | 2159 + | 55 | 26.90B | 4.80 | | |
| 1130 | ---- | ---- | ---- | 5.20N | 3.40- | 18 | .265 | ---- | 553 | 3780 + | 222 | 23.50B | 3.20 | | |
| 1135 | ---- | ---- | ---- | 3.70N | 2.30- | 14 | .193 | ---- | 552 | 2552 + | 283 | 20.50B | 2.20 | | |
| 1140 | ---- | ---- | ---- | 2.50N | 1.50- | 10 | .136 | ---- | 179 | 3506 - | 70 | 17.70B | 1.50 | | |
| 1145 | ---- | ---- | ---- | 1.70N | 1.00- | 7 | .094 | ---- | 105 | 2233 - | 32 | 15.10B | 1.00 | | |
| 1150 | ---- | ---- | ---- | 1.20N | .70- | 5 | .067 | ---- | 25 | 2505 - | 19 | 12.80B | .70 | | |
| 1155 | ---- | ---- | ---- | 0.80N | .45- | 3 | .045 | ---- | 59 | 2413 - | 47 | 10.70B | .50 | | |
| 1160 | ---- | ---- | ---- | 0.60N | .30- | 3 | .030 | ---- | 54 | 2296 + | 28 | 8.90B | .35A | | |
| 1165 | ---- | ---- | ---- | 0.40N | .25- | 1 | .024 | ---- | 33 | 689 - | 19 | 7.40B | .30 | | |
| 1170 | ---- | ---- | ---- | 0.25N | .15- | 1 | .015 | ---- | 1 | 507 | UNCH | 6.10B | .30A | | |

обычно значение для EUR/USD 1.5-2 пункта, поэтому данным расхождением можно пренебречь.

Рисунок 3 – определение верхней границы рынка (EURO FX CALL)

| | | | | | | | | | | | | | | | |
|-------|-------------|------|------|------|--------|------|--------|------|------|------|--------|--------|--------|--------|------|
| TOTAL | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 0 | ---- | 0 | ---- | ---- | ---- |
| NOV16 | EURO FX PUT | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- |
| 900 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 1 | UNCH | .20 | .10A | |
| 965 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 2 | UNCH | .60B | .20A | |
| 975 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 1 | UNCH | .80B | .15A | |
| 990 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 2 | UNCH | 1.20B | .25A | |
| 995 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 10 | UNCH | 1.30B | .05 | |
| 1000 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 146 | UNCH | 1.60 | .10 | |
| 1005 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 3 | UNCH | 1.80B | .05 | |
| 1010 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 44 | UNCH | 2.00B | .10 | |
| 1015 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 6 | UNCH | 2.30B | .25A | |
| 1020 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 19 | UNCH | 2.60B | .05 | |
| 1025 | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | ---- | 11 | UNCH | 3.00B | .10 | |
| 1030 | ---- | ---- | ---- | ---- | 0.05N | ---- | UNCH | .002 | ---- | ---- | 43 | UNCH | 3.40B | .10 | |
| 1035 | ---- | ---- | ---- | ---- | 0.05N | ---- | UNCH | .004 | ---- | ---- | 46 | UNCH | 4.00B | .10A | |
| 1040 | ---- | ---- | ---- | ---- | 0.10N | ---- | UNCH | .007 | ---- | 1 | 45 + | 1 | 4.50B | .10A | |
| 1045 | ---- | ---- | ---- | ---- | 0.10N | ---- | UNCH | .008 | ---- | ---- | 171 | UNCH | 5.20B | .10 | |
| 1050 | ---- | ---- | ---- | ---- | 0.15N | ---- | .10- | 0 | ---- | ---- | 165 | UNCH | 5.90B | .10 | |
| 1055 | ---- | ---- | ---- | ---- | 0.20N | ---- | .15- | 0 | ---- | ---- | 2 | 264 + | 2 | 6.70B | .15 |
| 1060 | ---- | ---- | ---- | ---- | 0.25N | ---- | .20- | 0 | ---- | ---- | 570 | UNCH | 7.60B | .20A | |
| 1065 | ---- | ---- | ---- | ---- | 0.30N | ---- | .25- | 0 | ---- | ---- | 1 | 641 + | 1 | 8.60B | .25A |
| 1070 | ---- | ---- | ---- | ---- | 0.40N | ---- | .35- | 0 | ---- | ---- | 5 | 816 + | 1 | 9.80B | .30A |
| 1075 | ---- | ---- | ---- | ---- | 0.60N | ---- | .50- | 1 | .043 | ---- | 775 | 2692 + | 766 | 11.10B | .40 |
| 1080 | ---- | ---- | ---- | ---- | 0.70N | UNCH | .70- | .060 | ---- | 4 | 2810 + | 1 | 12.50B | .50 | |
| 1085 | ---- | ---- | ---- | ---- | 1.00N | UNCH | 1.00 | .084 | ---- | 4 | 1235 - | 1 | 14.10B | .80 | |
| 1090 | ---- | ---- | ---- | ---- | 1.40N | ---- | 1.50+ | .120 | ---- | 76 | 2707 + | 45 | 15.80B | 1.00A | |
| 1095 | ---- | ---- | ---- | ---- | 1.90N | ---- | 2.10+ | .163 | ---- | 835 | 4567 + | 654 | 17.80B | 1.40 | |
| 1100 | ---- | ---- | ---- | ---- | 2.70N | ---- | 3.00+ | .220 | ---- | 400 | 4106 + | 227 | 19.90B | 1.80 | |
| 1105 | ---- | ---- | ---- | ---- | 3.70N | ---- | 4.10+ | .287 | ---- | 237 | 4032 + | 121 | 22.20B | 2.40 | |
| 1110 | ---- | ---- | ---- | ---- | 5.00N | ---- | 5.70+ | .370 | ---- | 249 | 3900 + | 82 | 24.80B | 3.30A | |
| 1115 | ---- | ---- | ---- | ---- | 6.60N | ---- | 7.60+ | .460 | ---- | 313 | 3137 + | 77 | 27.60B | 4.40A | |
| 1120 | ---- | ---- | ---- | ---- | 8.70N | ---- | 10.00+ | .556 | ---- | 190 | 2610 + | 160 | 30.40B | 5.70 | |
| 1125 | ---- | ---- | ---- | ---- | 11.20N | ---- | 13.00+ | .650 | ---- | 27 | 1589 - | 15 | 32.50B | 7.40 | |
| 1130 | ---- | ---- | ---- | ---- | 14.10N | ---- | 16.50+ | .734 | ---- | 1 | 906 + | 1 | 36.90B | 9.40 | |
| 1135 | ---- | ---- | ---- | ---- | 17.60N | ---- | 20.40+ | .806 | ---- | ---- | 464 | UNCH | 40.50B | 11.90A | |
| 1140 | ---- | ---- | ---- | ---- | 21.50N | ---- | 24.60+ | .863 | ---- | ---- | 230 | UNCH | 44.30B | 14.60A | |
| 1145 | ---- | ---- | ---- | ---- | 25.70N | ---- | 29.10+ | .905 | ---- | ---- | 59 | UNCH | 48.20B | 17.40A | |
| 1150 | ---- | ---- | ---- | ---- | 30.10N | ---- | 33.70+ | .937 | ---- | ---- | 50 | UNCH | 52.30B | 20.60A | |

Рисунок 4 – определение нижней границы рынка (EURO FX PUT)

Если необходимо использовать точное значение, то можно воспользоваться сервисом cme-equotes.com (требуется пройти регистрацию, разные ценовые тарифы за пользование сервисом). Страница-вкладка *CME E-equivalents* содержит искомую информацию. Для EUR/USD расхождения незначительные, однако, если методика торговли, основанная на использовании границ рынка будет применяться для других финансовых инструментов, для которых CME Group публикуются отчеты (GBP/USD, AUD/USD, USD/CAD,

USD/CHF, USD/JPY), то данную поправку следует учитывать, т.к. разница может составлять более 20 пунктов, что может быть существенно и привести к преждевременному входу или выходу из рынка, а, значит, и к потерям денежных средств или к получению меньшего размера прибыли. В используемой алгоритмической модели, реализованной затем программно *форвардпоинт* не учитывается, т.к. для валютной пары EUR/USD расхождения незначительные.

1.4 Формализованные алгоритм информационно-аналитической системы – нахождение границ рынка, открытие ордеров

Для информационно-аналитической системы была выбрана следующая алгоритмическая модель оценки состояния рынка по торгуемому финансовому инструменту EUR/USD. Используемые идентификаторы:

NGR – текущее значение нижней границы рынка, полученное из последнего доступного загруженного по ftp протоколу бюллетеня CME Group;

BGR – текущее значение верхней границы рынка, полученное из последнего доступного загруженного по ftp протоколу бюллетеня CME Group;

K0 – текущее значение котировки EUR/USD на момент оценивания;

K1 – значение котировки EUR/USD отстоящее на значение интервала времени T от момента оценивания;

T – интервал времени между значением последней оцениваемой котировки и предшествующем значением (в работе принят равным 24 часам для дней понедельник-пятница и 72 часам для интервала пятница-понедельник);

TP – число пунктов, после изменения на которое значения финансового инструмента фиксируется прибыль;

SL – число пунктов, после изменения на которое значения финансового инструмента фиксируется убыток;

D – разница между K1 и K2 в пунктах;

EPS – задаваемое число пунктов (30 и более).

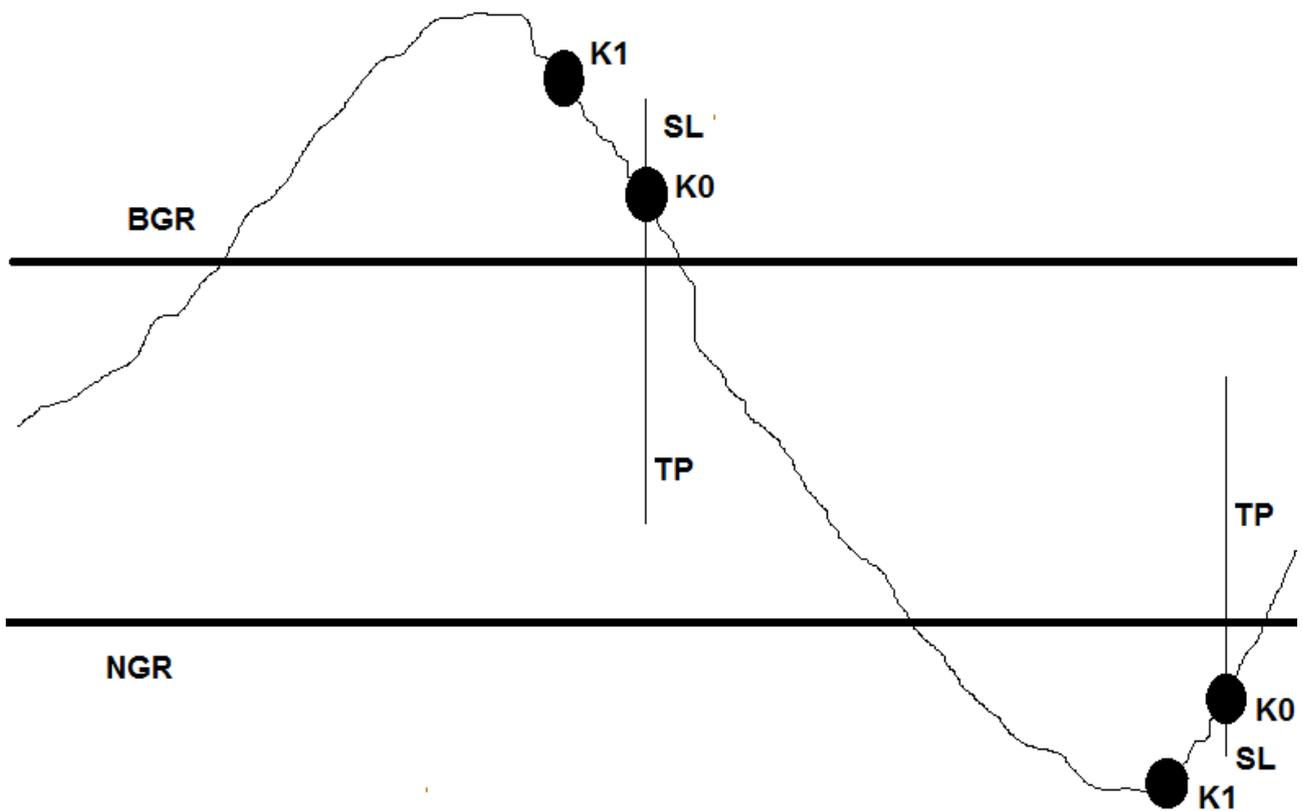
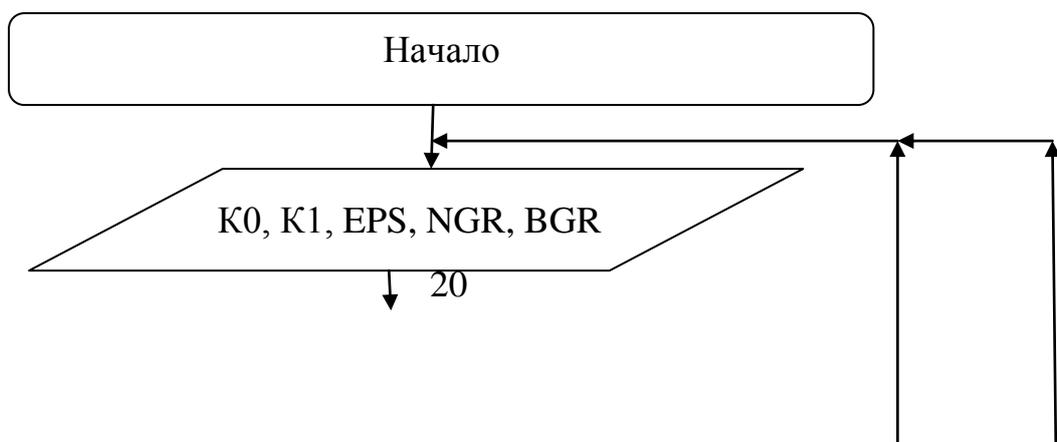


Рисунок 5 – открытие ордеров с учетом расположения границ рынка относительно размещения контрольных точек (K0 и K1) значений котировок финансового инструмента

Алгоритм открытия ордеров

1. Находим значения K0, K1, NGR, BGR.
2. Определяем $|K0-K1|=D$, если $D < EPS$ ждем следующих суток и повторяем с п.1. Если $D \Rightarrow EPS$ переходим к п.3
3. Если $K1 > K0 > BGR$, то открываем ордер на продажу с заданными значениями TP и SL, ждем следующих суток и повторяем с п.1. Иначе переходим к п.4.
4. Если $K1 < K0 < NGR$, то открываем ордер на покупку с заданными значениями TP и SL, ждем следующих суток и повторяем с п.1. Иначе ждем следующих суток и повторяем с п.1.



