

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники
Кафедра инженерной психологии и эргономики

УДК 004.415.2.031.43

Новак
Павел Сергеевич

ИНЖЕНЕРНО– ПСИХОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНТЕРНЕТ–
ПЛОЩАДКИ ДЛЯ СОВЕРШЕНИЯ СДЕЛОК В СФЕРЕ ЭЛЕКТРОННОЙ
КОММЕРЦИИ

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

1-23 80 08 – Психология труда, инженерная психология, эргономика

Магистрант П.С. Новак

Научный руководитель
Н.И. Силков, кандидат
технических наук, доцент

Заведующий кафедрой ИПиЭ
К.Д. Яшин, кандидат
технических наук, доцент

Нормоконтролер
Ю.Д. Пашковская, старший
преподаватель, магистр
технических наук

Минск 2020

ВВЕДЕНИЕ

В настоящее время уровень продаж через сетевое соединение с сетями международного информационного обмена (Интернет) очень высок. Этому способствует множество причин, однако основной является то, что такая форма продажи удобна как для покупателя, так и для продавца.

Однако существует одна большая проблема: велик риск столкнуться с недобросовестным продавцом или мошенником. Чтобы решить данную проблему, необходимо организовать такую сделку, чтобы и покупатель и продавец были максимально (на сколько это возможно) уверены в том, что все условия сделки будут соблюдены со стороны их оппонентов. Одним из вариантов является вовлечение третьей стороны, а именно сервиса-гаранта (эскроу). При таком подходе сделка происходит в следующем порядке:

- 1) Согласование сторон на предмет передачи товара, оказания услуг и денег;
- 2) Передача товара, данных и денег эскроу-сервису и соответственно осведомление участников;
- 3) Проверка достоверности, качества исполнения (использование скриншотов, видео в качестве доказательства);
- 4) Передача эскроу-сервисом денежных средств исполнителю (если все стороны удовлетворены);
- 5) В случае спорных моментов, с которыми случается сталкиваться, происходит возврат данных, товара и денежных средств;

Однако на сегодняшний момент, существует немало escrow-сервисов, и для того, чтобы новый сервис не "затерялся" среди имеющихся на рынке, он должен соответствовать определённым инженерно-психологическим требованиям, так как главным показателем успешности такого веб-сервиса является количество пользователей сервиса и сумма, на которую данные пользователи не будут бояться совершать сделки.

Цель диссертации: реализация и инженерно-психологическое обеспечение интернет-площадки для совершения сделок в сфере электронной коммерции.

Задачи:

- 1) провести аналитический обзор аналогов и технологий разработки интернет-площадок для совершения сделок в сфере электронной коммерции;
- 2) спроектировать и реализовать веб-сервис для совершения сделок в сфере электронной коммерции;
- 3) провести испытания разработанного сервиса;

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель работы: реализация и инженерно-психологическое обеспечение интернет-площадки для совершения сделок в сфере электронной коммерции.

Актуальность: уровень продаж через сетевое соединение с сетями международного информационного обмена (Интернет) очень высок, однако велик риск столкнуться с недобросовестным продавцом или мошенником.

Объектом исследования выступает система "человек - веб-сайт".

Предмет исследования - методы реализации и улучшения веб-сервисов для совершения сделок в сфере электронной коммерции.

В результате работы разработана и улучшена интернет-площадка для совершения сделок в сфере электронной коммерции, проведено юзабилити тестирование разработанной площадки.

Структура магистерской диссертации представлена тремя главами, где проводится аналитический обзор аналогов и технологий разработки интернет-площадок для совершения сделок в сфере электронной коммерции, рассматривается проектирования и практическая разработка интернет-площадки, предоставляются результаты испытания разработанной площадки на предмет юзабилити.

Результаты работы были апробированы на 56-ой Научной Конференции Аспирантов, Магистрантов и Студентов БГУИР.[1-А][2-А]

СОДЕРЖАНИЕ РАБОТЫ

В первой главе проводится аналитический обзор следующих аналогов: Escrow.com, Skydeal и Boulevard Escrow .

Сервис Escrow.com считается одним из лучших сервисов для проведения безопасных сделок с точки зрения риска контрагента, так как обеспечивается безопасность (в финансовом плане) как покупателя, так и продавца, а все средства, используемые в транзакции, депонируются.

Достоинства сервиса:

а) большое количество типов товаров, которые могут использоваться в сделке;

б) самый надежный, лицензированный эскроу-сервис в мире согласно отзывам представителей ведущих компаний электронной коммерции, включая Uniregistry, GoDaddy, ClassicCars.com и AutoTrade.

Недостатки сервиса:

а) большая комиссия;

б) отсутствует чат.

SkyDeal – это сервис защищенной сделки, позволяющей снизить риски проведения торговых сделок как для покупателя, так и для продавца.

Принцип работы SkyDeal заключается в удержании суммы оплаты по сделке на SkyBuy до того момента пока товар не будет доставлен покупателю, и покупатель не подтвердит его соответствие условиям сделки или не истечет срок на приемку товара со стороны покупателя.

