УДК 336.74

РАЗРАБОТКА ЗАЩИЩЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПРОВЕДЕНИЯ ОПЕРАЦИЙ НА КРИПТОБИРЖЕ BINANCE

А. А. Текучев, И. С. Краснокутский, М. М. Казарян, О. А. Сафарьян
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

В статье изучены и проанализированы существующие системы автоматического совершения сделок на криптобиржах, их достоинства и недостатки. Представлена концепция собственного разрабатываемого программного продукта, а также предложены и реализованы различные методы защиты, позволяющие обеспечить безопасность разрабатываемого программного средства. Результатом данной статьи является реализация работающего прототипа системы автоматического совершения сделок на криптобирже с использованием изученных методов защиты данных.

***Ключевые слова*:** BINANCE, криптобиржа, криптовалюта, Telegram, база данных, бот, криптоалгоритм, RSA.

DEVELOPMENT OF A SECURE AUTOMATED SYSTEM FOR CONDUCTING OPERATIONS ON THE BINANCE CRYPTOCHANGE EXCHANGE

A. A. Tekuchev, I. S. Krasnokutsky, M. M. Kazaryan, O. A. Safaryan
Don State Technical University (Rostov-on-Don, Russian Federation)

The article studies and analyzes the existing systems for automatic transactions on crypto exchanges, their advantages and disadvantages. The concept of our own developed software product is presented, as well as various protection methods are proposed and implemented to ensure the safety of the developed software. The result of this article is a working prototype of a system for automatically making transactions on a crypto exchange using the studied data protection methods.

***Keywords*:** BINANCE, crypto exchange, cryptocurrency, Telegram, database, bot, crypto algorithm, RSA.

Введение. В настоящее время разработка технологии блокчейн открывает все больше возможностей в разных IT отраслях, в том числе и в экономическом сегменте. Одним из примеров применения данной технологии являются криптовалюты [1]. Термин криптовалюта вошел в обиход благодаря тому, что для проверки транзакций используется шифрование, которое обеспечивает надежность и безопасность (для хранения и передачи данных о криптовалюте между кошельками и в общедоступные реестры используется расширенное кодирование).

С момента появления первых криптовалют этот рынок, имея свои достоинства и недостатки, стремительно растет, образуя новую экономическую систему. Одним из главных преимуществ является анонимность всех транзакций, которые невозможно отследить, и безопасность операций. Однако существует и весомый минус — нестабильность стоимости криптовалют [2].

С появлением криптовалют большое распространение получили боты, совершающие сделки на различных криптобиржах. Бот — виртуальный робот-программа, который функционирует на основе специального алгоритма, выполняющий автоматически и/или по заданному расписанию какие-либо действия через интерфейсы, предназначенные для людей. Программа собирает необходимую информацию, анализирует ее и создает запросы на бирже в автономном режиме [3].

Основная часть. Важным аспектом является защита данных систем от различных злоумышленников. Ежедневно происходит взлом систем хранения данных подобных программ по причине неправильного обеспечениях их сохранности [4–6].

Правильно организованный алгоритм хранения паролей в базе данных позволит снизить риск полного взлома системы и предотвратить утечку паролей пользователей злоумышленнику [7].

В данной статье рассматриваются программные средства, существующие на данный момент, обеспечивающие безопасность такой системы. Целью данной статьи является реализация программного средства защищенной автоматизированной системы проведения операций на криптобирже binance.

Существующие аналоги. Рассмотрим уже существующие программные средства для совершения операций на криптобиржах. Стоит отметить, что количество таких программ растет каждый месяц, каждая из которых имеет свои особенности. Наиболее популярные системы приведены в таблице 1.

Таблица 1

Существующие аналоги

Название системы	**Характеристики**		
	Количество поддерживаемых платформ	**Настройка стратегий торговли**	**Лицензия**
RevenueBot	6	Присутствует	Платная (20% от прибыли)
3Commas	23	Присутствует	Платная (бесплатный пробный период)
Stratum Bot	2	Отсутствует	Платная (ежемесячная оплата)

В некоторых системах предусмотрены различные стратегии торговли с возможностью настройки тех или иных параметров, а также поддержка разных бирж и запуск сразу нескольких потоков.

Так, например, интересной особенностью 3Commas-системы является то, что пользователи могут создавать собственные стратегии торговли и продавать их другим пользователям данной площадки.

