ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ / INFORMATICS AND INFORMATION PROCESSES

РАЗРАБОТКА МОДИФИЦИРОВАННОГО АЛГОРИТМА АУТЕНТИФИКАЦИИ ДЛЯ СИСТЕМЫ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Научная статья

Тепин К.С.[1,] *, Князев В.Н.[2]
[1] ORCID : 0009-0001-0210-2030;
[2] ORCID : 0000-0003-2142-0277;
[1, 2] Пензенский Государственный Университет, Пенза, Российская Федерация

* Корреспондирующий автор (kostya.tepin.99[at]mail.ru)

Аннотация

Целью данного исследования является разработка модифицированного алгоритма аутентификации в системе электронной коммерции с целью повышения надежности процесса аутентификации пользователей. Научная новизна проведенного исследования заключается в том, что предложен модифицированный алгоритм аутентификации, который отличается от известных алгоритмов наличием пяти ключей, а именно: двух пар открытых и закрытых ключей шифрования и одного публичного ключа аутентификации, а также комбинированным использованием JWT аутентификации и модифицированного алгоритма ассиметричного шифрования RSA, позволяющего повысить криптографическую стойкость шифра. Все вышеперечисленное позволяет повысить надежность процесса аутентификации в системе электронной коммерции. Кроме того, на этапе проектирования системы электронной коммерции была разработана онтологическая модель предметной области. Также была разработана имитационная модель для оптимизации режима работы службы доставки. Созданная имитационная модель имеет комплексный характер и учитывает взаимодействие программного обеспечения разрабатываемой системы электронной коммерции и человеческий фактор сотрудников службы доставки.

Ключевые слова: электронная коммерция, информационная безопасность, криптография, криптографические алгоритмы, JWT, алгоритмы шифрования, RSA, онтологическое моделирование, имитационное моделирование.

DEVELOPMENT OF A MODIFIED AUTHENTICATION ALGORITHM FOR E-COMMERCE SYSTEM

Research article

Tepin K.S.[1,] *, Knyazev V.N.[2]
[1] ORCID : 0009-0001-0210-2030;
[2] ORCID : 0000-0003-2142-0277;
[1, 2] Penza State University, Penza, Russian Federation

* Corresponding author (kostya.tepin.99[at]mail.ru)

Abstract

The aim of this study is to develop a modified authentication algorithm in the e-commerce system in order to improve the reliability of the user authentication process. The scientific novelty of the conducted research lies in the fact that the modified authentication algorithm is proposed, which differs from the known algorithms by the presence of five keys, namely: two pairs of public and private encryption keys and one public authentication key, as well as the combined use of JWT authentication and modified RSA asymmetric encryption algorithm, which allows to increase the cryptographic strength of the cipher. All of the above can improve the reliability of the authentication process in an e-commerce system. In addition, an ontological model of the subject area was developed during the design phase of the e-commerce system. A simulation model was also developed to optimize the mode of operation of the delivery service. The created simulation model has a complex character and takes into account the interaction between the software of the developed e-commerce system and the human factor of the delivery service employees.

Keywords: e-commerce, information security, cryptography, cryptographic algorithms, JWT, encryption algorithms, RSA, ontology modelling, simulation modelling.

Введение

Специфика предметной области электронной коммерции предполагает обработку в информационных системах значительного объёма конфиденциальной информации пользователей. Утечка, модификация или несанкционированный доступ к информации такого типа, как правило, приводит к материальным или репутационным убыткам. Поэтому для программных средств электронной коммерции важнейшим требованием является обеспечение достаточного уровня надежности и информационной безопасности.

Использование криптографии позволяет защититься от подобных рисков и сопутствующего ущерба.

В данной статье рассматриваются вопросы создания модифицированного алгоритма аутентификации, повышающего уровень надежности и безопасности для разрабатываемой системы электронной коммерции [1], [2], [3], [4].

Далее рассмотрим проведение онтологического и имитационного моделирования в контексте понимания того, где и как будет применен предложенный модифицированный алгоритм аутентификации и что из себя представляет разработанная система электронной коммерции, поскольку онтологическая модель предшествует эффективному

проектированию системы электронной коммерции, а имитационное моделирование позволяет оптимизировать ее структуру и режим функционирования.

Основные результаты

Кратко рассмотрим вопросы разработки системы электронной коммерции. Процесс проектирования системы электронной коммерции начинается с этапа анализа предметной области. Одним из эффективных методов, применяемых на данном этапе, является онтологический анализ [7].