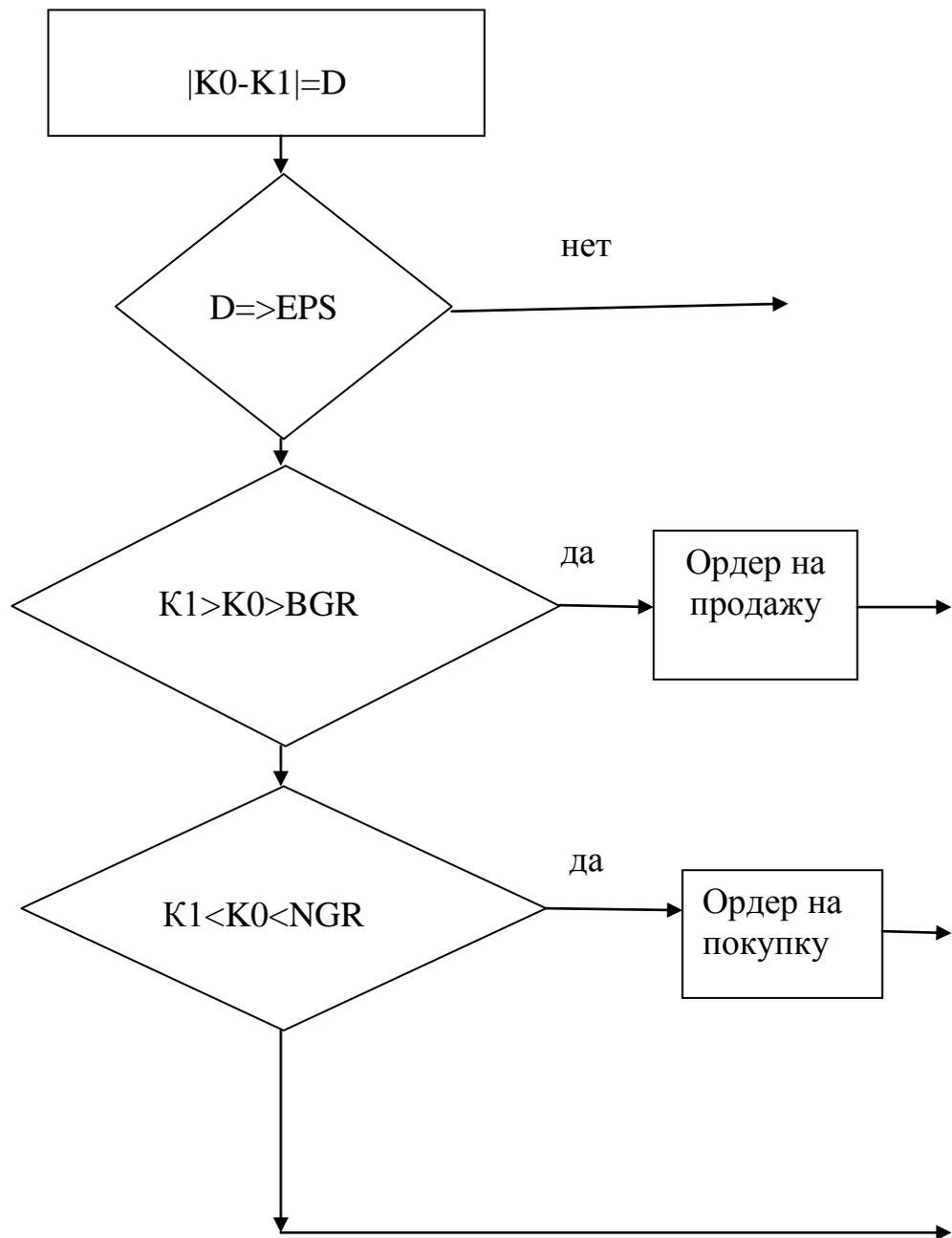


Рисунок 5 – алгоритм открытия ордеров

На Рис.5 представлен алгоритм рекомендаций открытия ордеров. Значение EPS следует брать 30 и более пунктов, SL – от 130 пунктов, TP – 250-300 пунктов, но не более чем значение нижней границы рынка, если ордер открыт на продажу и не более, чем значение верхней границы рынка, если ордер открыть на покупку.

2 Программная реализация модулей информационно-аналитической системы

Для разработки информационной системы, предлагающей торговые рекомендации трейдерам согласно рассмотренному алгоритму (Рис. 5) необходимо решить следующие подзадачи

- реализовать в программном коде получение по ftp протоколу бюллетеней с сервера GME Group;
- конвертация pdf файлов в txt формат, поиск значений нижней и верхней границы рынка, занесение найденной информации в таблицу базы данных;
- подсистема регистрации и аутентификации пользователей;
- подсистема визуализации информации о нижней и верхней границах рынка

2.1 Получение бюллетеней с ftp сервера CME Group

Проанализировав существующие методы загрузки файлов с ftp серверов в автоматизированном режиме [3], был разработан php скрипт ftp.php для загрузки файлов с сервера:

```
<?
print "<h1>Закачка</h1>\n"; $host = "ftp.cmegroup.com";
$connect = ftp_connect($host); if(!$connect) { echo("Ошибка соединения");
exit; } else { echo("Соединение установлено"); echo "<br>"; }
ftp_login($connect, "anonymous", "");
ftp_pasv($connect,true);
ftp_chdir($connect, "/bulletin");
echo ftp_pwd($connect);
echo "</br>";
$buff = ftp_nlist($connect, ".");
$local_file = $UPLOADDIR."/chicago/DailyBulletin_pdf_20150805149.zip";
$server_file = 'DailyBulletin_pdf_20150805149.zip';
echo "<p>Идет закачка с сервера.</p>";
```

```
ftp_get($connect, $local_file, $server_file, FTP_BINARY);  
echo "<p>Закачка завешена.</p>";  
ftp_close($connect);  
?>
```

В примере выполняется загрузка с использованием имени и пути `"/chicago/DailyBulletin_pdf_20150805149.zip"`; – данный фрагмент изменяется в системе с учетом имени скачиваемого файла и его размещения; `ftp_login` – функция коннекта к ftp-серверу, `ftp_pasv` – определение режима доступа.

Выполненное тестирование модуля `php` показало, что файлы загружаются с ftp сервера CME Group.

2.2 Выбор СУБД. Структура базы данных информационно-аналитической системы

Для хранения информации было решено использовать реляционную базу данных, главными объектами которой являются таблицы. Было принято решение свести к минимуму используемое число таблиц, база данных должна находиться в первой нормальной форме. Были рассмотрены коммерческие и свободно распространяемым СУБД – ORACLE SQL Server, MS SQL Server 2012/2014 Express Edition, Enterprise Edition и Standard Edition, MySQL. Были рассмотрены варианты выбора системы управления базами данных (СУБД) для работы с базой данных информационной системы. Были рассмотрены MS SQL Server и MySQL. Предпочтение было отдано MySQL, т.к. все версии MS SQL Server за исключением MS SQL Server Express Edition являются платными. Решение на основе MS SQL Server Express Edition возможно, т.к. информационная система работает только с одной базой данных, а MS SQL Server Express Edition поддерживает только одну пользовательскую базу данных. Окончательным критерием выбора послужило то, что по СУБД MySQL в сети Интернет было найдено больше документации и подходящих примеров использования. MySQL — свободная реляционная система управления базами данных, разработку которой осуществляет корпорация

Oracle, получившая права на торговую марку вместе с поглощённой Sun Microsystems, которая ранее приобрела шведскую компанию MySQL AB. Продукт распространяется под GNU General Public License и под собственной коммерческой лицензией. MySQL хорошее решение для малых и средних приложений, кроме того MySQL входит в портативную сборку серверов Денвер, которая использовалась для отладки программного обеспечения разрабатываемого в ходе выполнения данной работы.

Было решено остановиться на использовании СУБД MySQL Server (mysql версия 5.5), т.к. данная СУБД является свободно распространяемой, кроме того в сети Интернет по работе с ней опубликовано большое число примеров и подробная документация присутствует на сайте разработчиков в свободном доступе, языком для исполнения скриптов был выбран php (версия 4).

Спроектированная база данных (БД) состоит из трех основных таблиц (Рис. 6). Таблица EUR/USD содержит данные о верхней и нижней границах рынка на рассматриваемую календарную дату, таблица USERS – отвечает за информацию о пользователях системы – фамилия, имя, отчество, контактные данные и пр. Третья таблица AUTHN – используется для хранения данных, используемых в процедурах авторизации и аутентификации пользователей.

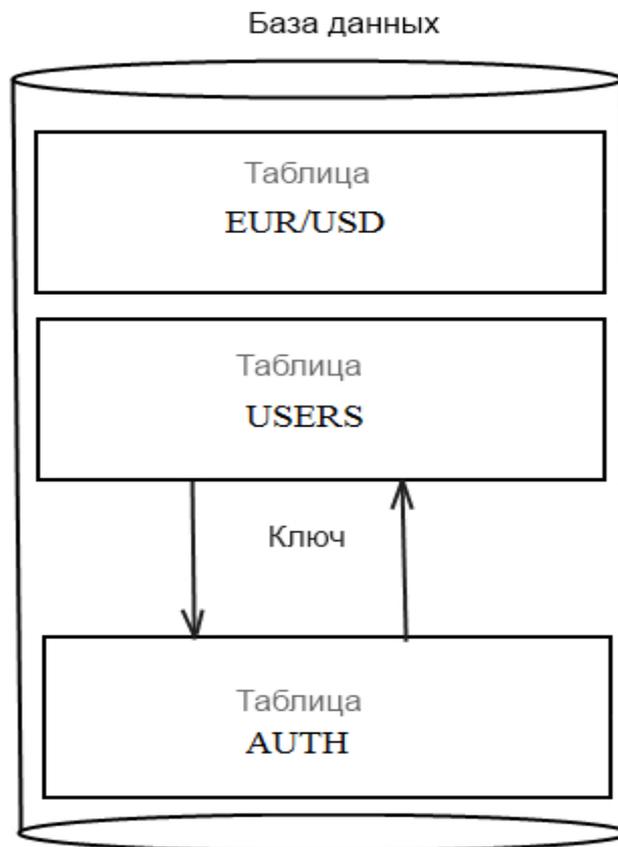


Рисунок 6 – обобщенная структура базы данных

Для взаимодействия с БД был разработан модуль `information.php`:

```

<?
require_once "constant.inc";
require_once "mysql.inc";
$link = mysql_connect( "localhost", $DBUSER, $DBPASS ) or die ( "Could not connect" );
$res = mysql_query( "use $DB", $link );
if ( !$res ) die ( "Нет соединения с базой '$DB'" );
?>
<script>
var plugin; var http = createObject(); var error_text = "";
var err = []; err[-1] = 'USB-токен не найден'; err[-2] = 'USB-токен не залогинен
пользователем'; err[-3] = 'PIN-код не верен'; err[-4] = 'PIN-код не корректен';
err[-5] = 'PIN-код заблокирован'; err[-6] = 'Неправильная длина PIN-кода'; err[-7]
= 'Отказ от ввода PIN-кода';
err[-10] = 'Неправильные аргументы функции'; err[-11] = 'Неправильная длина
аргументов функции'; err[-12] = 'Открыто другое окно ввода PIN-кода'; err[-20] =
'Контейнер не найден'; err[-21] = 'Контейнер уже существует'; err[-22] =
'Контейнер поврежден'; err[-30] = 'ЭЦП не верна'; err[-40] = 'Не хватает свободной
памяти чтобы завершить операцию'; err[-50] = 'Библиотека не загружена'; err[-51]
= 'Библиотека находится в неинициализированном состоянии'; err[-52] =
'Библиотека не поддерживает расширенный интерфейс'; err[-53] = 'Ошибка в
библиотеке rtpkcs11esp'; function createObject() { var request_type;
var browser = navigator.appName;

```

```

if (browser == "Microsoft Internet Explorer") {
    request_type = new ActiveXObject("Microsoft.XMLHTTP");
} else {
    request_type = new XMLHttpRequest();
}
return request_type; }
function errorReply() {
    if (http.readyState == 4) {
        if (http.responseText.indexOf("valid") > 0) {
            link_token();
        } else {
            alert(http.responseText);
        }
    }
}
function chklogin() {
    ulogin = document.getElementById('user_login');
    nocache = Math.random();
    http.open('get',
'validation.php?tlogin='+encodeURIComponent(ulogin.value)+'&nocache='+nocache);
    http.onreadystatechange = errorReply;
    http.send(null);
}

function link_token() {
    plugin = document.getElementById("cryptoPlugin");
    xkey = document.getElementById('usr_xkey');
    ykey = document.getElementById('usr_ykey');
    rxkey = document.getElementById('r_xkey');
    rykey = document.getElementById('r_ykey');
    ulogin = document.getElementById('user_login');
    if (ulogin.value == "") {
        inf.innerHTML = "Введите логин";
        return;
    }
    if (!plugin.valid) {
        inf.innerHTML = "Установите плагин";
        return;
    }
    if ( !(plugin.rtwIsTokenPresentAndOK() === true) ) {
        alert("USB-токен отсутствует!");
    }
    if (!plugin.rtwIsUserLoggedIn()) {
        plugin.rtwUserLoginDlg();
    }
    if (plugin.rtwIsUserLoggedIn()) {
        key = plugin.rtwGenKeyPair(ulogin.value + '%##<?php echo getenv("HTTP_HOST");
?>');
        rkey = plugin.rtwGetPublicKey('repair key');
        plugin.rtwLogout();
        if (key) {
            xkey.value = key.substring(0,64);
            ykey.value = key.substring(64);
            if (rkey) {
                rxkey.value = rkey.substring(0,64);
                rykey.value = rkey.substring(64);
            }
        }
        tform = document.getElementById('regform');
        tform.submit();
    }
}

```

```

    } else {
        alert("Ошибка при создании ключевой пары.");
    }
} else {
    alert("Введен ошибочный PIN-код.");
}
}
function pluginit() { // ...
}
</script>
<html>
<head>
<meta http-equiv=Content-Type content="text/html; charset=UTF-8">
<meta http-equiv="Pragma" content="no-cache">
<link type="text/css" rel="StyleSheet" href="my.css">
</head>
<body bgcolor="<? print $COLOR; ?>">
<?
$query = sprintf("select * from `EUR` where `TIME`<=NOW()");
// print "$query<br>";

$res = mysql_query($query, $link);
$num_rows = mysql_num_rows( $res);
if ($num_rows > 0) {
$хi=0;

    $body    = "<div style=\"text-align:center;\"><button name=\"associate\" style
= \"margin:20px\" align=\"center\">Аутентификация: интегрировать ключ RuToken Web
с используемым логином</button><table style=\"text-align:center;\" align=\"center\"
border=\"1\" cellspacing=\"0\" cellpadding=\"5\"><tbody>\n";
    $body    .= "<tr><th>&nbsp;</th><th>&nbsp;</th><th colspan=\"2\">Опционные уровни
первого порядка (ОУ-1)<br>Границы рынка</th><th colspan=\"2\">";
    $body    .= "<tr><td>Валюта</td><td>Дата</td><td>CALL - верхняя граница
рынка</td><td>PUT - нижняя граница рынка</td>";
while($rows = mysql_fetch_array($res))
{
    $curr    = "EUR";
    $data    = date("Y-m-d H:i:s", strtotime($rows["TIME"]));
    $ou1_cal = $rows["CALL"];
    $ou1_put = $rows["PUT"];
    $хi++;
    $body    .= "<tr>
<td>$curr</td>
<td>$data</td>
<td>$ou1_cal</td><td>$ou1_put</td>
</tr>\n";
}

// echo "картинки уже есть в базе<br>";

```

```

$html_body = $HTML_BODY_PART1;
$line = "<br>"; print $line; $html_body .= $line;
$html_body .= $line;
$body .= "</tbody></table>\n";
print "<tr><td align=\"center\">$body</td></tr>\n"; $html_body .= "<tr><td
align=\"center\">$body</td></tr>\n</div>";
}
if (isset($_POST['associate'])) {
include_once ("config.php");
$login = $_POST['associate'];
$user_xkey = $_POST['user_xkey'];
$user_ykey = $_POST['user_ykey'];
$r_xkey = $_POST['repair_xkey'];
$r_ykey = $_POST['repair_ykey'];
if ( $user_xkey && $user_ykey && $r_xkey && $r_ykey ) {
mysql_query("INSERT INTO sample_users SET user_login='".$login."',
user_xkey='".$user_xkey."', user_ykey='".$user_ykey."', r_xkey='".$r_xkey."',
r_ykey='".$r_ykey.'");
header("Location: login.php");
exit(); } else {
header("Location: register.php");
exit(); }
}
print "</center>\n";
print "</body>\n";
print "</html>\n";
?> </body>

```

Модуль использует данные для обращения к базе данных из файла mysql.inc

```

<?
global $DB;
global $DBHOST;
global $DBUSER;
global $DBPASS;
$DBHOST = "localhost";
$DB = "fxdb";
$DBUSER = "root";
$DBPASS = "Pa$$w0rd";
?>

```

DBHOST – IP адрес или разрешаемое DNS имя хоста; DB – имя базы данных, DBUSER– имя пользователя (root) БД, DBPASS – хранит значение пароля для подключения к БД.

Модуль dbfunc.inc – позволяет контролировать корректность подключения к БД, наличие таблицы для занесения в нее данных значений границ рынка.

```

<?
# Проверим, есть ли данная таблица в базе
function table_exist( $link, $tbl ) {
    global $Q;
    $query = "show tables like '$tbl'";
    $res = mysql_query( $query, $link );
    if ( $Q ) print "$query<br>";
    $num_rows = mysql_num_rows( $res );
    if ( $num_rows == 0 ) {
        print "<h4>Таблица '$tbl' в базе не найдена!</h4>";
        return 0;
    }
    return 1;
}
function set_view_cols( $view_name ) {
    global $Q;
    global $link;
    $arr_view_cols = array();
    $query = "desc $view_name";
    if ( $Q ) print "$query<br>";
    $res = mysql_query($query, $link);
    $num_rows = mysql_num_rows($res);
    for ( $i=0; $i<$num_rows; $i++ ) {
        $row = mysql_fetch_row( $res );
        $field = $row[0];
        $arr_view_cols[ $field ] = $i;
    }
    return $arr_view_cols;
} ?>

```

Для загрузки начальной страницы сайта используется файл index.php.

```

<html><head><meta http-equiv="Content-Type" content="text/html;
charset=windows-1251" /> <meta http-equiv="Cache-Control" content="no-
store" /> <meta http-equiv="refresh" content="0; url=login.php">
</head><body></body></html>

```

За решение задачи аутентификации отвечает файл login.php.