Все системы имеют свою систему безопасности. Так, в программе Stratum Bot используется привязка к устройству, на котором может она быть запущена. Помимо этого, доступ к ее использованию обеспечивается специальным криптографическим ключом, получаемым при покупке данной системы.

Программная разработка. Для обеспечения безопасного хранения и передачи данных в разрабатываемом программном средстве были применены следующие методы защиты:

– создана база данных, необходимая для хранения пользовательской информации, такой как конфиденциальные api-ключи, а также для ведения логирования;

– использованы библиотеки, которые предоставляют доступ к бирже и чату по уникальным криптографическим токенам для обеспечения дополнительной безопасности.

Для реализации первого пункта была выбрана PostgreSQL — СУБД, сильными сторонами которой являются:

– быстрые и надежные механизмы транзакции и репликации;

– наличие встроенных языков программирования;

– гибкая система распределения прав;

– поддержка криптографических методов защиты информации, реализованных во встроенных модулях.

Реализованная база данных содержит в себе три таблицы, которые необходимы для работы программы:

– deals — хранит сведения о совершенных сделках на крипто-бирже для обеспечения возможности проведения дополнительных статистических и финансовых расчетов;

– logs — содержит курс криптовалюты, агрегируемый в течение времени работы бота, а также вспомогательные расчеты, за счет которых бот принимает решение о покупке или продаже;

– users — содержит набор пользователей, а также права доступа и api-ключи данных пользователей.

Структура описанной базы данных с наименованием полей и их типами представлена на рис. 1.

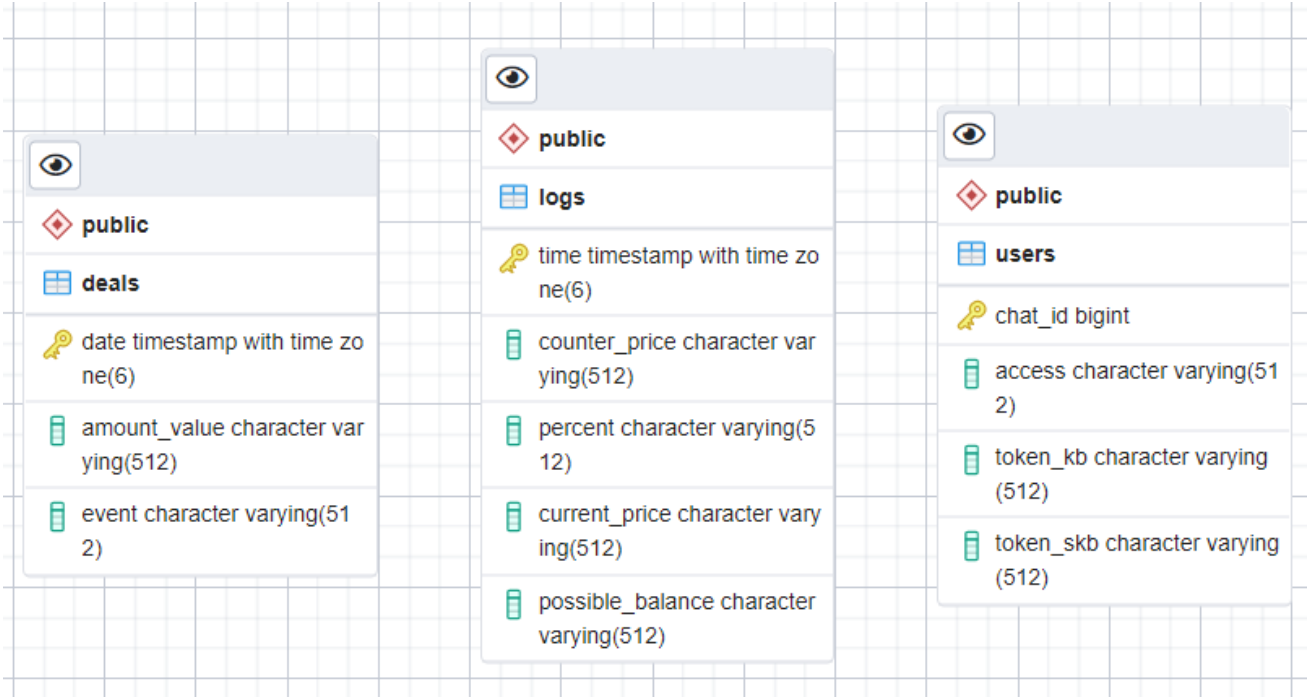

Рис. 1. Структура базы данных

Для управления ботом биржи через мессенджер был разработан специальный чат-бот, нацеленный на упрощенный и удобный доступ к функционалу этого бота. Чтобы обеспечить секретность передаваемых данных, в качестве мессенджера был выбран Telegram, так как в нём для работы с ботом используется специальный уникальный токен, который отправляется на сервер Telegram по https протоколу для обеспечения дополнительной безопасности.