В среде Protege был разработан набор классов, свойств этих классов, а также набор связей и взаимодействий между ними. Онтологический граф предметной области показан на рисунке 1.

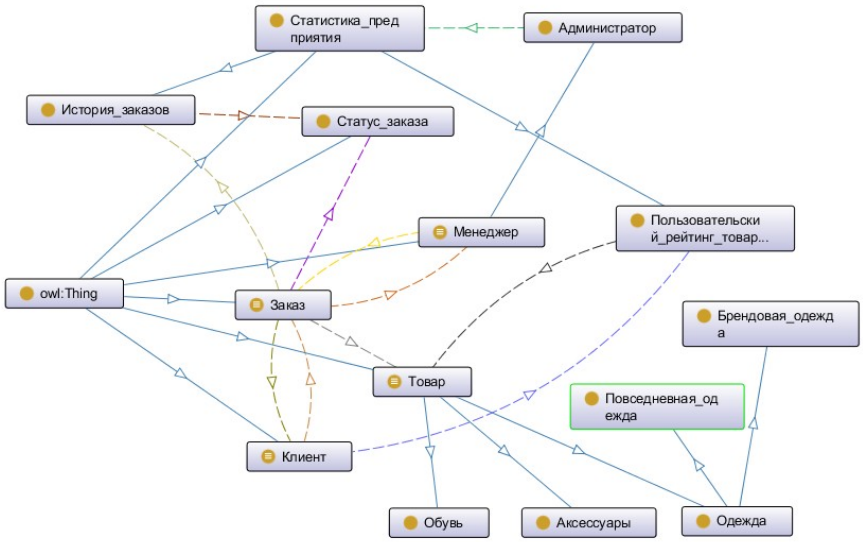

Рисунок 1 - Онтологический граф модели предметной области

Онтологический подход к проектированию систем управления знаниями позволяет создавать системы, в которых знания, накопленные внутри организации, становятся доступными для большинства пользователей. Основные преимущества этого подхода: онтология представляет пользователю целостный, системный взгляд на определенную предметную область; знания о предметной области представлены единообразно, что упрощает их восприятие; построение онтологии позволяет восстановить недостающие логические связи предметной области.

Например, в электронной коммерции онтологическое представление знаний используют для поддержки автоматизированного обмена данными между покупателями и продавцами, для вертикальной интеграции рынков, а также для повторного использования описаний различными электронными торговыми точками.

Созданная онтологическая модель позволяет проводить эффективное проектирование системы электронной коммерции. Модель основана на детальной структуризации предметной области, что облегчает этап анализа предметной области и проектирования системы.

Еще одной возможностью повышения эффективности этапов анализа и проектирования является применение имитационного моделирования. В предметной области систем электронной коммерции важной частью анализа является оптимизация процесса доставки товара службой доставки предприятия электронной коммерции. Стоит отметить, что данное моделирование имеет своей целью оптимизацию количества работников службы доставки, поэтому моделирование целесообразно проводить только для варианта доставки товара службой доставки. Другие способы доставки в данной модели не учитываются. Q-схема имитационной модели службы доставки представлена на рисунке 2.

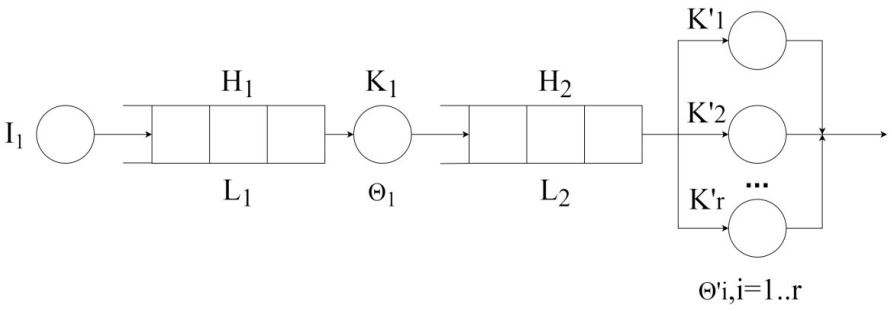

Рисунок 2 - Q-схема модели службы доставки

Поток заявок в данную модель обеспечивается источником I_1. Фрагмент системы, обеспечивающий регистрацию и управление доставкой товаров, обозначен обработчиком K_1. Очередь H_2 обозначает пропускную способность серверной части системы электронной коммерции.