2.3 Организация доступа к web-сайту, аутентификация пользователей

Был разработан php модуль login.php, код которого представлен ниже

```

<?
require_once "constant.inc"; require_once "mysql.inc"; require_once "request.php";
$link = mysql_connect( $DBHOST, $DBUSER, $DBPASS ) or die ( "Could not connect" );
$res = mysql_query( "use $DB", $link ); if ( !$res ) die ( "Нет соединения с базой '$DB'" );
?>
<html> <head> <meta http-equiv=Content-Type content="text/html; charset=UTF-8">

```

```

<meta http-equiv="Pragma" content="no-cache">
<link rel="SHORTCUT ICON" href="favicon.ico"/>
<link type="text/css" rel="StyleSheet" href="my.css">
<script type="text/javascript" src="trim.js"></script>
<script>
<!--
function check_pass( form ) {
  if ( form.login.value.trim() == "" ) {
    alert( "Пожалуйста введите ИМЯ пользователя" );
    return false;
  }
  if ( form.password.value.trim() == "" ) {
    alert( "Пожалуйста введите ПАРОЛЬ доступа" );
    return false;
  }
  return true;
}
-->
</script>
</head>

```

```

<body bgcolor="<? print $COLOR; ?>">
<center>
<?
# нажали Выход
if ( isset($exit_flag) && $exit_flag == 1 ) {
  $sid = $_REQUEST['sid'];
  $query = "delete from session where sid='$sid'";
  if ($Q) print "$query<br>";
  mysql_query($query, $link);
  $query = "delete from connect where sid='$sid'";
  if ($Q) print "$query<br>";
  mysql_query($query, $link);
  $msg = 2;
}
# Форма для аутентификации
print "<h4><font color=#000065>Информационно-аналитическая система
трейдера.</font></h4>";
print "<p>Для входа в систему Вы должны ввести имя и пароль.</p>";
print "\n<form name=form_login action=\"first.php\" method=\"post\">\n";

print "<table border=\"0\" cellspacing=\"0\" cellpadding=\"0\"><tbody>\n";
print "<tr><th align=right>имя:</th><td><input name=\"login\" size=12
value=\"\"></td><td>&nbsp;</td>\n";
print "<tr><th align=right>пароль:</th><td><input name=\"password\" type=\"password\"
size=12 value=\"\"></td>\n";
print "<td>&nbsp;<input type=\"submit\" name=\"act_btn\" value=\"Вход\"
onClick=\"return check_pass(form_login);\"></td>\n";
print "</tbody></table>\n";
print "\n</form>";
if ( isset($msg) )
  switch ( $msg ) {
    case 1: print "<h4><font color=red>Неверное имя или пароль.</font></h4>"; break;

```

```

case 2: print "<h4><font color=red>Вы вышли из программы.</font></h4>"; break;
case 3: print "<h4><font color=red>Таблица 'auth' не найдена.</font></h4>"; break;
case 4: print "<h4><font color=red>Истек срок использования
программы!</font></h4>"; break;
}
mysql_close( $link );
?>
</center>
</body>
</html>

```

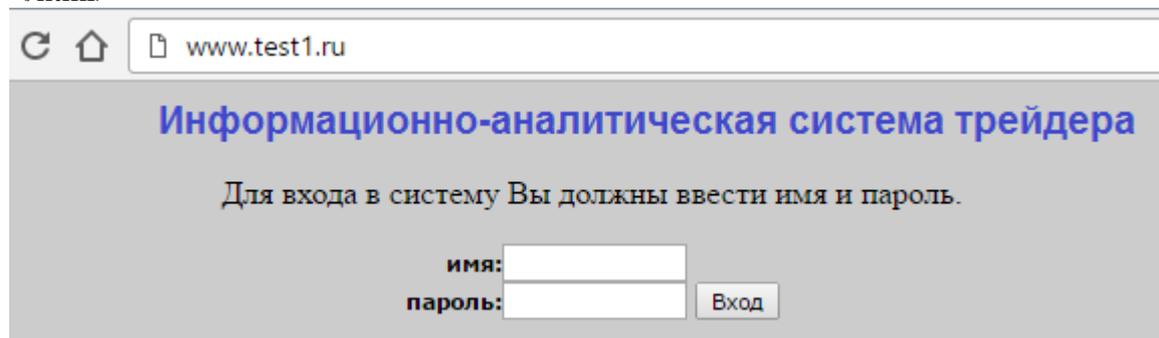


Рисунок 7 – скриншот интерфейса аутентификации пользователей разработанной системы

Модуль имеет типовую структуру, у пользователя запрашивается пара – логин и пароль. Для администрирования пользователей был разработан модуль `adm-1.php`, позволяющий регистрировать новых пользователей, ограничивать возможность использования системой до определенной даты, удалять пользователей, наделять пользователей специальным атрибутом, дающим право администрировать таблицу пользователей, т.е. присваивать пользователю права администратора (значение `adm_flag = 1`).

Текст разработанного модуля:

```

<? if (!isset($qmsg)) $qmsg="Вы успешно вошли в систему"; echo "<p>$qmsg</p>"; $adm_flag = 1;

```

Текущая дата. получаем список всех id

```

mysql_query("SET SESSION group_concat_max_len = 1000000", $link); $row =
mysql_fetch_row(mysql_query("SELECT group_concat(auth_id separator ',') from auth where
auth_id>1 order by auth_id", $link)); $all_id = $row[0]; $js_all_id_arr = "[".$all_id]";

```

получаем список всех логинов

```

$query = "select auth_id, auth_login, auth_password, auth_access, auth_fio,
DATE_FORMAT(auth_valid_date,'%d.%m.%Y') as auth_valid_date from auth where auth_id>1
order by auth_id desc";

```

```

$res = mysql_query($query, $link); $num_rows = mysql_num_rows($res);
    $cols = 6; $h = 30; print "\n<style type=\"text/css\">\n";
if (!strstr($agent, "MSIE")) print ".tableone {table-layout: fixed; border-collapse:collapse;}\n";
print ".tabletwo {table-layout: fixed; border-collapse:collapse;"; if (!strstr($agent, "MSIE")) print "
width: 100%;"; print "}\n";
print ".tableone {background:#669966; border:1px solid #000; color:#000;}\n";
print ".tableone td {border:1px solid #669966; color:#000; text-align:center;}\n";
print ".tableone tbody {background:#ccc; color:#000;}\n";
print ".tabletwo td {text-align:center;}\n"; print ".first {overflow-x:auto;}\n"; printf (".innerb
{height:%dem; overflow-y:scroll;}\n", $h); print "</style>\n";
    # число столбцов с данными + колонка под скроллбар
    $colspan = $cols + 1;
    # контейнеры для скроллинга таблицы
    print "<div class=\"first\" id=\"div_first\">\n"; print "<table class=\"tableone\"
cellpadding=\"5\">\n";
        # Печатаем шапку
print "<thead><tr> <td style=\"width:30px\" align=\"center\">№</td> <td style=\"width:200px\"
align=\"center\">Логин</td> <td style=\"width:100px\" align=\"center\">Пароль</td> <td
style=\"width:100px\" align=\"center\">Права</td> <td style=\"width:100px\"
align=\"center\">Срок до</td> <td style=\"width:200px\" align=\"center\">ФИО</td> <td
style=\"width:16px\"></td> </tr></thead>\n"; print "<tfoot><tr><td colspan=\"\$colspan\">всего:
$num_rows</td></tr></tfoot>\n"; print "<tbody>\n<tr><td colspan=\"\$colspan\" align=\"left\">\n";
    # таблица с данными
print "<div class=\"innerb\">\n<table class=\"tabletwo\" cellspacing=\"0\"
cellpadding=\"5\">\n<tbody>\n";
for ($i=1; $i<=$num_rows; $i++) {
    $row = mysql_fetch_row( $res ); $auth_id = $row[0]; $auth_login = $row[1];
    $auth_password = $row[2]; $auth_access = $row[3]; $auth_fio = $row[4];
    $auth_valid_date = $row[5]; print "<tr id=\"\$auth_id\" onclick=\"javascript:
click_row('\$auth_id','\$auth_login','\$auth_password','\$auth_access','\$auth_fio','\$auth_valid_date','\$js
_all_id_arr);\">
        <td style=\"width:30px\" align=\"center\">$i</td> <td style=\"width:200px\"
align=\"center\">$auth_login</td> <td style=\"width:100px\"
align=\"center\">$auth_password</td> <td style=\"width:100px\"
align=\"center\">$auth_access</td> <td style=\"width:100px\"

```

```

align="center">$auth_valid_date</td> <td style="width:200px"
align="center">$auth_fio</td> </tr>\n";
} // for
print "</tbody>\n</table>\n</div>\n"; # innerb
print "</td>\n</tr>\n</tbody>\n</table>\n</div>\n"; # first
echo "<br>";
// echo "Права: 1-обычный пользователь, 2-администратор";
print "<table border="0" cellspacing="0" cellpadding="2">\n";
print "<tbody>";
print "<tr><th align="right">Логин</th><td><input type="text" name="new_login"
size="20"></td></tr>";
print "<tr><th align="right">Пароль</th><td><input type="text"
name="new_password" size="20"></td></tr>";
print "<tr><th align="right">Права</th><td><input type="text" name="new_access"
size="4">1-пользователь, 2-администратор</td></tr>";
print "<tr><th align="right">Срок до</th><td><input type="text"
name="new_valid_date" size="16"></td></tr>";
print "<tr><th align="right">ФИО</th><td><input type="text" name="new_fio"
size="50"></td></tr>";
print "</tbody>\n"; print "</table>";

# кнопки редактирования данных
print "<table border="0" cellspacing="0" cellpadding="5"><tbody>\n"; print "<tr>"; print
"<td><input type="submit" value="добавить" name="db_process_btn" class="fixed_btn"
onClick="javascript: return add_row();"></td>\n"; print "<td><input type="submit"
value="изменить" name="db_process_btn" class="fixed_btn" onClick="javascript: return
chg_row();"></td>\n"; print "<td><input type="submit" value="удалить"
name="db_process_btn" class="fixed_btn" onClick="javascript: return del_row();"></td>\n";
print "</tr>\n"; print "<tr>\n"; print " <td colspan="3">Изображение: <input
name="adm_selfoto_btn" type="file" size="32"> <input name="db_process_btn"
type="submit" value="загрузить" onClick="javascript: return
check_filename();"></td>";print "</tr>\n"; print "<tr>\n"; print "<td align="left"
colspan="3">";

# Календарная дата

```

```

print "Календарная дата:\n"; print "<select name=\"cal_day\">\n"; if (
!isset($cal_day) ) $cal_day = $nday; for ( $i=1; $i<=31; $i++ ) { print "<option
value=\"$i\""; if ( $cal_day==$i ) print " selected"; printf(">%02d</option>\n", $i);
}print "</select>";

```

Месяц

```

print "<select name=\"cal_mon\">\n"; if ( !isset($cal_mon) ) $cal_mon = $nmon;
$i = -1; foreach ( $MONTH as $mon ) { $i += 1;
print "<option value=\"$i\""; if ( $cal_mon==$i ) print " selected"; print
">$mon</option>\n"; } print "</select>";

```

Год

```

print "<select name=\"cal_year\">"; if ( !isset($cal_year) ) $cal_year = $nyear;
foreach ( $YEAR as $y ) { print "<option value=\"$y\"";
if ( $cal_year==$y ) print " selected"; print ">$y</option>\n"; } print "</select>\n"; print
"&nbsp;<input type=\"submit\" value=\"сбросить\" name=\"caldate_btn\" class=\"fixed_btn\"
onClick=\"javascript: return remove_caldate_row();\" disabled>\n"; print "</td>\n";
print "</tr>\n"; print "</tbody></table>\n";

```

Изображение

```

print "<table border=\"0\" cellspacing=\"0\" cellpadding=\"2\"><tbody>\n"; print "<tr>"; print "<td
align=\"center\">gbp</td>"; print "<td align=\"center\">eur</td>"; print "<tr>"; print
"<td><textarea name=\"eur_comm\" rows=\"4\" cols=\"32\">$eur_comm</textarea></td>";
print "</tr>\n"; print "<tr>"; print "<td colspan=\"12\" align=\"center\"><input
type=\"submit\" name=\"db_process_btn\" value=\"установить комментарии к
финансовому инструменту\"></td>"; print "</tr>\n"; print "</tbody></table>\n";print
"<hr>"; $fname_arr = array(); $r_count = 0; print "<table border=\"1\" cellspacing=\"0\"
cellpadding=\"2\"><tbody>\n"; i = 0;
print "</tbody></table>\n"; ?>

```

Было выполнено тестирование разработанного скрипта, показавшее, что корректность его работы. Обеспечивается возможность однофакторной аутентификации на основе использования пары логин – пароль, однако целесообразно усилить защиту системы обеспечив возможность прохождения двухфакторной аутентификации на основе использование аппаратного токена ruToken Web.

Календарная дата: 05 февраль Опционный месяц, год: февраль
2017 2017

Дата выхода бюллетеня: 03 февраль 2017

| Границы рынка | | | |
|---------------|------------|-------|-------|
| Валюта | Дата | CALL | PUT |
| eur | 01.02.2017 | 1.050 | 1.100 |
| eur | 05.02.2017 | 0 | 1.030 |
| eur | 26.01.2017 | 1.050 | 1.100 |

mysql-5.5 ▶ data ▶ fxdb

| Имя | Тип |
|------------------|------------|
| auth.frm | Файл "FRM" |
| db.opt | Файл "OPT" |
| eur.frm | Файл "FRM" |
| sample_users.frm | Файл "FRM" |
| sample_users.MYD | Файл "MYD" |
| sample_users.MYI | Файл "MYI" |

Рисунок 8 – скриншот интерфейса формы с информацией о границах рынка (CALL – BGR – верхняя граница рынка, PUT – NGR – нижняя) граница рынка, ниже файлы таблиц БД формата MySQL.

Полная подборка разработанных модулей информационно-аналитической системы представлена на DVD диске, прилагаемой к записке дипломной работы. Следует отметить, что кроме получения информации о верхней и нижней границе рынка пользователи системы могут видеть дополнительную информацию, отображаемую ниже таблицы в виде картинки. Аналитик, который на равне с системным администратором может быть задействован в обслуживании информационной системы, может помещать дополнительную информацию с рекомендациями о торговле.

3 Организация двухфакторной аутентификации пользователей с помощью аппаратных ключей Рутокен Web. Разработка специализированного клиента для доступа к сайту системы и защита его ключами HASP

Рассмотрено использование персонального средства аутентификации в формате USB-ключа – Рутокен Web [4], а также программное решение с его использованием. Аппаратный ключ выступает в роли компонента системы аутентификации (проверка соответствия пользователя его идентификатору) и идентификации (процесс распознавания пользователя по его идентификатору) пользователя. Преимущество Рутокен Web в том, что он, как средство аутентификации поддерживается большинством современных операционных систем, бизнес-приложений и продуктов по информационной безопасности, а минус его заключается в относительной дороговизне устройства (Электронный идентификатор Актив Рутокен Web 1151 руб. http://www.xcomspb.ru/aktiv_rytoken_web_245350.html).

3.1 Разработка и тестирование php модуля двухфакторной аутентификации с использованием аппаратных ключей Рутокен Web

Для разработки специализированного php модуля для информационной системы использовали универсальные модули, рекомендуемые разработчиками программно-аппаратного решения (доступны для загрузки по ссылке <https://www.rutoken.ru/products/all/rutoken-web/#implementation>).

Для хранения данных была сгенерирована таблица, формируемая следующим запросом:

```
CREATE TABLE 'sample_users' (  
  'user_id' int(11) unsigned NOT NULL auto_increment,  
  'user_login' varchar(30) NOT NULL,  
  'user_xkey' varchar(64) NOT NULL,  
  'user_ykey' varchar(64) NOT NULL,  
  'r_xkey' varchar(64) NOT NULL,
```

'r_ykey'

PRIMARY KEY ('user_id')

) ENGINE=MyISAM DEFAULT CHARSET=utf8 AUTO_INCREMENT=1 ;");

Далее с официального сайта rutoken.ru был скачан набор для PHP разработчика. Были использованы только два файла из этого инструментария это:

1. login.php;

2. register.php.

Login.php — используется для аутентификации пользователя.

Register.php используется для регистрации и генерации открытого и закрытого ключей. При успешной регистрации, в памяти USB-токена сохраняется ключевая пара (e_(Login, SiteName),d_(Login, SiteName)), предназначенная для защищенной аутентификации пользователя с логином Login на Web-сайте Установка соответствия между открытым ключом e_(Login, SiteName) и логином Login осуществляется на стороне сервера (Web-сайта). Пользователь может повторно пройти процедуру регистрации на Web-сайте, но уже с другим логином. Количество повторных регистраций на одном и том же Web-сайте ограничено только объемом доступной памяти USB-токена, предназначенной для хранения контейнеров. Выполнив настройку вводим адресу <http://www.test1.ru/register.php>. Отображается форма для ввода логина. Подключив электронный ключ, ввели в поле ввода логина Usertest и нажали «Зарегистрироваться» (Рис. 9). Система попросила ввести ПИН-Код Рутокен Web, был введен код «088152». Система завела открытый и закрытый ключ для пользователя «Usertest».