Взаимодействие с программой начинается с запуска бота в мессенджере telegram. Если пользователь запускает бота впервые, чат-id заносится в ранее описанную базу данных в таблицу users с нулевым правом доступа. При этом пользователь видит сообщение, указанное на рис. 2.

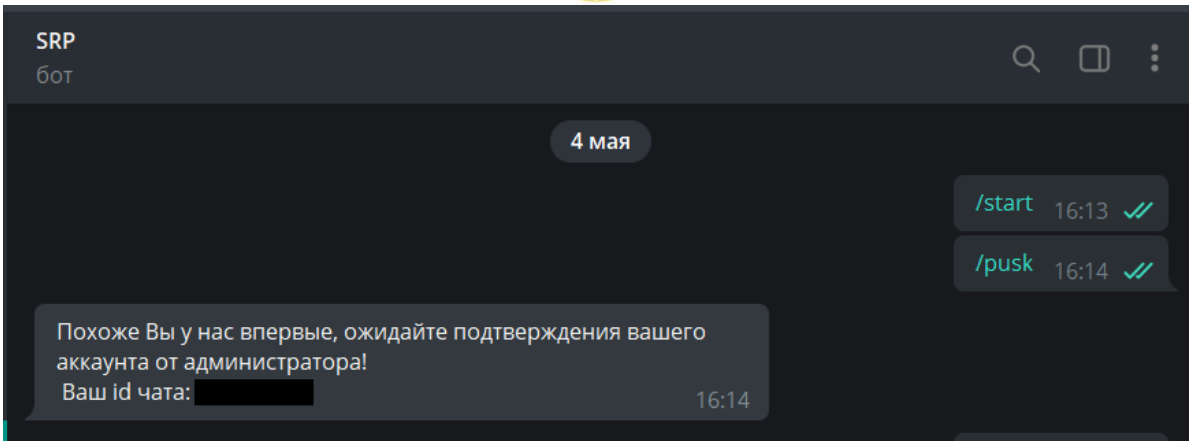

Рис. 2. Запуск бота в первый раз

После чего пользователь задает api-ключи, полученные на крипто-бирже binance, используя команду /settings. Переданные пользователем api-ключи заносятся в таблицу users ранее рассмотренной базы данных. При этом ключи, как и другая конфиденциальная информация, шифруются ассиметричным алгоритмом RSA. Далее администратор должен выдать право на использование бота данному пользователю. До этого момента пользователь будет получать сообщения, указанные на рис. 3.

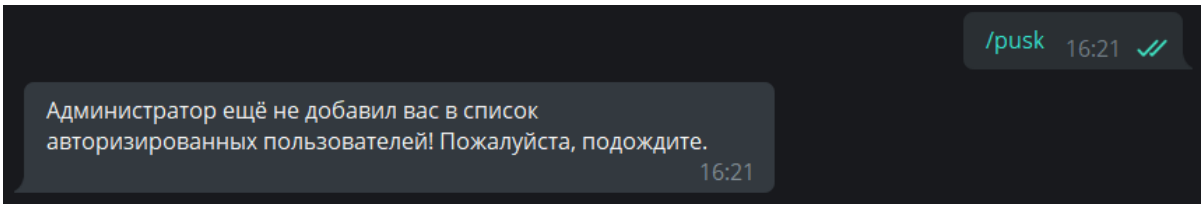

Рис. 3. Ответ бота при нулевом праве доступа

Добавление пользователю права на использование бота — задача администратора системы. Один из вариантов выполнения sql-кода представлен на рис. 4.

```
update users SET access=1 where chat_id=ИД_ЧАТА;
```

Рис. 4. Выдача прав пользователю

Когда права на использование бота получены, пользователь может запустить бота, после чего бот начнет совершать сделки на бирже. При этом в диалоговом окне будет выводится информация о совершенных сделках покупки и продажи, пример которой представлен на рис. 5.

Рис. 5. Информация о состоянии активов

Для дополнительной безопасности история сделок, хранящаяся в таблице deals, а также значения из таблицы users шифруются криптографическим алгоритмом RSA. Данные шифруются открытым ключом размером 1024 бит. Пример зашифрованных данных приведен на рис. 6.