Очередь H_2 аккумулирует товары, предназначенные для доставки клиенту. Средняя длина данной очереди на прямую зависит от количества работников службы доставки, обозначенных обработчиками K_1' - K_r', где r – оптимизируемое число работников службы доставки. Стоит отметить, что очередь H_1 представляет собой очередь запросов на серверную часть системы и ее переполнение возможно только при большой нагрузке на сервер в виде нештатной ситуации либо при DDoS-атаке. Однако очередь H_2 содержит заявки ожидающие обработки службой доставки и ее заполнение напрямую зависит от количества работников и оптимальности режима их работы.

Исследование имитационной модели проводилось средствами GPSS Studio. На рисунке 3 представлен процесс исследования.

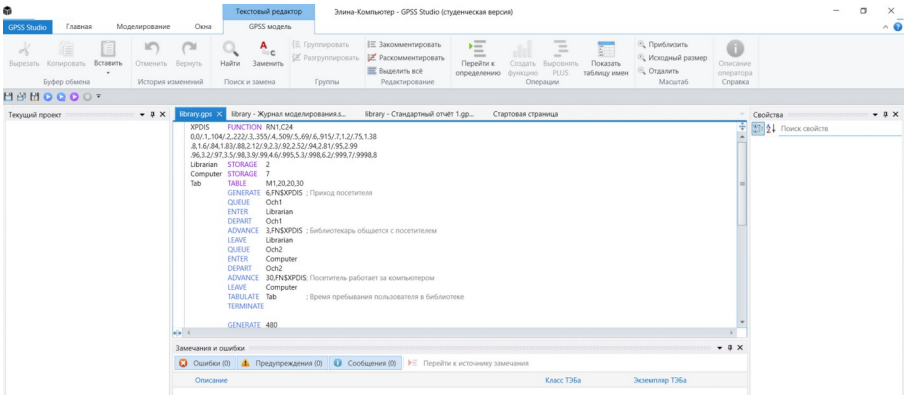

Рисунок 3 - Моделирование в среде GPSS Studio

Полученная гистограмма частот времени пребывания заявки в системе представлена на рисунке 4.

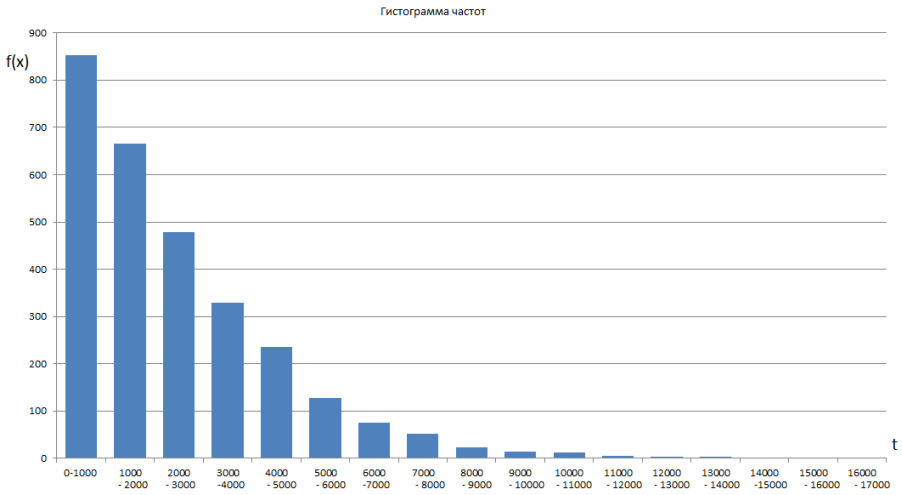

Рисунок 4 - Гистограмма частот времени пребывания заявки в системе

Результатом исследования данной модели стало определение оптимального количества работников службы доставки. Полученное оптимальное значение $r = 3$.

Теперь рассмотрим вопросы создания модифицированного алгоритма аутентификации, повышающего уровень надежности и безопасности для разрабатываемой системы электронной коммерции. Для программных средств электронной коммерции в виде трехзвенной архитектуры с клиентом, сервером и базой данных возможны следующие пути повышения надежности с использованием криптографии [8], [9], [10]:

– модифицирование алгоритма аутентификации;

– применение модифицированного алгоритма шифрования при передаче данных между различными компонентами архитектуры программной части системы;

– повышение надежности хранения данных в базе данных посредством добавления улучшенного алгоритма хеширования.

Наиболее важным из перечисленных улучшений является фактор повышения надежности алгоритма аутентификации, так как уязвимость данного фрагмента может поставить всю систему под опасность неправомерного

доступа. Роль аутентификации заключается в том, что пользователь для доступа к системе должен предъявить фактор аутентификации, т.е. определенный вид уникальной информации.