Регистрация нового пользователя

Для регистрации выберите логин и нажмите кнопку «Зарегистрироваться». Логин пользователя должен состоять из цифр и букв латинского алфавита (любого регистра), а также иметь длину не менее трех и не более тридцати символов.

Логин пользователя:

Зарегистрироваться

Краткая справка

В случае успешной регистрации, будет сгенерирована ключевая пара ($e_{(\text{Login}, \text{SiteName})}, d_{(\text{Login}, \text{SiteName})}$), предназначенная для защищенной аутентификации пользователя с логином **Login** на Web-сайте **SiteName**:

- $e_{(\text{Login}, \text{SiteName})}$ — открытый ключ — хранится на Рутокен Web, передается на Web-сайт и привязывается к логину пользователя;
- $d_{(\text{Login}, \text{SiteName})}$ — закрытый ключ — хранится на Рутокен Web и не может быть извлечен из памяти USB-токена.

Таким образом, на сервере сохраняется пара ($\text{Login}, e_{(\text{Login}, \text{SiteName})}$). Пользователь может повторно пройти процедуру регистрации на Web-сайте, но уже с другим логином. Количество повторных регистраций на одном и том же Web-сайте ограничено только объемом доступной памяти USB-токена, предназначенной для хранения контейнеров.

Рисунок 9 – инструмент разработчика PHP для Рутокен Web

Теперь открытый ключ хранится в базе данных, а закрытый ключ на Рутокен Web. Двухфакторная защита представляет собой использование аппаратного ключа и пин-кода, который необходимо ввести для подтверждения регистрации. Следующим шаг – внедрение аутентификации в информационную систему посредством Рутокен Web.

Внедрение двухфакторной аутентификации и проверка защиты – система для проверки прав пользователя предусматривает форму ввода логина и пароля. Форма для однофакторной аутентификации представлена рис. 7. Необходимо добавить возможность двухфакторной аутентификации, используя электронный ключ, поэтому в этот php модуль будет добавлена форма аутентификации и регистрации при успешной проверке прав.

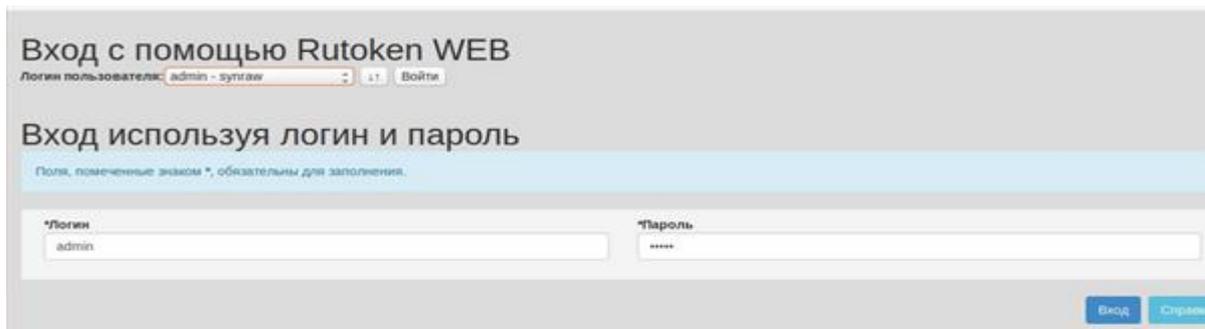


Рисунок 10 – страница аутентификации с возможностью входа используя электронный ключ Рутокен Web.

Видно, что на рисунке 10, появилась возможность выбора «Логина пользователя», кнопки «обновить», и кнопки «войти». Теперь аутентификация может работать следующим образом:

- Пользователь может использовать логин и пароль.
- Пользователь может использовать электронный ключ.

Аутентификация посредством электронного ключа проходит в 3 этапа:

1. Попадая на сайт <http://www.test1.ru/> необходимо нажать на кнопку «Войти», предварительно подключив электронный ключ Рутокен Web.
2. На странице аутентификации выбрать нужный логин из выпадающего списка, нажать «войти».
3. После успешной проверки прав, необходимо нажать «Админ панель» (Эта кнопка появляется только при успешной аутентификации)

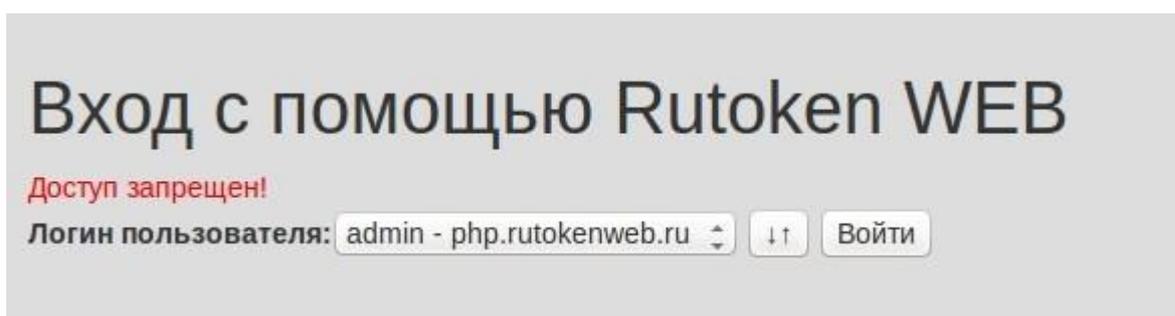


Рисунок 11 – аутентификация возможна только с корректно настроенным ключом Рутокен Web.

Теперь проверяем возможность аутентификации используя другой «контейнер» на этом USB Рутокен Web, который принадлежит другому сайту.

На главной странице сайта нажали кнопку «Войти», в выпадающем списке логинов rutoken выбрали логин, который не принадлежит этому домену, и нажали войти. Появилась надпись: «Доступ запрещен», и кнопки «Админ Панель» не появилось (Рис. 11).

Рассмотрим страницу аутентификации без ключа rutoken. Извлекли ключ из USB порта и перешли на страницу аутентификации. На странице пропало выпадающее меню с логинами, зарегистрированными на Рутокен Web и войти также не удастся. Подключив ключ и нажав на «обновить» (кнопка со стрелками вверх и вниз) список выбора логинов вновь появился, можно выбрать необходимый логин и пройти аутентификацию снова.

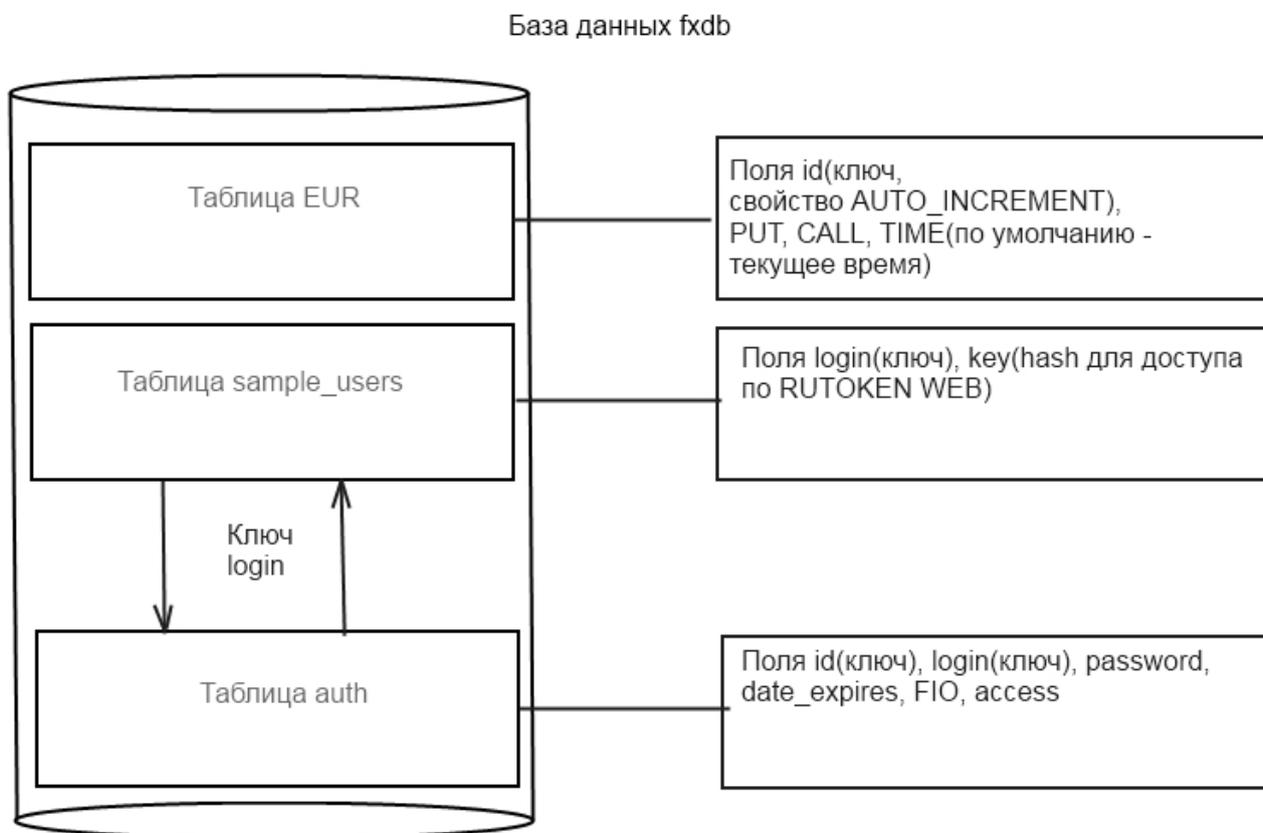


Рисунок 12 – в таблицы добавлены поля, поддерживающие работу с Рутокен Web

После интеграции с усиленной системой защиты таблицы БД fxdb имеют вид (Рис. 12): таблица EUR содержит данные по финансовому инструменту EUR/USD, она заполняется на сервере в автоматическом режиме. Таблица auth

содержит логины и пароли пользователей системы, информацию об окончании срока лицензии пользователя и его правах доступа. Таблица `sample_users` сопряжена с таблицей `auth`, в ней хранятся данные для доступа по ключу Рутокен Web. Реализована возможность использования USB-токена вместо стандартной процедуры аутентификации парой логин/пароль. В результате выполненного тестирования можно сделать выводы о том, что с технической точки зрения использование усиленной системы защиты, поддерживающей двухфакторную аутентификацию на основе Рутокен Web, технически возможно и целесообразно. Однако окончательное решение должно быть принято с учетом экономической целесообразности использования данного относительно дорогого программно-аппаратного решения.

3.2 Разработка специализированной программы-клиента для подключения к информационно-аналитической системе

Для разработки специализированного клиента было принято решение использовать объектно-ориентированный язык высокого уровня Паскаль, представленный средой разработки Delphi. Средство разработки программного кода было выбрано исходя из того, что данный язык изучался ранее, кроме того средой разработки поддерживается компонент `WebBrowser`, позволяющий достаточно просто отображать веб-страницы. Например, для вызова и отображения страницы Яндекс может быть использован следующий программный код, обрабатываемый после нажатия кнопки:

```
procedure TForm1.Button1Click(Sender: TObject);  
begin WebBrowser1.Navigate('http://yandex.ru/');  
end;
```

Компонент `WebBrowser` позволяет выполнять запросы, используя методы `get` и `post`.

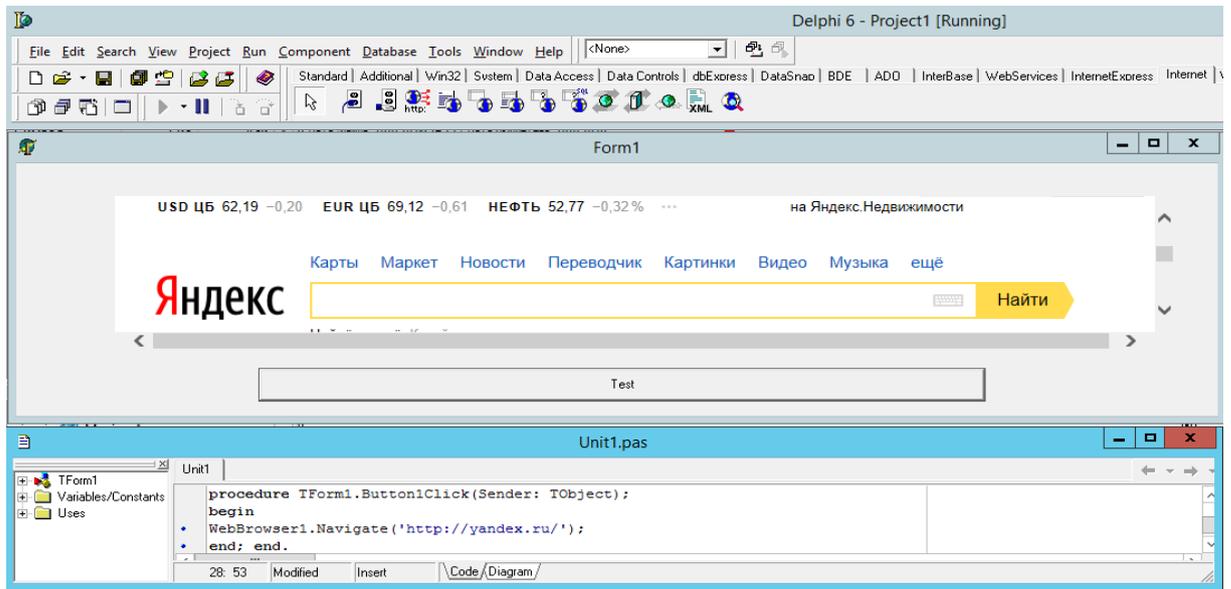


Рисунок 13 – разработка тестового приложения с использованием компонента WebBrowser

Программный код основного модуля (Unit1.pas) разработанного клиента, позволяющего подключаться к информационной системе без многократного ввода логина и пароля (можно сохранить в файле настроек), возможность сохранять получаемую информацию в файл, печать информации в удобном для трейдера виде и пр. Дополнительные опции, облегчающие работу трейдера, могут быть запрограммированы при необходимости.

```

unit Unit1;
interface
uses
  Windows, Messages, SysUtils, Classes, Graphics, Controls, Forms, Dialogs,
  ExtCtrls, OleCtrls, SHDocVw, StdCtrls, Buttons, Menus;
type
  TForm1 = class(TForm)
    Panel1: TPanel; WebBrowser1: TWebBrowser; Edit1: TEdit;
    START: TBitBtn; Timer1: TTimer; MainMenu1: TMainMenu;
    File1: TMenuItem; Exit1: TMenuItem; N1: TMenuItem;
    Print1: TMenuItem; N2: TMenuItem; User1: TMenuItem;
    UsePrinter1: TMenuItem; About1: TMenuItem;
  procedure WebBrowser1DocumentComplete(Sender: TObject;
    const pDisp: IDispatch; var URL: OleVariant);
  procedure WebBrowser1NewWindow2(Sender: TObject; var ppDisp: IDispatch;
    var Cancel: WordBool);
  procedure BitBtn1Click(Sender: TObject);
  procedure STARTClick(Sender: TObject);
  procedure Timer1Timer(Sender: TObject);
  procedure Exit1Click(Sender: TObject);
  end;

```

```

    procedure Print1Click(Sender: TObject);
    procedure User1Click(Sender: TObject);
    procedure UsePrinter1Click(Sender: TObject);
    procedure About1Click(Sender: TObject);
    procedure FormClose(Sender: TObject; var Action: TCloseAction);
    private
    { Private declarations }
    procedure WMMouseActivate(var Msg: TMessage); message
WM_MOUSEACTIVATE;
    public
    { Public declarations }
end;
var
Form1: TForm1;
flag: integer;
s:string;
_URL, Flags, TargetFrameName, PostData, Headers: Olevariant;
implementation
    {$R *.DFM}
    uses mshtml, Unit2, Unit3;
    procedure TForm1.WMMouseActivate(var Msg: TMessage);
begin
    try
        inherited;
        if Msg.LParamHi = 516 then
            Msg.Result:= MA_NOACTIVATEANDEAT;
        except
        end;
    end;
    procedure TForm1.WebBrowser1DocumentComplete(Sender: TObject;
const pDisp: IDispatch; var URL: OleVariant);
begin //
if flag=0 then
begin
Edit1.Text:=WebBrowser1.LocationURL;
s:=Edit1.Text;
Delete(s,32,5);
Edit1.Text:=s;
end;
end;
    procedure TForm1.WebBrowser1NewWindow2(Sender: TObject;
var ppDisp: IDispatch; var Cancel: WordBool);
var newForm:TForm1;
begin //
newForm:=TForm1.Create(Application);
newForm.Show;
ppDisp:=newForm.WebBrowser1.ControlInterface;
end;
    procedure TForm1.BitBtn1Click(Sender: TObject);
begin
    Edit1.Text:=s;
    _URL:=s;
    flag:=1;