Data Output | Explain | Messages | Notifications

	time [PK] timestamp with time zone	counter_price character varying (512)
680	2022-05-10 22:03:22.363747+03	TE2AlfrDEx+VCSbaxEnBVrWBQ6gdusPbtfIl0ExLyj/4HLntj+DG2SfEQVbowUg5nAMJRlos5zN0fTNrlEPQZiq
681	2022-05-10 22:03:29.078197+03	IIwxGm9l0NClryMJbfBYvhR33twJIcLRync1BfLJbrpbOKRuD4M0Caaki2TiQLRbs0SjR3QkRs2PP2tUeq2wb.
682	2022-05-10 22:03:35.111528+03	IScIFqMrxaw6RkeowiH1vb58a1JvL/E9CD4BoByx1wzPJcgUp3QMYJRAT8jZnDIU1h1TcvKCHdMB9Kso5YI
683	2022-05-10 22:03:41.173097+03	waFBt3a/QHPPlJuvb//V2fDW/FrY3fcOdE7ARJo8NRF287LwSdTyLtH26hwqiXxlBnAsH/YhImO3w94MHq2
684	2022-05-10 22:03:47.912348+03	MQVTLLaTMjtB45uUhT2R4wsF8yLsZ6CRws7ctH9k5MTjj/WhOhYo/EOdz4nOd3dYhXxcHLIpTndrEbQjflqz

Рис. 6. Зашифрованные значения базы данных алгоритмом RSA

Также предполагается, что закрытый ключ, использующийся для расшифровки, находится на внешнем носителе для обеспечения дополнительной безопасности. Следовательно, если база данных попадет к злоумышленнику, пароли и другую конфиденциальную информацию он получить не сможет.

Заключение. Проанализированы уже готовые программные решения, а также реализовано собственное программное средство, позволяющее совершать торговые сделки на криптобиржах. Безопасность программного средства обеспечена различными методами и средствами, такими как ассиметричное шифрование, хранение ключей на внешних носителях, разграничение прав пользователей, а также использование защищенного мессенджера, использующего уникальные токены для передачи данных.

Библиографический список

1. Катасонов, В. Ю. Цифровые финансы. Криптовалюты и электронная экономика. Свобода или концлагерь? / В. Ю. Катасонов — Москва : Книжный мир, 2017. — 637 с.

2. Козак, Ю. Биткоин на автопилоте. Или как заработать на криптовалюте / Ю. Козак. — Москва : Издательские решения, 2015. — 623 с.

3. Что такое боты — определение и описание / Касперский : [сайт]. — URL: https://www.kaspersky.ru/resource-center/definitions/what-are-bots (дата обращения : 20.03.2022).

4. Панасенко, С. Алгоритмы шифрования. Специальный справочник / С. Панасенко. — Санкт-Петерсбург : БХВ-Петербург, 2013. — 830 с.

5. Баричев, С. Г. Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. — Москва : Гостехиздат, 2011. — 176 с.

6. Горев, А. И. Обеспечение Информационной Безопасности / А. И. Горев, А. Симаков. — Москва : РГГУ, 2011. — 153 с.

7. Глушаков, С. В. Базы данных / С. В. Глушаков, Д. В. Ломотько. — Москва: Харьков : Фолио, 2019. — 504 с.

Об авторах:

Текучев Александр Андреевич, студент кафедры «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), user3x52@gmail.com

Краснокутский Илья Сергеевич, студент кафедры «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), bag2525@mail.ru

Казарян Максим Маратович, студент кафедры «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), maksimhs@gmail.com

Сафарян Ольга Александровна, доцент кафедры «Компьютерная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), кандидат технических наук, доцент, ORCID: https://orcid.org/0000-0002-7508-913X, safari_2006@mail.ru

About the Authors:

Tekuchev, Aleksandr A., Student of the Department of Informatics and Computer Engineering, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), user3x52@gmail.com

Krasnokutsky Ilya S., Student of the Department of Informatics and Computer Engineering, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), bag2525@mail.ru

Kazaryan Maxim M., Student of the Department of Computer Science and Computer Engineering, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), maksimhs@gmail.com

Safaryan, Olga A., Associate professor of the Cybersecurity of IT Systems Department, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), Cand.Sci. (Eng.), Associate professor, ORCID: https://orcid.org/0000-0002-7508-913X, safari_2006@mail.ru