Так как программные средства разрабатываемой системы электронной коммерции созданы с использованием языка Java, оптимальным способом создания алгоритма повышения надежности является построение аутентификации по стандарту JWT.

JSON Web Token (JWT) – это способ построения уникального ключа аутентификации в соответствии со стандартом RFC 7519 [11]. Данные пользователя, пересылаемые с использованием JWT сообщения, подписываются с помощью JWT-токена. Таким образом, получатель может убедиться в подлинности сообщения. Однако существенным недостатком JWT является то, что данный стандарт не подразумевает шифрования передаваемой информации.

JWT сообщение состоит из нескольких частей: заголовок, полезная нагрузка, подпись сообщения.

Процесс аутентификации пользователя средствами JWT происходит следующим образом [12], [13], [14]:

– клиент обращается на сервер с помощью публичного аутентификационного ключа;

– сервер создаёт JWT-токен и отправляет его в клиентское приложение;

– при последующих запросах клиент добавляет полученный токен, формируя таким образом JWT сообщение;

– при каждом запросе, сервер определяет, является ли пользователь тем, за кого себя выдает.

На последнем шаге серверное приложение использует криптографический алгоритм, который позволят проверить, является ли входящее JWT сообщение именно тем, что было создано сервером для конкретного пользователя. Этот процесс называется JWT верификацией.

Особенность технологии JWT состоит в том, что она применяется не для сокрытия или маскировки данных, а только для подписи сообщения с целью аутентификации источника данных. Аутентификационный публичный ключ в виде JWT-токена приходит в клиентское приложение в открытом виде и легко может быть перехвачен злоумышленником.

Был проведен обзор аналогичных алгоритмов аутентификации. Поскольку было принято решение о реализации программного обеспечения системы электронной коммерции на языке Java, то в качестве возможных аналогов рассмотрены наиболее популярные Java библиотеки OAuth 2.0 [15] и Javax.crypto [16], содержащие соответствующие алгоритмы аутентификации. В таблице 1 представлено данное сравнение.

Таблица 1 - Сравнение аналогичных алгоритмов аутентификации

Алгоритм	Использование JWT	Алгоритм шифрования	Количество ключей	Длина ключа	Совмещение сигнатуры JWT подписи с шифром
Предлагаемый	Да	Модифицированный RSA	5	4096	Да
OAuth 2.0	Да	RSA	4	2048	Нет
Javax.crypto	Нет	RSA	4	2048	Нет

На основе выявленных в таблице 1 недостатков существующих алгоритмов аутентификации, было принято решение создать свой алгоритм аутентификации, который будет отличаться от известных алгоритмов большим количеством ключей, большей длиной ключа, совмещением сигнатуры JWT подписи с шифром, использованием модифицированного асимметричного алгоритма шифрования на основе RSA. Предлагаемый алгоритм аутентификации позволяет повысить надежность процесса аутентификации пользователей в системе электронной коммерции.

В качестве модифицированного алгоритма шифрования была предложена модификация популярного алгоритма RSA, которая позволяет повысить уровень криптостойкости шифра.

Важнейшей частью асимметричного алгоритма шифрования RSA является функция вычисления модуля, которая дополнительно рандомизирует псевдослучайные значения, генерируемые компьютером. Функция модуля обычно использует случайный характер расположения простых и составных чисел на числовой прямой. В стандартной реализации RSA для этого используется функция Эйлера, имеющая вид [15]:

$$\varphi(n) = \begin{cases} n-1, & \text{если } n - \text{ простое}, \\ \prod_{p|n}^{n}\left(1-\frac{1}{p}\right), & \text{если } n - \text{ любое составное} \end{cases} \quad (1)$$

где n – случайное сгенерированное число, $n \in \mathbb{Z}, n > 0$, p – простое число, итерирующее все разложения числа n на простые множители.

Для повышения разброса случайных чисел, формирующих модуль, целесообразна замена функции Эйлера на родственную функцию, дающую расходящуюся последовательность чисел. Такой цели может служить функция Кармайкла [17]:

$$\lambda(n) = \begin{cases} \frac{1}{2}\varphi(n), & \text{если } \exists k : n = 2^k, k \geq 3, \\ \varphi(n), & \text{в остальных случаях} \end{cases}, \quad (2)$$

Комбинированный алгоритм аутентификации совмещает как использование JWT-токена с целью аутентификации, так и модифицированный асимметричный алгоритм шифрования всех данных системы с целью защиты информации.

Диаграммы деятельности для модифицированного алгоритма аутентификации показаны на рисунках 5 и 6.