```

```

    Flags := 0; TargetFrameName := 0; Postdata := 0; Headers := 0;
    WebBrowser1.Navigate2(_URL, Flags, TargetFrameName, PostData, Headers);
end;
procedure TForm1.STARTClick(Sender: TObject);
var
s:string;
begin
User1.Visible:=false;
    flag:=0;
    s:="";
    s:=Form2.login.Text;
if Form2.RadioButton1.Checked=true then
    begin
        _URL
:= 'http://www.test1.ru/first.php?act_btn=%D0%92%D1%85%D0%BE%D0%B4&login=demouser
&password=demouser_pass';
        end
    else
        if Form2.RadioButton2.Checked=true then
            if length(s)>0 then
                _URL
:= 'http://www.test1.ru/first.php?act_btn=%D0%92%D1%85%D0%BE%D0%B4&login='+Form2.l
ogin.Text+'&password='+Form2.password.Text
            else
                _URL := 'http://www.test1.ru/';
                Flags := 0; TargetFrameName := 0; Postdata := 0; Headers := 0;
                WebBrowser1.Navigate2(_URL, Flags, TargetFrameName, PostData, Headers);
                START.Visible:=false;
                Timer1.Enabled:=true;
            end;
        procedure TForm1.Timer1Timer(Sender: TObject);
        begin
            if ((Pos('base.php',s)>0) and (Form2.CheckBox1.Checked=true)) then
            begin
                Edit1.Text:=s;
                _URL:=s;
                flag:=1;
                Flags := 0; TargetFrameName := 0; Postdata := 0; Headers := 0;
                WebBrowser1.Navigate2(_URL, Flags, TargetFrameName, PostData, Headers);
                Timer1.Enabled:=false;
            end;
        end;
        procedure TForm1.Exit1Click(Sender: TObject);
        begin
            Close;
        end;
        procedure TForm1.Print1Click(Sender: TObject);
        var
        vaIn, vaOut: OleVariant;
        begin
            try
                inherited;
                WebBrowser1.ControlInterface.ExecWB(OLECMDID_PRINT,
OLECMDEXECOPT_DONTPROMPTUSER, vaIn, vaOut);

```

```

        except
        end;
end;
procedure TForm1.User1Click(Sender: TObject);
begin
Form2.Visible:=true;
end;
procedure TForm1.UsePrinter1Click(Sender: TObject);
begin
WebBrowser1.ExecWB(OLECMDID_PRINT, OLECMDEXECOPT_DODEFAULT);
end;
procedure TForm1.About1Click(Sender: TObject);
begin
Form3.Visible:=true;
end;
procedure TForm1.FormClose(Sender: TObject; var Action: TCloseAction);
var
f:textfile;
begin
assignfile(f,'web_forex_cme.txt');
Rewrite(f);
writeln(f,Form2.login.Text);
writeln(f,Form2.password.Text);
CloseFile(f);
end;
end.

```

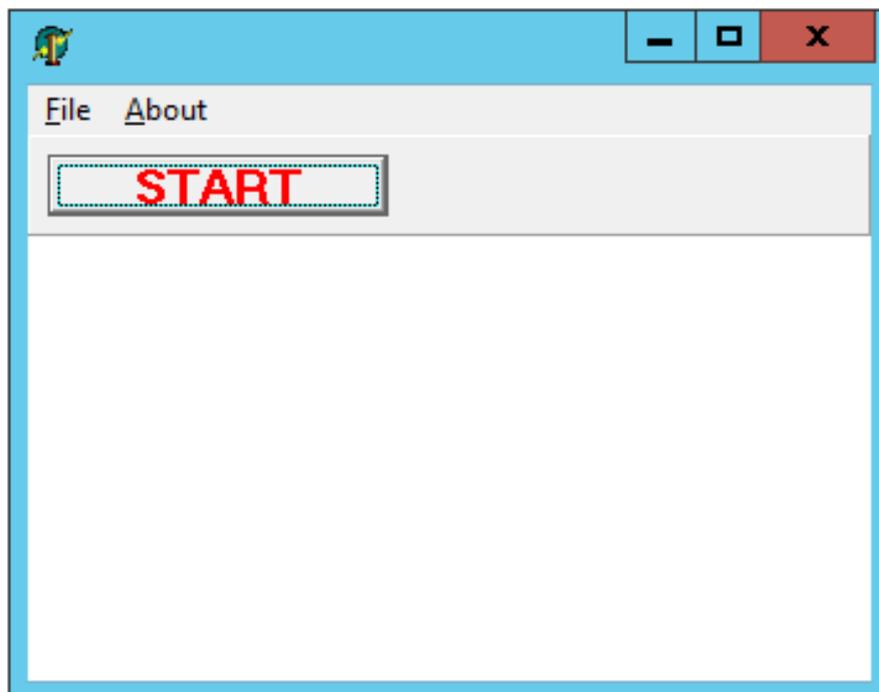


Рисунок 14 – вид интерфейса главной формы клиента

На рисунке 14 представлен общий вид интерфейса разработанной программы. Программа позволяет вводить и сохранять в файле настройки для

работы в демонстрационном (демо пользователь) и в полнофункциональном режиме (Рис. 15), информация о разработчике программы может быть получена при обращении к пункту меню About (Рис. 16).



Рисунок 15 – возможность сохранять настройки для входа в систему

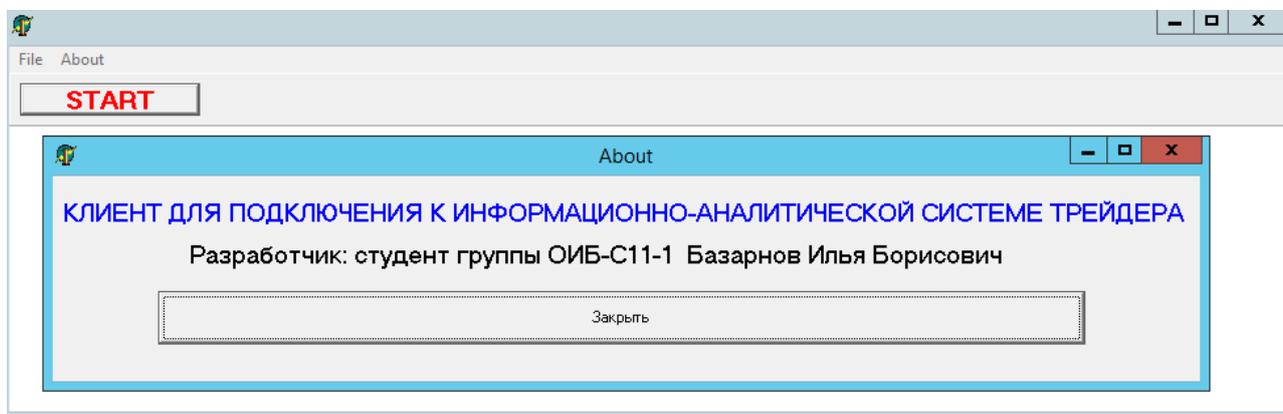


Рисунок 16 – окно с информацией о разработчике программы

На рисунке 17 приведен скриншот отображающий рабочие данные по граница рынка, после того, как клиент вошел в информационно-аналитическую систему и получил данные с web-сайта информационной системы.

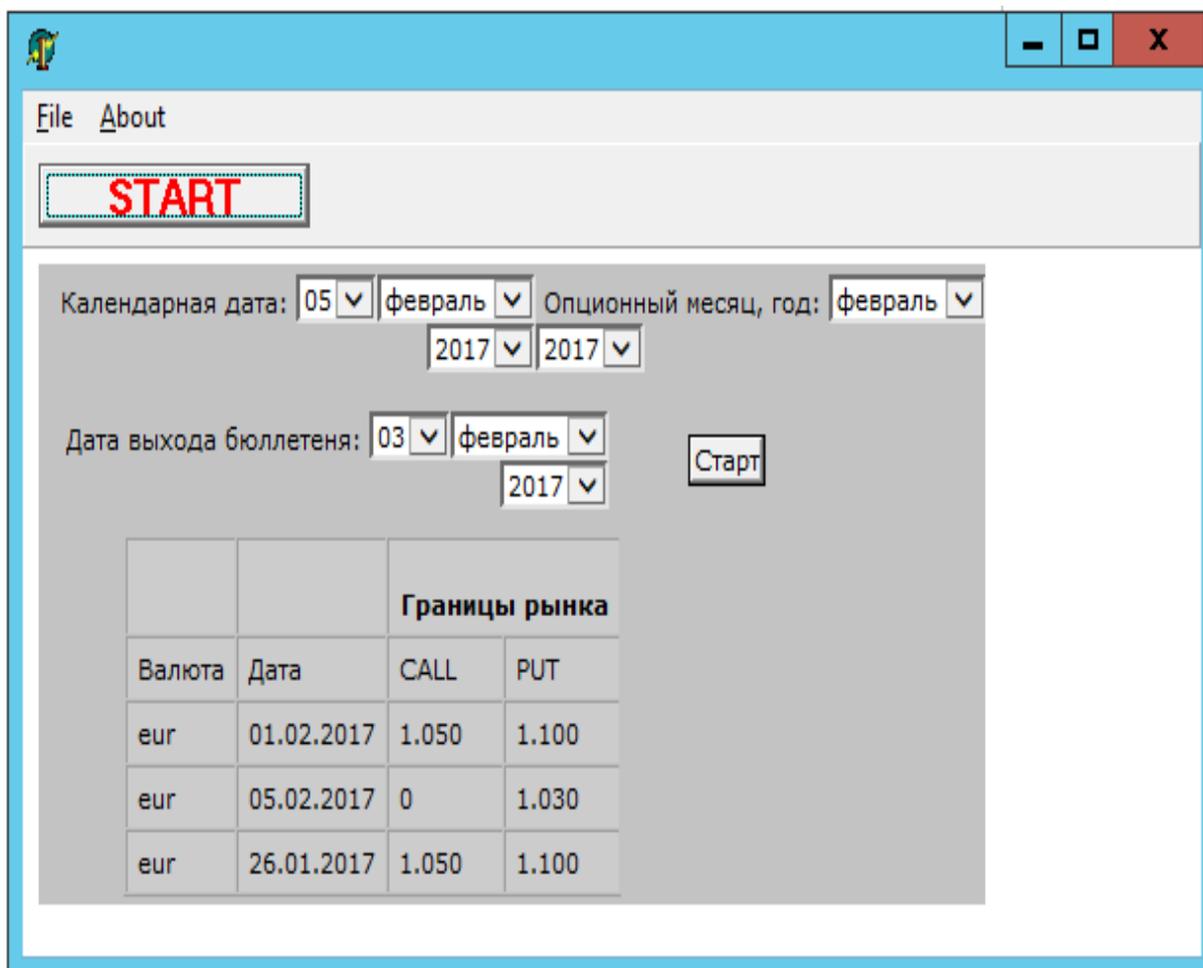


Рисунок 17 – клиент получил данные с web-сайта информационной системы

Следует отметить, что в ходе разработки было создано и успешно протестировано в работе программное обеспечение, которое можно рассматривать как небольшой, но вполне самостоятельный программный продукт для работы с сайтом информационной системы. Разработанное ПО может быть взято за основу для разработки более функциональной версии программы-клиента, которую можно дополнить возможностями расширенного протоколирования действий пользователя, запись полученных данных на дисковые носитель в разных форматах, возможность выгрузки и отправки информации из программы клиента в виде почтовых, sms или push сообщений по указанным пользователям координатам. В целом все базовые поставленные задачи, связанные с разработкой и тестирование программы-клиента для работы с сайтом информационно-аналитической системы, были успешно выполнены.

3.3 Защита специализированной программы-клиента для подключения к информационно-аналитической системе ключами серии Hasp

Одним из имеющихся сформированных и наиболее распространенных средств защиты и лицензирования является решение программно - аппаратной защиты HASP SRM. Santinel HASP SRM (Hardware Against Software Piracy) – система, предназначенная для лицензирования и защиты программного обеспечения от несанкционированного использования, нелегального распространения, модифицирования и аутентификации пользователей при доступе к защищенным ресурсам при помощи программных или аппаратных ключей защиты. Каждый ключ содержит микроконтроллер, имеющий свой уникальный алгоритм работы. При запуске приложение будет требовать присоединение ключа. Комплекс является разработкой российской компании Aladdin Knowledge SystemsLtd. Более половины разработчиков в мире используют защиту программ с помощью HASP SRM, так как она наиболее проста в реализации, обладает высокой надежностью в соотношении цена/качество и гибкостью.

При выборе средства защиты, необходимо учитывать соотношение себестоимость продукта/последствия и потери при взломе. Если при взломе потери будут невелики, да и стоимость самого проекта не слишком высока, то нет необходимости ставить дорогостоящую защиту. И, напротив, если важность продукта и стоимость его разработки высоки, то есть смысл ставить дорогостоящую, надежную защиту и тем самым избежать потерь от взлома, который в данном случае маловероятен. Ключи HASP SRM реализуют шифрование с помощью алгоритма AES 128.

Состав программного пакета HASP SRM Vendor Suite:

- HASP SRM Envelope – приложение для навесной защиты продуктов.
- HASP SRM Toolbox – приложение для генерации кода, внедряемого в исходный код приложения, которое подвергают защите.

- HASP SRM Business Studio – приложение для разработки, создания и обновления лицензии для программного обеспечения и форматирования памяти ключей.
- HASP SRM Run-Time Envelopment – приложение для поддержки связи между ключом и приложением под защитой после того, как пользователь выполнит его установку на своем компьютере.
- HASP SRM Run-Time API – приложение, для реализации встраиваемой защиты, путем внедрения в исходный код API - вызовов.
- HASP SRM Control Center – веб - приложение для удаленного обновления лицензий.

Покупаемый у производителя комплект SDK (Software Developer Kit) включает в себя:

- мастер-ключ, который позволяет создавать лицензии, вносить изменения в условия лицензии, которая уже находится в эксплуатации, устанавливая связь с ключами и записывать данные в память ключей;
- пользовательские ключи (HASP HL, HASP SL). Все они, кроме версии Basic, имеют встроенную память с возможностью записи и чтения данных;
- так же в комплекте есть подробные примеры работ и фрагменты кода.

При размещении первого заказа на сайте производителя системы защиты, разработчику присваивается уникальный код (код разработчика), который хранится в памяти мастер – ключа, и позволяет ПО обмениваться данными с ключами, код должен оставаться секретным. Так же при заказе ключам присваивается код серии, в которой содержится код разработчика, код серии печатается на корпусе ключей.

У разработчиков есть два варианта защиты своего продукта, можно выбрать тип ключа по своему усмотрению уже после установки защиты:

- с помощью аппаратных ключей HASP HL (подключаемые к USB-порту компьютера), которые предоставляют более надежную защиту;

- с помощью ключей HASP SL (программный аналог), обеспечивающий более простой и гибкий способ защиты, но с привязкой к конкретному устройству. Такой вариант удобен для распространения продуктов в сети Интернет.

Функционал ключей одинаков, различия в том, что данные программных ключей хранятся не в самом ключе, а в защищенном хранилище в памяти компьютера.

В выполненной работе для защиты программного обеспечения использовались ключи HASP HL. Особенности ключей HASP HL:

- предоставляют более надежную защиту;
- позволяют строго следовать условиям лицензии, так как эти условия хранятся в памяти ключа;
- использование программного обеспечения на любом устройстве при наличии ключа;
- не требует подключения к сети Интернет для активации продукта.

Принцип работы аппаратных ключей. В процессе запуска и выполнения работы программа, на которую устанавливают защиту, обращается к ключу HASP, и если ключ дает верный ответ и работает по необходимому алгоритму, то сбои в работе программы отсутствуют. Если же ключ дает неверный ответ, и ключ вовсе отсутствует, то программа завершает работу совсем или переходит в демонстрационный режим с ограниченными возможностями.

Особенности ключей HASP SL:

- минимальные временные затраты на установку защиты, можно сразу активировать и использовать продукт, следуя условиям лицензии;
- прямая связь с пользователем дает возможность собирать информацию использовать ее для маркетинговых целей.

Способы защиты программного обеспечения. Достоинства и недостатки. Можно реализовать навесную защиту готовых продуктов (exe-файлов, dll-библиотек, интернет страниц и Java-приложений) автоматически с помощью механизма HASP Envelope, использующий код шифрования AES/128 и/или встраиваемую защиту вручную с помощью библиотечных функций обращения

к ключу (функции API — Application Program Interface). Достоинствами навесной защиты является то, что:

- установка защиты реализуется достаточно быстро и просто, почти автоматически;
- для того, чтобы установить защиту, нет необходимости иметь какие-либо навыки программирования;
- устанавливается на абсолютно любую программу (даже без доступа к ее исходному коду).

Недостатки данного решения:

- защита хорошо "навешивается" только на стандартный код программирования, если структура исполняемого файла не стандартна, то возникают ошибки;
- навесная защита – самая распространенная, большое число хакеров могут пробовать свои силы для обхода или взлома этого типа защиты.

Целесообразно использовать навесную защиту, когда защита программы отсутствует, установка защиты существенно затрудняет взлом программы. Более эффективным решением можно считать использование навесной в совокупности со своей собственной уникальной защитой. Когда разработчик программного обеспечения располагает достаточным количеством времени, финансов и имеет квалифицированных специалистов по защите программного обеспечения, то имеет смысл реализовать встроенную, более стойкую защиту с помощью приложения HASP SRM Run-Time API, путем внедрения в код разработчика API - функций.

Достоинства встраиваемой защиты:

- быстрая и простая установка, нет необходимости настраивать отдельное приложение для защиты;
- маловероятное возникновение конфликтов между модулями продуктов.

Недостатки встраиваемой защиты:

- необходимо более высокая квалификация специалистов;

- система становится менее гибкой, если защита организована под определенное оборудование;
- для встраиваемой защиты часто используются сторонние приложения, если в них возникает ошибка, то до момента обновления приложения продукт находится под угрозой.

Для реализации усиленной защиты, целесообразно установить комбинированную защиту, т.е. объединить оба вида защиты.

Лицензирование защиты. Суть лицензирования – важно следить за тем, кто использует разработанный продукт, соблюдают ли пользователи требования по использованию продукции. Если продукция распространяется в тестовом бесплатном режиме, то тестирование должно быть ограниченным по времени или количеству запусков. Задачей лицензирования является привязка ключа к компьютеру, или пользователю. Для этого необходимо связаться с производителем, который высылает ключ с уникальным идентификационным номером. Предварительно заказчиком заполняется анкета на сайте производителя и туда же пересылается идентификационный номер компьютера для генерации ключа, в котором будет содержаться зашифрованная информация о пользователе, продукте и условиях лицензии.

Виды лицензии:

- "одна лицензия – один компьютер"
- "одна лицензия – один пользователь"

HASP SRM предоставляет свободу выбора в реализации модели лицензирования, ориентируясь на изменения потребительского спроса. Есть готовая модель, функции которой можно использовать отдельно или совместно:

- демонстрационная версия HASP SRM Demo (оплата после окончания тестирования);
- подписка, аренда, прокат;
- оплата отдельных модулей;
- оплата отдельных функций;
- ограничение лицензии по времени;

- ограничение лицензии по количеству запусков.

Для разработки своего собственного лицензионного плана необходимо:

- провести анализ приложения, выделить в нем компоненты и/или функции, которые будут подвергаться лицензированию;
- объединить все функции и компоненты необходимые для пользователя;
- выбрать ключи защиты, которые будет поставляться пользователю в комплекте с продукцией;
- определить условия лицензии.

Главным конкурентом ключей HASP являются электронные ключи Guardant, предназначенные для защиты программного обеспечения от несанкционированного копирования и распространения. Ключи являются разработкой российской компании "Актив". Состав комплекта разработчика Guardant – комплект разработчика включает в себя:

- набор утилит для установки приложения;
- набор утилит, устанавливающих автоматическую защиту приложений (не нужно знать исходного программного кода, не нужны навыки программирования);
- библиотеки с API-ключами, для создания собственных уникальных алгоритмов защиты на различных языках программирования;
- примеры работ с ключом;
- обучающие документы, содержащие рекомендации по работе с комплектом разработчика.

С использованием технологий Guardant защита может быть реализована следующим образом:

- автозащита (с помощью Мастера лицензирования);
- полуавтоматический режим защиты (режим работы под контролем профилировщика);
- полностью ручной режим защиты (создание собственных механизмов защиты с помощью Guardant API).

Особенности ключей Guardant:

- в ключах реализован симметричный алгоритм шифрования, на нем так же основана генерация псевдослучайных чисел;
- наличие электронной цифровой подписи;
- модель с возможностью работы в сети;
- модель с батарейкой и часами реального времени;
- модель, с возможностью загрузки собственного кода на C/C++;
- дистанционное безопасное обновление памяти.

Главными отличиями от ключей HASP являются:

- поддержка неограниченной лицензии;
- есть возможность выполнения кода внутри ключа;
- экономия средств (т.к. не нужно приобретать 2 ключа: мастер-ключ и ключ разработчика, как у HASP);
- возможность работы на операционных системах Windows и Linux (HASP поддерживает только Windows).

Нельзя однозначно сказать какое средство защиты лучше. Каждый разработчик вправе выбирать то средство защиты, которое ему больше подходит [4].

Для установки навесной защиты был использован демонстрационный комплект ключей HASP HL серии DEMOMA и полнофункциональный серии CRAZX. Для установки навесной защиты программного пакета HASP SRM Vendor Suite использовались приложения:

- HASP SRM Envelope – приложение для установки и настройки параметров многослойной навесной защиты. Наличие защиты никак не влияет на работу приложения, только запрашивает ключ при его отсутствии при запуске приложения.
- HASP SRM Business Studio – это средство для управления бизнес – процессами: лицензирование продукта, создание продукта, распространение продукции и удаленное обновление программного обеспечения, а так же активация программных продуктов.

В приложении HASP SRM Business Studio ведется работа с компонентами, настройка параметров защиты компонентов, включение компонентов в состав продукта. Компонент – это целое приложение или отдельные его части и даже функции. Лицензионные настройки могут применяться к каждому компоненту по – отдельности.

Продукт может состоять из некоторого количества компонентов – до 64 000. Компоненты можно включать при необходимости в состав любых продуктов, но их свойства нужно изменять до включения в продукт, так как после добавления не будет возможности менять их свойства или удалять их. Оформление: продукт будет состоять из одного компонента, лицензионные настройки будут «без ограничений», навесная защита программного обеспечения будет выполнена с помощью ключа HASP HL, так же будет выполнена привязка к аппаратному ключу HASP HL для того, чтобы продукт можно было использовать только с ключом.

Установка программного пакета Sentinel HASP – v.5.10 и создание полнофункционального лицензионного продукта:

- Необходимо установить программный пакет HASP SRM с CD-диска, следуя инструкциям программы – мастера.
- Далее выполнить следующие действия для запуска HASP SRM Vendor Suite: из меню «Пуск» выбрать раздел «Программы», далее Aladdin – HASP SRM – VendorSuite.
- Выбрать приложение Business Studio. В поле имя пользователя и поле пароль ввести «HASP».
- Определим компонент, назовем его «Simplex». Для этого необходимо выполнить следующие действия.
- В окне Business Studio открыть раздел Licensing Plan (Лицензионный план) и выбрать пункт Manage Features (работа с компонентами).
- В поле Batch Code (Код серии) выбрать серию ключа. Для данного проекта использовались ключи серии CRAXZ.

- Для того, чтобы выбрать VendorKey с именем CRAZX, необходимо открыть раздел Setup (Установки), выбрать пункт Master Keys (Мастер ключи), далее Introduce Master (Ввести Мастер ключ). В появившемся окне определить имя ключа и путь для сохранения информации из мастер-ключа.
- Теперь выбираем пункт New Feature (Создать компонент). Ввести название компонента, возле пункта Specify Feature ID (номер компонента) ставим флажок и вводим число 66. Нажимаем ОК и после этого в списке появится компонент.

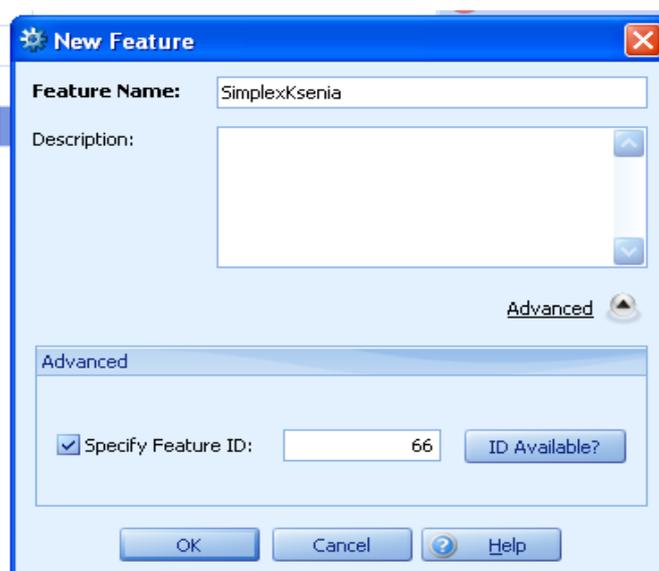


Рисунок 18 — создание компонента

- В разделе Manage Products выбрать продукт, нажать Define License Terms, в открывшемся окне необходимо определить условия лицензии:
— в поле LicenseType (Тип лицензии) выбираем Perpetual (Без ограничений). Нажать ОК. После у продукта в списке будет статус «Ready».

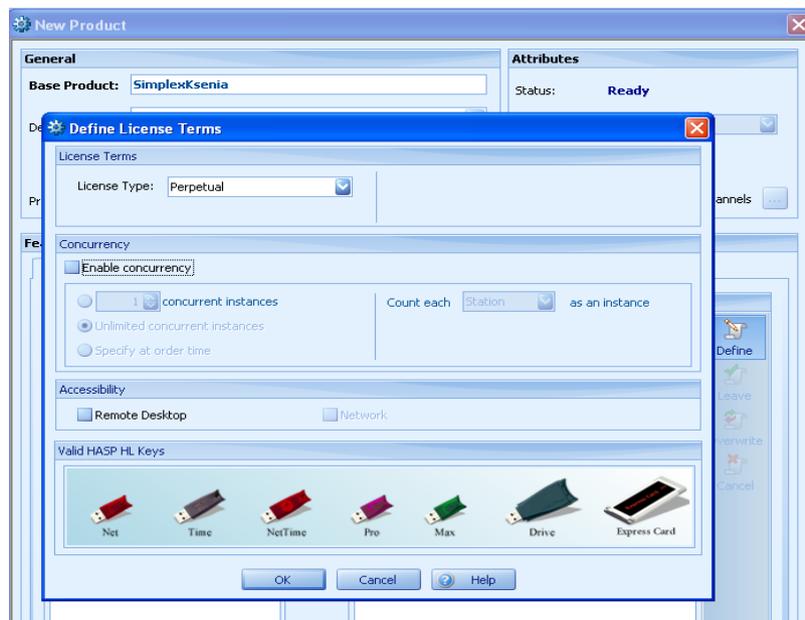


Рисунок 19 – Создание продукта с неограниченной лицензией



Рисунок 20 – Статус продукта "Готов"

9) Закрываем окно BusinessStudio.

Привязка к ключу HASP HL.

Открыть Business Studio, в разделе Production выбрать пункт Manage Orders, нажать кнопку New (Новый заказ), далее в разделе Customer (Заказчик), так же выбираем New, указываем его имя.

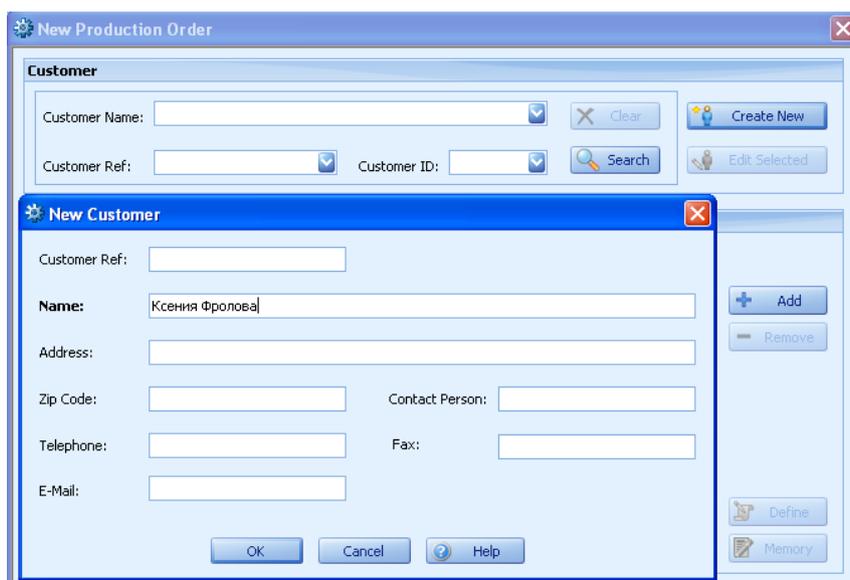


Рисунок 20 – Создание нового заказа для нового заказчика

Нажимаем Add (Добавить), выбираем необходимый продукт из списка, добавляем его. Для настройки привязки к ключу выполняем:

– Открываем Order Details (Сведения о заказе) и выбираем параметр HASP HL Keys, в поле Number of Keys необходимо ввести 1, так как будет использоваться 1 ключ.

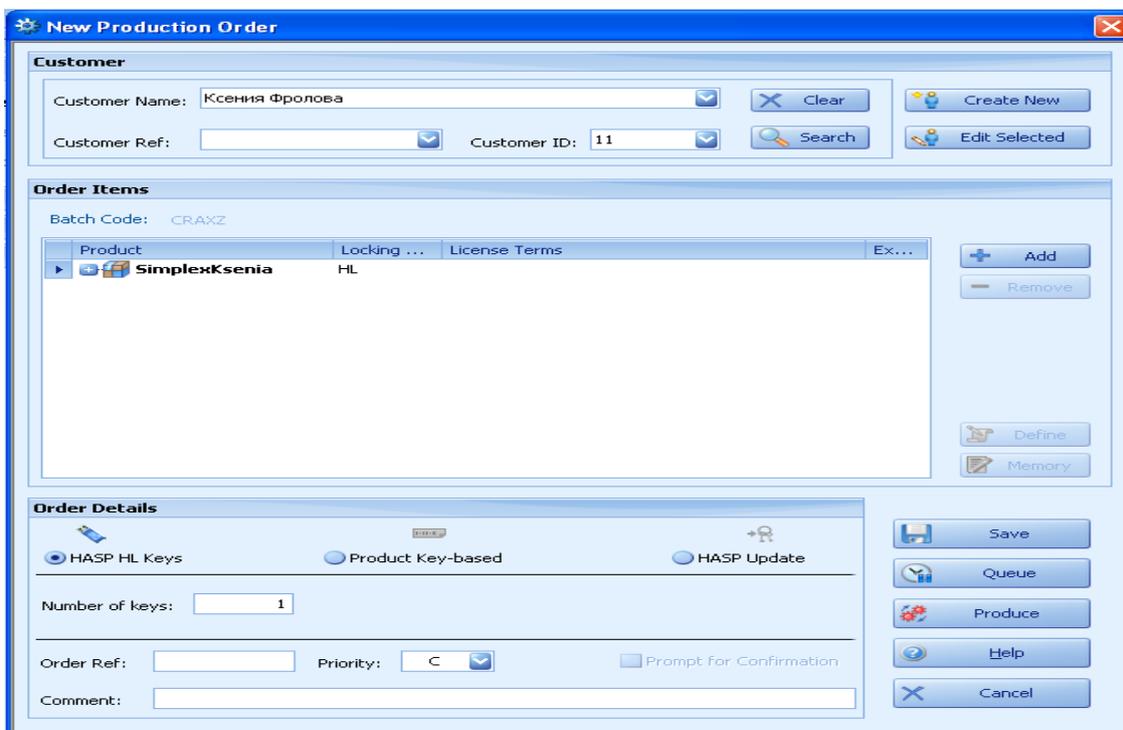


Рисунок 21 – Добавление продукта в заказ и выполнение привязки к конкретному ключу

Далее необходимо нажать кнопку Produce Now (В обработку), присоединить ключ и нажать кнопку BurnNow.