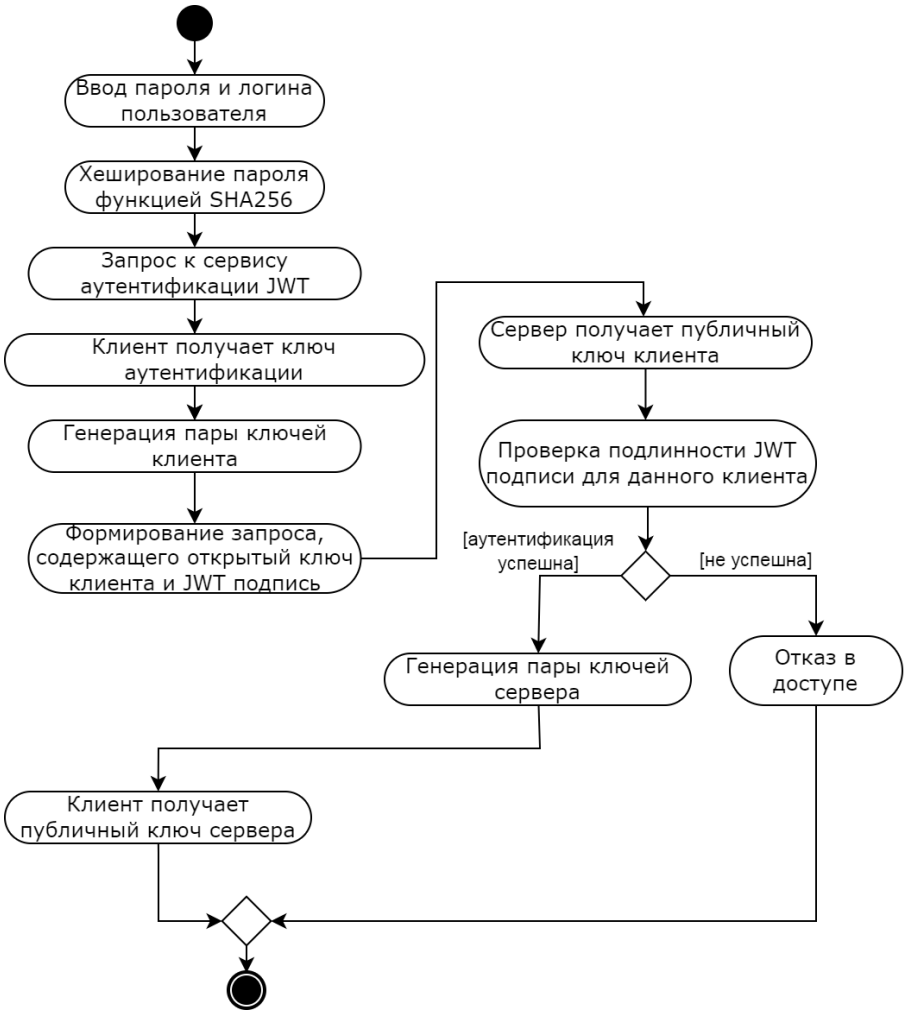

Рисунок 5 - Диаграмма деятельности модифицированного алгоритма аутентификации на этапе обмена ключами

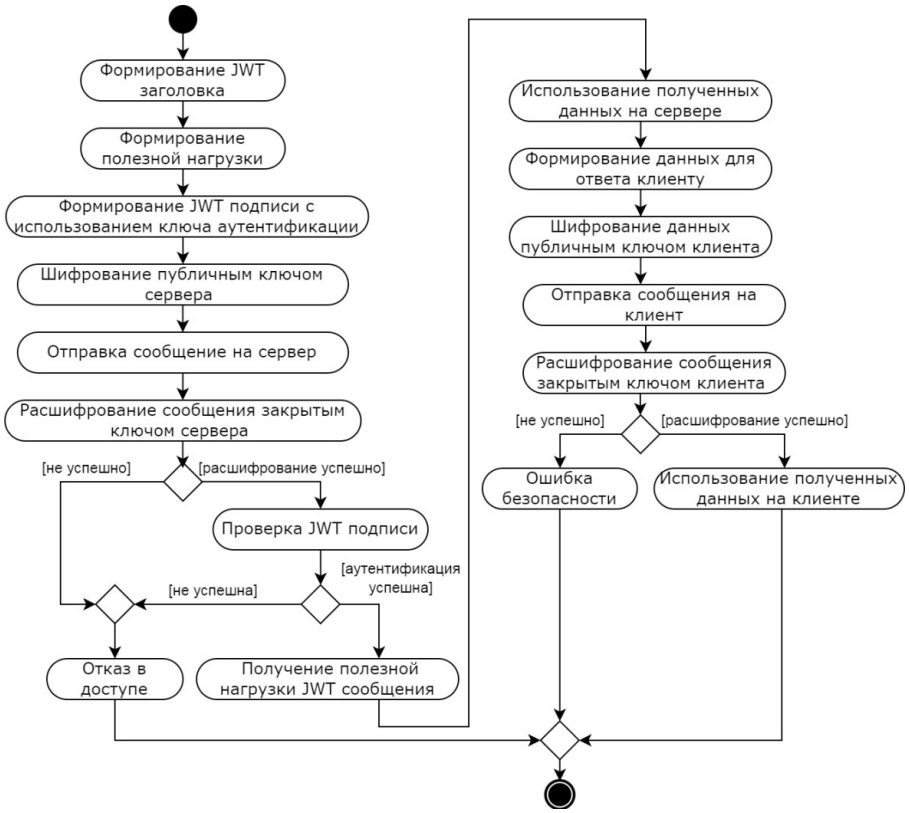

Рисунок 6 - Диаграмма деятельности модифицированного алгоритма аутентификации на этапе использования ключей

Предлагаемый алгоритм подразумевает использование пяти ключей – двух пар открытых и закрытых ключей шифрования и одного публичного ключа аутентификации. Сообщения, которые пересылаются между компонентами системы, не только шифруются модифицированным асимметричным алгоритмом шифрования, но и содержат JWT сообщение, включающее токен аутентификации.

Данная особенность позволяет повысить криптографическую стойкость процесса аутентификации. Исходя из этого, разработанный алгоритм аутентификации для системы электронной коммерции является обоснованным и позволяет сделать вывод о преимуществе системы электронной коммерции в безопасности аутентификации.

Заключение

В ходе проведенного исследования, с учетом сформулированной цели, был показан процесс разработки модифицированного алгоритма аутентификации в системе электронной коммерции с целью повышения надежности процесса аутентификации пользователей.

Научная новизна проведенного исследования заключается в том, что предложен модифицированный алгоритм аутентификации, который отличается от известных алгоритмов наличием пяти ключей, а именно: двух пар открытых и закрытых ключей шифрования и одного публичного ключа аутентификации, а также комбинированным использованием JWT аутентификации и модифицированного алгоритма ассиметричного шифрования RSA, позволяющего повысить криптографическую стойкость шифра. Все вышеперечисленное позволяет повысить надежность процесса аутентификации в системе электронной коммерции.

Кроме того, на этапе проектирования системы электронной коммерции была разработана онтологическая модель предметной области. Также была разработана имитационная модель для оптимизации режима работы службы доставки. Созданная имитационная модель имеет комплексный характер и учитывает взаимодействие программного обеспечения разрабатываемой системы электронной коммерции и человеческий фактор сотрудников службы доставки.

Полученные результаты использованы для повышения уровня защищённости процесса аутентификации в системе электронной коммерции, реализованной на языке Java.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Тепин К.С. Имитационное моделирование бизнес-процессов системы электронной коммерции / К.С. Тепин, В.Н. Князев // Сборник избранных статей Международной научной конференции: Высокие технологии и инновации в науке. — Санкт-Петербург, 2022. — С. 131-134.

2. Тепин К.С. Исследование работы службы доставки предприятия электронной коммерции средствами имитационного моделирования / К.С. Тепин, В.Н. Князев // Сборник избранных статей Всероссийской (национальной) научной конференции: Фундаментальные и прикладные исследования. Актуальные проблемы и достижения. — Санкт-Петербург, 2022. — С. 26-28.

3. Тепин К.С. Проектирование программной системы электронной коммерции средствами языка UML / К.С. Тепин, В.Н. Князев // Сборник избранных статей Международной студенческой научной конференции: Поколение будущего. — Санкт-Петербург, 2022. — С. 85-89.

4. Тепин К.С. Исследование предприятия электронной коммерции средствами имитационного моделирования / К.С. Тепин // Сборник статей V Международного научно-исследовательского конкурса: Молодежный исследовательский потенциал. — Петрозаводск, 2022. — С. 90-102.

5. Тепин К.С. Вопросы применения экспертных систем в электронной торговле / К.С. Тепин, А.Г. Михалев, В.Н. Князев // Сборник научных статей IX Всероссийской межвузовской научно-практической конференции: Информационные технологии в науке и образовании. Проблемы и перспективы / Под редакцией Л.Р. Фионовой. — Пенза, 2022. — С. 91-94.