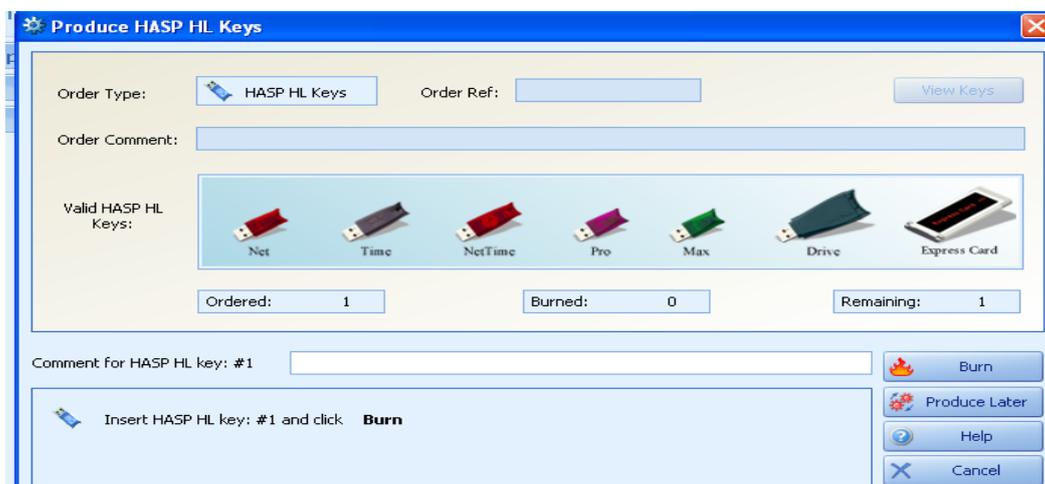


Рисунок 22 – Запуск продукта в обработку

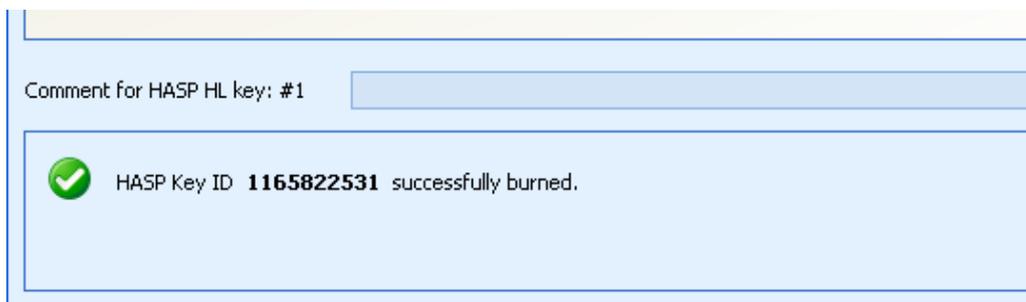


Рисунок 23 – Обработка прошла успешно

Нажать кнопку Done (Готово).

Установка навесной защиты при помощи аппаратного ключа HASP HL.

- Перед установкой защиты на приложение необходимо выполнить:
- Подключить ключ CRAZX.
- Выполнить цепочку действий: открыть «Пуск» - выбрать пункт «Программы» — Aladdin — HASP SRM — Vendor Suite — Envelope.
- Выбрать пункт Sentinel HASP Batch Code (Профиль HASP SRM), далее поставить флажок на пункте Use Vendor Code (Использовать файл с кодом разработчика) и указать путь к файлу.

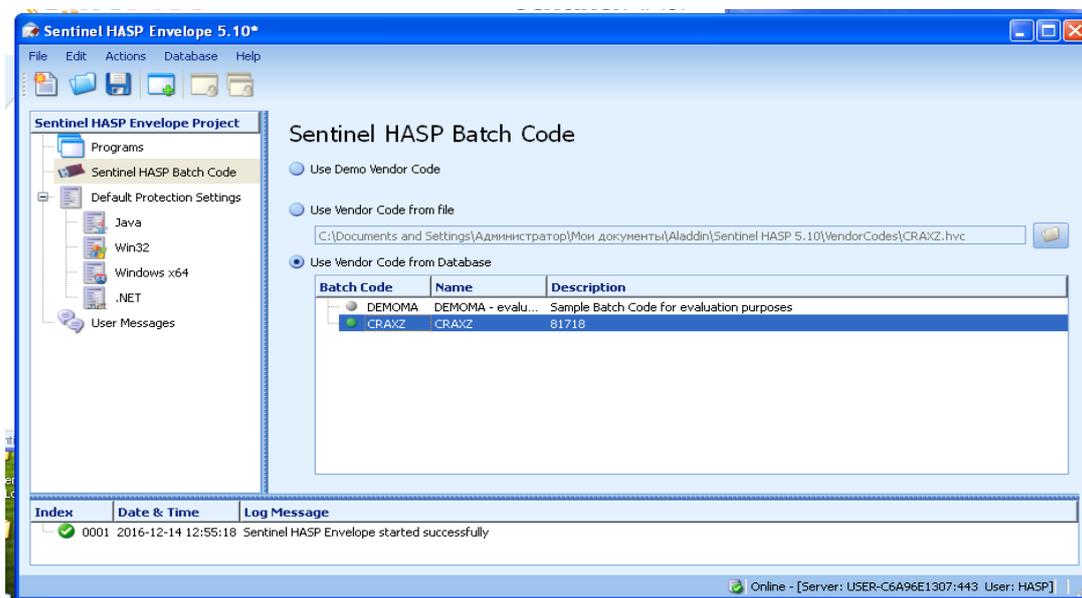


Рисунок 24 – Ссылка на файл с кодом разработчика

Непосредственная установка навесной защиты на приложение.

Выбрать пункт Programs (Программы). Нажать на кнопку Add Programs (Добавить программы), выбрать необходимый файл. После он появится в списке приложений раздела Программы.

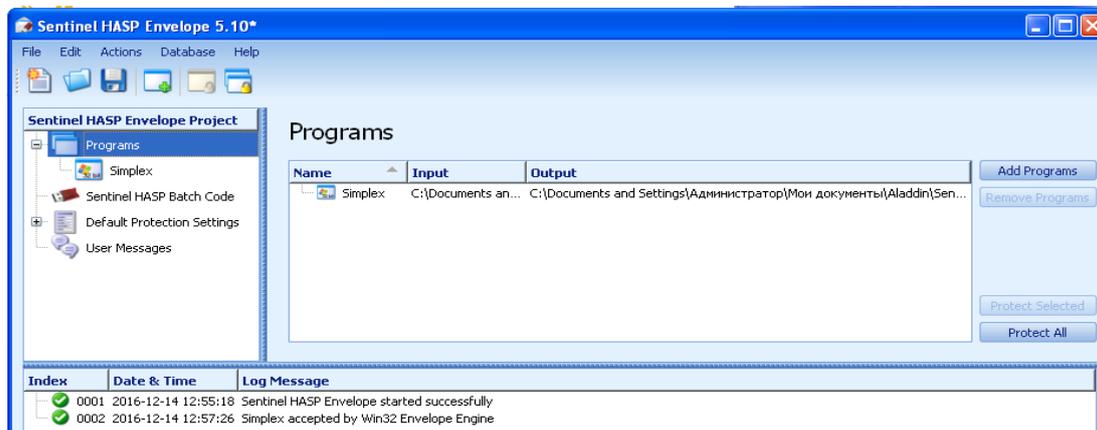


Рисунок 25 – Успешное добавление программы в список

Выбираем программу «Simplex», отобразятся ее параметры защиты. В поле Future ID (Номера компонента) указать значение 66, которое было выбрано ранее.

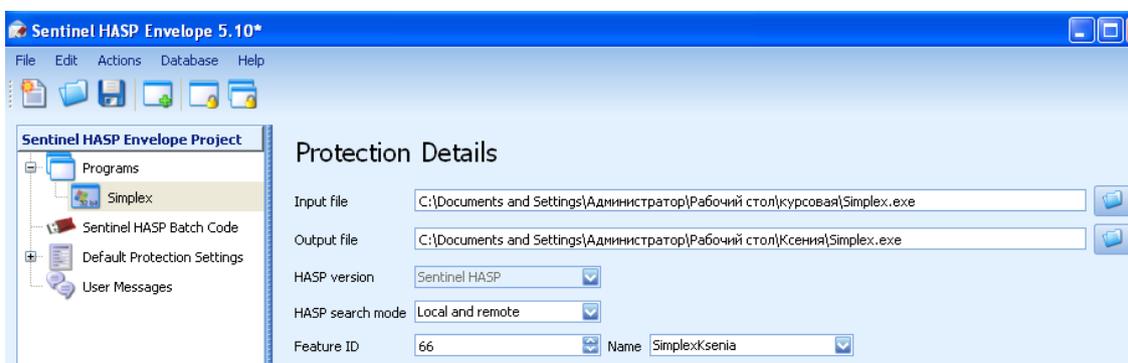


Рисунок 26 – Корректировка параметров защиты

Выбираем раздел User Messages (Сообщения для пользователя), выбрать MessageCode “HASP_HASP_NOT_FOUND” и в поле Caption ввести сообщение, которое будет выдаваться в случае отсутствия ключа. Далее выбрать раздел Default Protection Settings (Настройки шаблона защиты), выбрать раздел Win32, и настроить параметры защиты: установить значение для параметра HASP key background checks равное 20. Этот параметр обозначает, что каждые 20 сек приложение, будет проверять наличие ключа и в случае его отсутствия работа приложения прекратится — изменить положение бегунка слева направо напротив раздела Encryption level. Чем больше будет

перемещен бегунок, тем выше будет защита, но скорость загрузки будет увеличиваться.

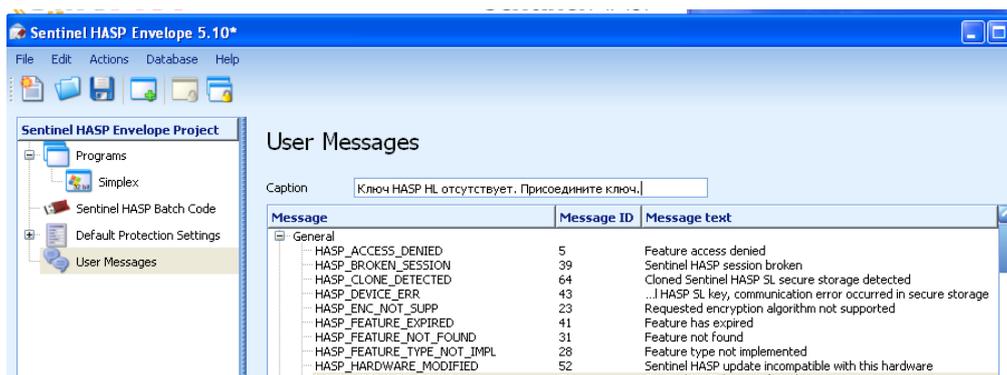


Рисунок 26 – Настройка сообщения, которое будет выдаваться при отсутствии ключа

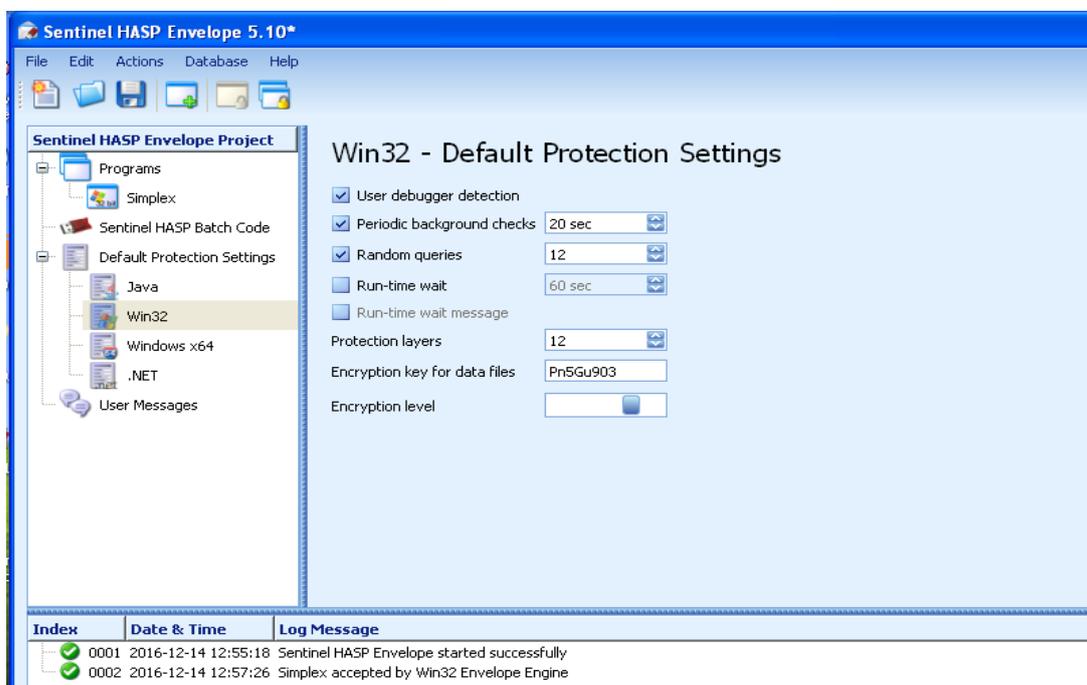


Рисунок 27 – Настройки защиты

В настройках защиты Protection Details (Настройки защиты) поставить флажок в пункте Show waitbox on startup (Показывать сообщение о загрузке), которое будет отображаться во время процесса загрузки. В разделе Programs выбрать приложение, далее нажать кнопку Protect (Установить защиту). После завершения установки защиты нажать ОК.

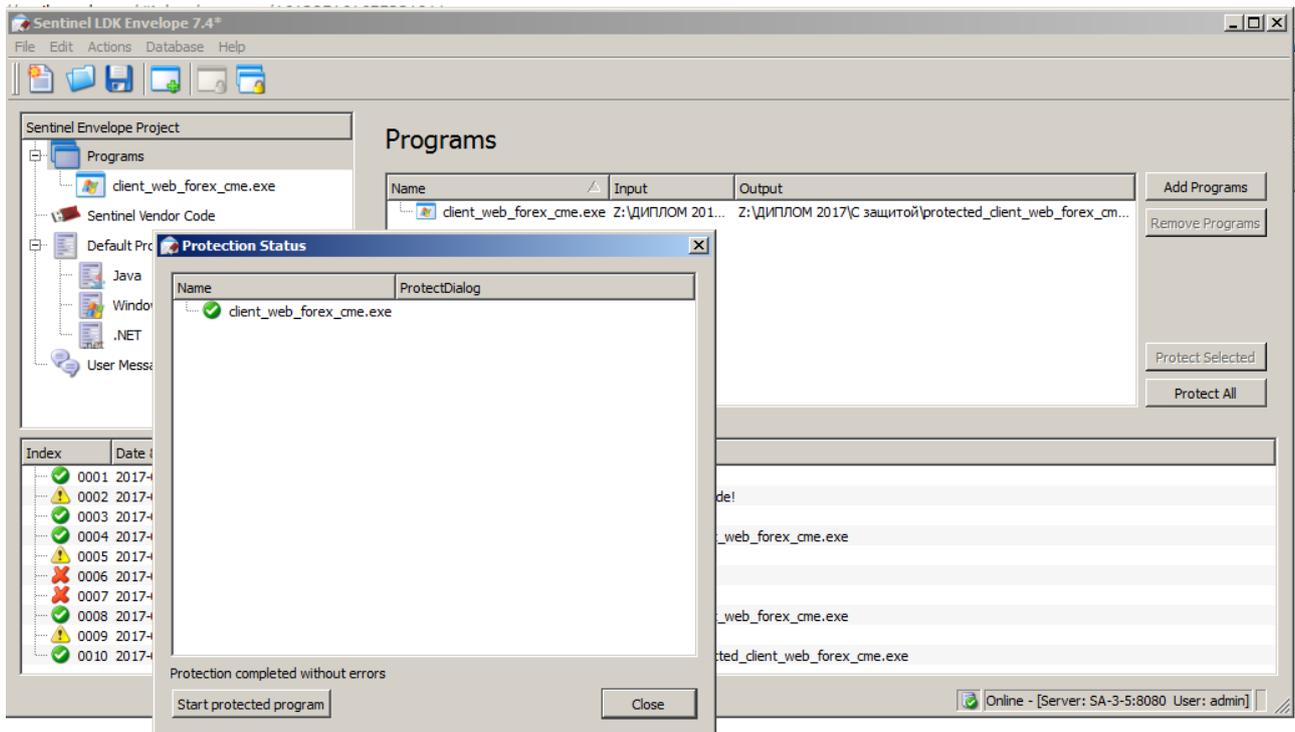


Рисунок 28 – После успешной установки защиты открывается окно программы

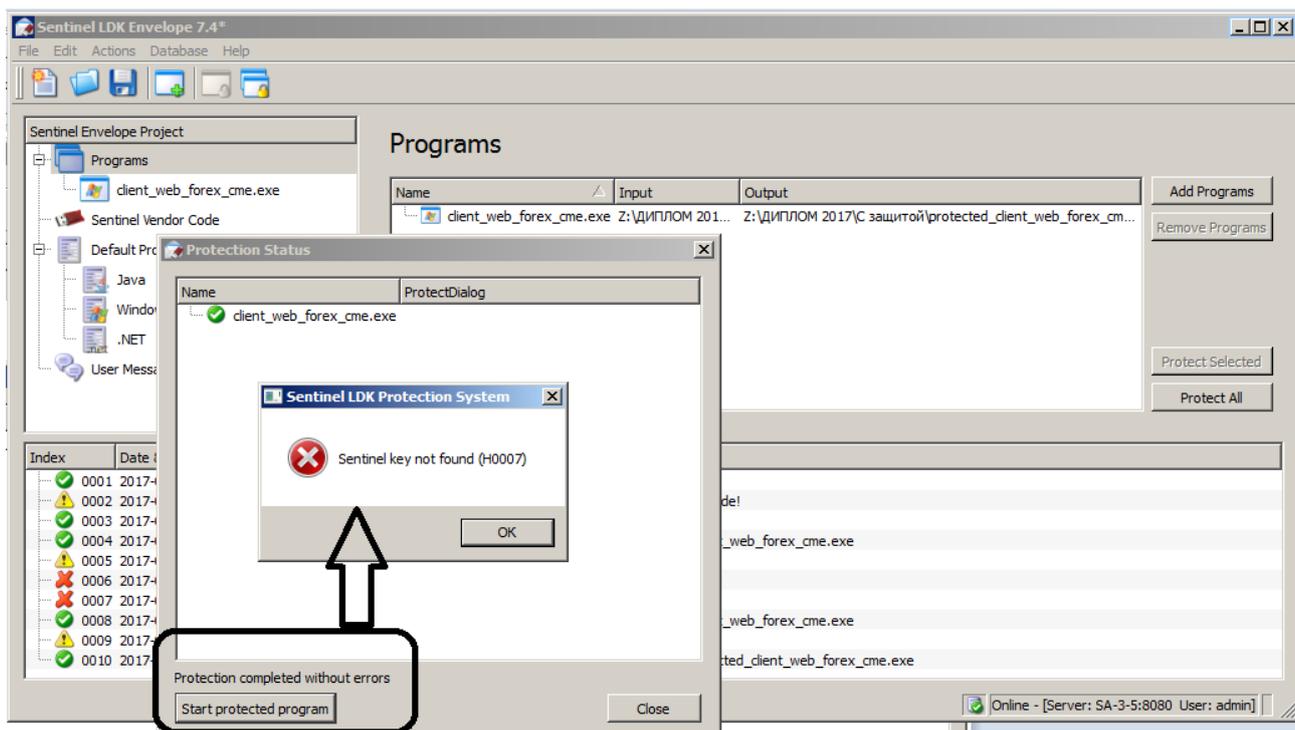


Рисунок 29 — Данное сообщение выдается при отсутствии ключа

После успешной установки защиты размер программы увеличивается. Исходный размер программы: 530 Кб. После установки защиты размер программы увеличился до 1950 Кб. Программа увеличилась на 368% (в 3,7 раза).