6. Тепин К.С. Разработка мобильного приложения для поддержки бизнес-процессов торгового предприятия / К.С. Тепин // Сборник статей XX Международного научно-исследовательского конкурса: Научные достижения и открытия 2021. — Пенза, 2021. — С. 36-43.

7. Цуканова Н.И. Онтологическая модель представления и организации знаний / Н.И. Цуканова. — М.: Горячая линия-Телеком, 2015. — 272 с.

8. Омассон Ж.Ф. О криптографии всерьез / Ж.Ф Омассон. — М.: ДМК Пресс, 2021. — 328 с.

9. Ажмухамедов И.М. Принципы обеспечения комплексной безопасности информационных систем / И.М. Ажмухамедов // Вестник Астраханского государственного технического университета. — 2016. — № 1 — С. 23-27.

10. Светлов М.С. Методы повышения надежности программного обеспечения информационных систем / М.С. Светлов // Математические методы в технике и технологиях ММТТ. — 2015. — № 10-2(59). — С. 109-113.

11. Introduction to JSON Web Tokens. — URL: https://jwt.io/introduction (accessed: 02.03.23).

12. Колесников А.О. Идентификация пользователей клиент-серверных приложений с помощью JWT-токена / А.О. Колесников // Сборник статей XXXVI международной научно-практической конференции. — Москва, 2021. — С. 42-43.

13. Лукашкин Е.В. Разработка аутентификации, базирующейся на JWT-токенах / Е.В. Лукашкин // Материалы XXIII Республиканской научной конференции студентов и аспирантов. — Гомель, 2020. — С. 268-269.

14. Макаров Д.А. Механизм авторизации с использованием технологии JWT / Д.А. Макаров // Теория и практика современной науки. — 2020. — № 1(55) — С. 474-476.

15. OAuth 2.0 Authorization Framework. — URL: https://auth0.com/docs/authenticate/protocols/oauth (accessed: 11.05.23).

16. Package javax.crypto. — URL: https://docs.oracle.com/en/java/javase/11/docs/api/java.base/javax/crypto/package-summary.html (accessed: 11.05.23).

17. Ишмухаметов Ш.Т. Введение в теорию чисел и теорию кодирования / Ш.Т. Ишмухаметов, Р.Х. Латыпов, Р.Г. Рубцова [и др.] — М.: Казанский университет, 2014. — 65 с.

Список литературы на английском языке / References in English

1. Tepin K.S. Imitacionnoe modelirovanie biznes-processov sistemy elektronnoj kommercii [Simulation Modeling of Business Processes of E-commerce Systems] / K.S. Tepin, V.N. Knyazev // Sbornik izbrannyh statej Mezhdunarodnoj nauchnoj konferencii: Vysokie tekhnologii i innovacii v nauke [Collection of selected articles of the International Scientific Conference: High Technologies and Innovations in Science]. — St. Petersburg, 2022. — P. 131-134. [in Russian]

2. Tepin K.S. Issledovanie raboty sluzhby dostavki predpriyatiya elektronnoj kommercii sredstvami imitacionnogo modelirovaniya [Research of the Delivery Service of an E-commerce Enterprise by Means of Simulation Modeling] / K.S. Tepin, V.N. Knyazev // Sbornik izbrannyh statej Vserossijskoj (nacional'noj) nauchnoj konferencii: Fundamental'nye i prikladnye issledovaniya. Aktual'nye problemy i dostizheniya [Collection of selected articles of the All-Russian (National) Scientific Conference: Fundamental and Applied Research. Current Problems and Achievements]. — St. Petersburg, 2022. — P. 26-28. [in Russian]

3. Tepin K.S. Proektirovanie programmnoj sistemy elektronnoj kommercii sredstvami yazyka UML [Designing an E-commerce Software System by Means of the UML Language] / K.S. Tepin, V.N. Knyazev // Sbornik izbrannyh statej Mezhdunarodnoj studencheskoj nauchnoj konferencii: Pokolenie budushchego [Collection of selected articles of the International Student Scientific Conference: The Generation of the Future]. — Saint Petersburg, 2022. — P. 85-89. [in Russian]

4. Tepin K.S. Issledovanie predpriyatiya elektronnoj kommercii sredstvami imitacionnogo modelirovaniya [Research of an E-commerce Enterprise by Means of Simulation Modeling] / K.S. Tepinv // Sbornik statej V Mezhdunarodnogo nauchno-issledovatel'skogo konkursa: Molodezhnyj issledovatel'skij potencial [Collection of articles of the V International Research Competition: Youth Research Potential]. — Petrozavodsk, 2022. — P. 90-102. [in Russian]

5. Tepin K.S. Voprosy primeneniya ekspertnyh sistem v elektronnoj torgovle [Questions of the Use of Expert Systems in Electronic Commerce] / K.S. Tepin, A.G. Mikhalev, V.N. Knyazev // Sbornik nauchnyh statej IH Vserossijskoj mezhvuzovskoj

nauchno-prakticheskoj konferencii: Informacionnye tekhnologii v nauke i obrazovanii. Problemy i perspektivy [Collection of scientific articles of the IX All-Russian Interuniversity Scientific and Practical Conference: Information Technologies in Science and Education. Problems and Prospects] / Edited by L.R. Fionova. — Penza, 2022. — P. 91-94. [in Russian]

6. Tepin K.S. Razrabotka mobil'nogo prilozheniya dlya podderzhki biznes-processov torgovogo predpriyatiya [Development of a Mobile Application to Support Business Processes of a Trading Enterprise] / K.S. Tepin // Sbornik statej HKH Mezhdunarodnogo nauchno-issledovatel'skogo konkursa: Nauchnye dostizheniya i otkrytiya 2021 [Collection of articles of the XX International Research Competition: Scientific Achievements and Discoveries 2021]. — Penza, 2021. — P. 36-43. [in Russian]

7. Tsukanova N.I. Ontologicheskaya model' predstavleniya i organizacii znanij [Ontological Model of Representation and Organization of Knowledge] / N.I. Tsukanova. — M.: Hotline-Telecom, 2015. — 272 p. [in Russian]

8. Omasson J.F. O kriptografii vser'ez [About Cryptography Seriously] / J.F. Omasson. — Moscow: DMK Press, 2021. — 328 p. [in Russian]

9. Azhmukhamedov I.M. Principy obespecheniya kompleksnoj bezopasnosti informacionnyh sistem [Principles of Ensuring Complex Security of Information Systems] / I.M. Azhmukhamedov // Vestnik Astrahanskogo gosudarstvennogo tekhnicheskogo universiteta [Bulletin of the Astrakhan State Technical University]. — 2016. — № 1 — P. 23-27. [in Russian]

10. Svetlov M.S. Metody povyshenija nadezhnosti programmnogo obespechenija informacionnyh sistem [Methods of Increasing the Reliability of Software Support of Information Systems] / M.S. Svetlov // Matematicheskie metody v tehnike i tehnologijah MMTT [Mathematical Methods in Engineering and Technologies of MMTT]. — 2015. — № 10-2(59). — P. 109-113. [in Russian]

11. Introduction to JSON Web Tokens. — URL: https://jwt.io/introduction (accessed: 02.03.23).

12. Kolesnikov A.O. Identifikacija pol'zovatelej klient-servernyh prilozhenij s pomoshh'ju JWT-tokena [Identification of Users of Client-Server Applications Using a JWT Token] / A.O. Kolesnikov // Sbornik statej XXXVI mezhdunarodnoj nauchno-prakticheskoj konferencii [Collection of articles of the XXXVI International Scientific and Practical Conference]. — Moscow, 2021. — P. 42-43. [in Russian]

13. Lukashkin E.V. Razrabotka autentifikacii, bazirujushhejsja na JWT-tokenah [Development of Authentication Based on JWT Tokens] / E.V. Lukashkin // Materialy XXIII Respublikanskoj nauchnoj konferencii studentov i aspirantov [Materials of the XXIII Republican Scientific Conference of Students and Postgraduates]. — Gomel, 2020. — P. 268-269. [in Russian]

14. Makarov D.A. Mehanizm avtorizacii s ispol'zovaniem tehnologii JWT [Authorization Mechanism Using JWT Technology] / D.A. Makarov // Teorija i praktika sovremennoj nauki [Theory and Practice of Modern Science]. — 2020. — № 1(55) — P. 474-476. [in Russian]

15. OAuth 2.0 Authorization Framework. — URL: https://auth0.com/docs/authenticate/protocols/oauth (accessed: 11.05.23).

16. Package javax.crypto. — URL: https://docs.oracle.com/en/java/javase/11/docs/api/java.base/javax/crypto/package-summary.html (accessed: 11.05.23).

17. Ishmuhametov Sh.T. Vvedenie v teoriju chisel i teoriju kodirovanija [Stolov Introduction to Number Theory and Coding Theory] / Sh.T. Ishmuhametov, R.H. Latypov, R.G. Rubcova [et al.] — M.: Kazan University, 2014. — 65 p. [in Russian]