В ходе выполнения работы была рассмотрена и апробирована на практике технология защиты программы-клиента [5,6] с помощью аппаратных ключей серии Hasp HL [7].

4 Безопасность жизнедеятельности

В ходе выполнения работы была разработана информационно-аналитическая система для трейдеров, торгующих на международном рынке Forex. Пользователи, работающие информационно-аналитической системой, много времени проводят за персональным компьютером, а время их работы является продолжительным. Поэтому требуется правильная организация рабочего места, от которого зависит здоровье человека, использующего данную программу, необходимо рассмотреть возможные угрозы, возникающие при работе в помещениях с компьютерной техникой.

4.1 Характеристика вредных факторов при работе с ПК

На организм человека может комплексно воздействовать ряд опасных и вредных факторов, из которых наиболее значительными являются:

- опасность появления высокого напряжения на металлических частях ПК, которое может привести к электротравме;
- несоответствие норм параметров микроклимата нормативным требованиям, повышенная температура из-за постоянного нагрева деталей ПК, пониженная влажность.
- Излучения:
 - электромагнитное излучения в разных диапазонах;
 - ультрафиолетовое излучение;
 - инфракрасное излучение;
 - электростатическое поле.

- Пониженный или повышенный уровень освещенности в помещениях, не соответствующие санитарным нормам визуальные параметры дисплея.
- Повышенный уровень содержания в воздухе патогенной микрофлоры и химических веществ.
- Психофизиологическая напряженность труда:
 - монотонность работы;
 - повышенное умственное напряжение из-за большого объема перерабатываемой и усваиваемой информации;
 - повышенное нервно-эмоциональное напряжение;
 - длительные статические нагрузки.

4.2 Организация рабочего места с ПК. Требования к помещениям с ПК

Помещения для эксплуатации ПК должны иметь естественное и искусственное освещение. Эксплуатация ПК в помещениях без естественного освещения допускается только при соответствующем обосновании и наличии положительного санитарно-эпидемиологического заключения, выданного в установленном порядке.

Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации.

Окна в помещениях, где эксплуатируется вычислительная техника, преимущественно должны быть ориентированы на север и северо-восток, и обеспечивать коэффициент естественной освещенности (КЕО) не ниже 1.2 в зонах с устойчивым снежным покровом и не ниже 1.5 на остальной территории.

Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.

Не допускается размещение мест пользователей ПЭВМ во всех образовательных и культурно-развлекательных учреждениях для детей и подростков в цокольных и подвальных помещениях.

Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно отражающие материалы с коэффициентом отражения для потолка – 0.7 – 0.8; для стен – 0.5 – 0.6; для пола – 0.3 – 0.5.

Полимерные материалы, используемые для внутренней отделки интерьера помещений с ПЭВМ должны иметь наличие положительного санитарно-эпидемиологического заключения.

Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением в соответствии с техническими требованиями по эксплуатации.

Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

4.3 Требования к размещению и оборудованию рабочего места с ПК

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами должно быть не менее 2 м, а расстояние между боковыми поверхностями мониторов – не менее 1.2 м.

В помещениях с источниками вредных производственных факторов рабочие места должны размещаться в изолированных кабинах с организованным воздухообменом. При выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рабочие места рекомендуется изолировать друг от друга перегородками высотой 1.5 – 2.0 м.

Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600 – 700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его

количества и конструктивных особенностей, характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0.5 – 0.7.

Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680 – 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм.

Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800–1400 мм, глубину 800-1000 мм при нерегулируемой его высоте, равной 725 мм. Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм. Конструкция рабочего стула (кресла) должна позволять менять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для снижения утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ. Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

Конструкция рабочего стула должна обеспечивать:

- ширину и глубину поверхности сиденья не менее 400 мм;
- поверхность сиденья с закругленным передним краем;
- регулировку высоты поверхности сиденья в пределах 400 - 550 мм и углам наклона вперед до 15 градусов и назад до 5 градусов;
- высоту опорной поверхности спинки 300 +/- 20 мм, ширину – не менее 380 мм и радиус кривизны горизонтальной плоскости - 400 мм;
- угол наклона спинки в вертикальной плоскости в пределах +/- 30 градусов;

- регулировку расстояния спинки от переднего края сиденья в пределах 260 - 400 мм;
- стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50 – 70 мм;
- регулировку подлокотников по высоте над сиденьем в пределах 230 +/- 30 мм и внутреннего расстояния между подлокотниками в пределах 350 – 500 мм.

Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

Клавиатуру следует располагать на поверхности стола на расстоянии 100 - 300 мм от края, обращенного к пользователю, или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

4.4 Требования к санитарно-гигиеническим параметрам рабочего места с ПК

В зависимости от категории трудовой деятельности и уровня нагрузки за рабочую смену при работе с ПЭВМ устанавливается суммарное время регламентированных перерывов, нормативные данные приведены в таблице 1.

Таблица 1 – Суммарное время регламентированных перерывов в зависимости от продолжительности работы, вида и категории трудовой деятельности с ПЭВМ.

| Категория работы с ПЭВМ | Уровень нагрузки за рабочую смену при видах работ с ПЭВМ | | | Суммарное время регламентированных перерывов, мин. | |
|-------------------------|--|-----------|--------|--|-------------|
| | группа А, | группа Б, | группа | при 8- | при 12-часо |
| | | | | | |

| | количество знаков | количество знаков | В, ч | часовой смене | вой смене |
|-----|-------------------|-------------------|------|---------------|-----------|
| I | до 20 000 | до 15 000 | до 2 | 50 | 80 |
| II | до 40 000 | до 30 000 | до 4 | 70 | 110 |
| III | до 60 000 | до 40 000 | до 6 | 90 | 140 |

В помещениях, где работа на ПЭВМ является основной, должны обеспечиваться оптимальные параметры микроклимата, приведенные в таблице 2.

Таблица 2 – Оптимальные нормы микроклимата для помещений с ПЭВМ.

| Период года | Категория работ | Температура воздуха С °, не более | Относительная влажность воздуха, % | Скорость движения воздуха, м/с |
|-------------|-----------------|-----------------------------------|------------------------------------|--------------------------------|
| Холодный | Легкая – 1а | 22-24 | 40-60 | 0,1 |
| | Легкая – 1б | 21-23 | 40-60 | 0,1 |
| Теплый | Легкая – 1а | 23-25 | 40-60 | 0,1 |
| | Легкая – 1б | 22-24 | 40-60 | 0,2 |

К категории 1а относятся работы, производимые сидя и не требующие физического напряжения, при которых расход энергии составляет до 120 ккал/ч. К категории 1б относятся работы, производимые сидя, стоя или связанные с ходьбой и сопровождающиеся некоторым физическим напряжением, при которых расход энергии составляет от 120 до 150 ккал/ч. Уровни электромагнитных излучений, считающихся безопасными для здоровья, приведены в таблице 3.

Таблица 3 – Временные допустимые уровни ЭМП, создаваемых ПЭВМ на рабочих местах.

| Наименование параметров | | ВДУ |
|------------------------------|---------------------------------|--------|
| Напряженность электрического | в диапазоне частот 5 Гц - 2 кГц | 25 В/м |

| | | |
|--|------------------------------------|---------|
| поля | в диапазоне частот 2 кГц - 400 кГц | 2,5 В/м |
| Плотность магнитного потока | в диапазоне частот 5 Гц - 2 кГц | 250 нТл |
| | в диапазоне частот 2 кГц - 400 кГц | 25 нТл |
| Напряженность электростатического поля | | 15 кВ/м |

Конструкция ПЭВМ должна обеспечивать мощность экспозиционной дозы рентгеновского излучения в любой точке на расстоянии 0,05 м от экрана и корпуса при любых положениях регулировочных устройств не должна превышать 0,1 мбэр/час (100 мкР/час). В результате работы ПЭВМ генерируется весьма широкий спектр звуков (включая ультразвук), причем каждый компьютер отличается в этом смысле своей индивидуальностью. Корпус компьютера при этом является резонатором и привносит в общую картину шума низкочастотные составляющие. Нормативные параметры звука приведены в таблице 4.

Таблица 4 – Допустимые значения уровней звукового давления в октавных полосах частот и уровня звука, создаваемого ПЭВМ.

| Уровни звукового давления в октавных полосах со среднегеометрическими частотами | | | | | | | | | Уровни звука в дБА |
|---|-------|--------|--------|--------|---------|---------|---------|---------|--------------------|
| 31,5 Гц | 63 Гц | 125 Гц | 250 Гц | 500 Гц | 1000 Гц | 2000 Гц | 4000 Гц | 8000 Гц | |
| 86 дБ | 71 дБ | 61 дБ | 54 дБ | 49 дБ | 45 дБ | 42 дБ | 40 дБ | 38 дБ | 50 |

Искусственное освещение в помещениях с ПЭВМ должно осуществляться системой общего равномерного освещения. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 – 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк.

Знание санитарно-гигиенических параметров и их соблюдение в пределах норм, правильный режим труда и отдыха, выполнение требований эргономики, пожарной и электробезопасности - позволяет снизить или совсем исключить влияние вредных и опасных факторов на работников, и повысить эффективность труда.

Выводы

Все основные задачи, согласно плану выполнения дипломной работы, были успешно выполнены.

Были рассмотрены торговые стратегии для рынка Forex, основанные на использовании данных бюллетеней биржи CME Group. Разработка собственных торговых стратегий выходит за рамки данной работы, так же, как и выбор наилучшей из списка возможных стратегий для торгуемого финансового инструмента. Была выбрана пара евродоллар (EUR/USD), как наиболее часто используемая трейдерами и торговая стратегия, основанная на том, что график торгового инструмента имеет тенденцию находится в основном в комфортной зоне цены для крупных игроков, т.е. цена находится ниже верхней границы рынка и выше нижней. Выход графика цены выше верхней границы рынка создает благоприятную ситуацию для открытия ордера на продажу. Если график опустился ниже нижней границы, то можно открывать ордер на покупку. Следует заметить, что границы рынка не являются постоянными и могут меняться, поэтому анализ границ рынка следует проводить с выходом каждого нового бюллетеня CME Group.

Была разработана информационно-аналитическая система, данные для обработки поступают в систему с ftp-сервера CME Group, зачисляемые php модулем разработанной информационной системы. Достаточно сложной задачей стало решение проблемы конвертации данных из оригинального pdf формата бюллетеней в текстовый формат (txt), используемый для дальнейшей работы. Было проанализировано программное обеспечение, которое можно использовать для целей конвертации. Число коммерческих библиотек составляет несколько десятков, но свободно распространяемые, которые можно было бы использовать бесплатно, практически не встречаются. После долгих поисков конвертер файлов pdf в txt был найден. Тестирование показало, что конвертированный текст в файле txt вполне пригоден для извлечения данных их дальнейшей обработки. Был разработан сайт информационно-аналитической

системы – php модули расчета границ рынка, получения данных с ftp-сервера СМЕ Group, модули аутентификации и авторизации пользователей, модуль администрирования. Выполненное тестирование показало, что обработка, начиная с загрузки бюллетеней с ftp-сервера СМЕ Group, и заканчивая публикацией данных по границам рынка (оперативно полученных в результате работы php модуля и сохраненных в базе данных MySQL) на сайте информационной системы, возможна в полностью автоматическом режиме – максимальный период тестирования 8 суток.

Учитывая, что разработанный вариант информационно-аналитической системы может быть доработан до коммерческого варианта программного продукта, был рассмотрен вариант усиления защиты доступа к закрытой области интерфейса, доступной только для зарегистрированных пользователей, с использованием двух факторной программно-аппаратной защиты, использующей РутOKEN WEB.

Для повышения уровня комфортной работы трейдеров с информационно-аналитической системой был разработан, с использованием среды визуального проектирования Delphi, специализированный программный клиент.

Рассмотрены варианты защиты разработанной программы-клиента с использованием программно-аппаратных (ключи серии HASP HL) и программных (виртуальные ключи HASP SL) решений. Использование ключей HASP SL целесообразно при стоимости ежемесячной подписки порядка 600 руб./мес., оформляемой не менее чем на три месяца (накладные расходы на использование программного ключа 60-100 руб.), если стоимость подписки более 1000 руб., то экономически целесообразно использовать программные ключи типа Hasp SL или дешевые (400-700 руб. за 1 шт.) ключи Hasp HL Basic. Если подписка дороже 1000 руб. месяц, то можно для защиты программы-клиента использовать ключи типа HASP HL Pro с защищенной памятью, позволяющей записывать в ключ индивидуальные идентификационные данные пользователя.

В плане дальнейшего совершенствования информационно-аналитической системы можно будет разработать модули системы информирования трейдеров о торговых сигналах поддерживающие не только доступ по протоколу http или https (что уже реализовано в разработанных модулях), но и информирование по электронной почте (smtp-протокол), с использованием рассылки SMS и PUSH уведомлений.

В ходе выполнения дипломной работы было подготовлено две публикации, которые опубликованы в трудах международных научных конференций (статьи проиндексированы в РИНЦ).

Литература

1. Ананченко И.В., Камашев А.О., Базарнов И.Б. Алгоритм открытия ордеров по валютной паре EUR/USD на рынке Форекс на основе данных опционных уровней первого порядка. В сборнике: Закономерности и тенденции инновационного развития общества. Сборник статей Международной научно-практической конференции. 2016. С. 62-64.
2. Камашев А.О., Базарнов И.Б., Ананченко И.В. Разработка защищенной информационно-аналитической системы для торговли на Forex по паре EUR/USD на основе опционных уровней первого порядка. В сборнике: Научная дискуссия современной молодёжи: экономика и право сборник статей международной научно-практической конференции. 2016. С. 457-459.
3. И.В. Ананченко Защити свою программу ключом HASP. Практическое руководство для начинающих по работе с HASP HL. LAP Lambert Academic Publishing. 2012, 80 с. ISBN: 978-3-659-25627-1
4. Защити свою программу ключом HASP. Практическое руководство для начинающих по работе с HASP HL. LAP Lambert Academic Publishing – ISBN: 978-3-659-25627-1. 2012 [Электронный ресурс] URL: <http://www.mctrewards.ru/studentam/knigi2012-2013>
5. Краткий курс по защите и лицензированию программного обеспечения с использованием HASP SRM. [Электронный ресурс] URL: <http://www.aladdin-rd.ru/support/downloads/get?ID=21054>
6. Guardant.ru официальный сайт. [Электронный ресурс] URL: <https://www.guardant.ru/products/all/>
7. HASP SRM : общие сведения о защите и лицензировании (1-10), (13-17) [Электронный ресурс] URL: <http://www.aladdin-rd.ru/support/downloads/get?ID=21057>

Приложения

Приложение А. DVD диск с исходными текстами программ и документацией