Достоинства сервиса:

а) возможность размещения собственного интернет магазина на сервисе;

б) наличие внутреннего чата;

в) большое количество типов товаров, которые могут использоваться в сделке.

Недостатки сервиса:

а) продавцу нет возможности разметить частное объявление, таким образом для создания сделки ему необходимо размещать только свой интернет магазин;

б) большая комиссия, так как необходимо оплатить и доставку товара (если не самовывоз) и непосредственно комиссию сервиса;

в) согласно отзывам, хоть внутренний чат и присутствует, но пользователю, который впервые пользуется услугами данного сервиса, сложно в нём разобраться.

Boulevard Escrow – это сервис, где предоставляются услуги условного депонирования для предприятий и частных лиц по всем США.

Достоинства сервиса:

а) широкий список типов сделок, с которыми работает сервис;

б) на сервисе имеется подробная информация о каждой категории сделок.

Недостатки сервиса:

- а) нет автоматизации проведения сделки;
- б) нельзя произвести расчёты по сумме, которая должна платиться покупателем продавцу включая комиссию сервиса, средствами самого сервиса;
- в) отсутствует внутренний чат.

Далее при помощи инструмента Google Trends проводится исследование в области динамики популярности рассмотренных аналогов с целью выявления дополнительных требований к разрабатываемой интернет-площадке для совершения сделок в сфере электронной коммерции.

Google Trends - это публичное web-приложение корпорации Google, основанное на поиске Google, которое показывает, как часто определенный термин ищут по отношению к общему объему поисковых запросов в различных регионах мира и на различных языках. На горизонтальной оси основного графика представлено время (начиная с некоторого момента в 2004), а на вертикальной — как часто термин искали по отношению к общему числу поисковых запросов во всем мире. Под основным графиком отображается распределение популярности по регионам, городам и языкам.

Результат сравнения динамики популярности за 12 месяцев рассмотренных выше escrow-сервисов представлен на рисунке 1.1:

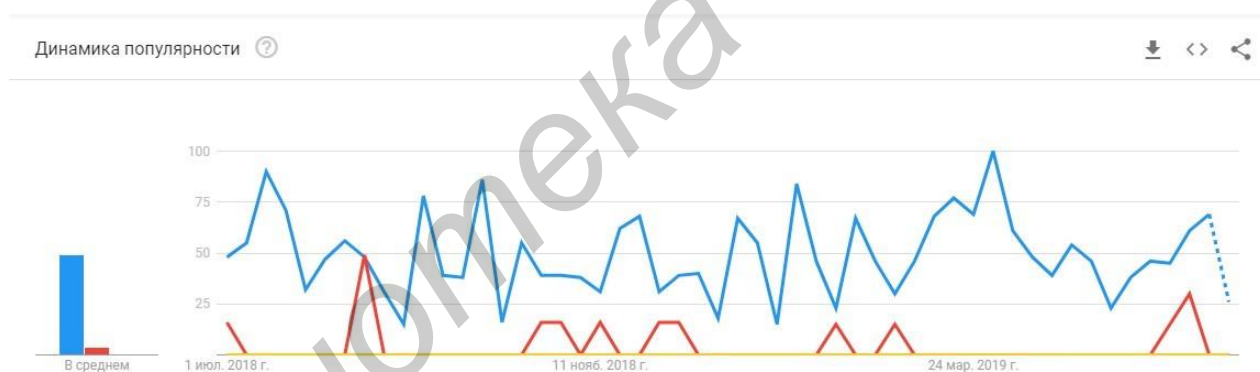


Рисунок 1.1 График сравнения динамики популярности

Синий график - Escrow.com, красный - SkyDeal, желтый - Boulevard Escrow.

В графике динамики популярности числа обозначают уровень интереса к теме по отношению к наиболее высокому показателю в таблице для определенного региона и периода времени. 100 баллов означают наивысший уровень популярности запроса, 50 – уровень популярности запроса, вдвое меньший по сравнению с первым случаем. 0 баллов означает местоположение, по которому недостаточно данных о рассматриваемом запросе.

По результатам исследования очевидно, что решения, которые были приняты при разработке сервиса Escrow.com являются самыми правильными, а решения, которые были приняты при разработке сервиса Boulevard Escrow - самыми неправильными. Таким образом, составлены требования, которыми должна обладать интернет-площадка для совершения сделок в сфере электронной коммерции:

- а) должна присутствовать автоматизация проведения сделки;
- б) желательно наличие внутреннего чата;
- в) желательно наличие неограниченного типа товаров, которые могут использоваться в сделке.

В конце первой главы проводится постановка задач магистерской диссертации: разработать и апробировать интернет-площадку для совершения сделок в сфере электронной коммерции.

Во второй главе описана разработка интернет-площадки для совершения сделок в сфере электронной коммерции.

Для того, чтобы создать удобный и качественный веб-сервис для совершения безопасных сделок необходимо соблюдать следующие требования:

- а) расширяемость функциональных возможностей;
- б) безопасность совершения сделки;
- в) стабильная работа сервиса.

К функциональным же требованиям относятся:

- а) синхронизация данных между браузером пользователя и сервером;
- б) хранение данных в кэше браузера;
- в) авторизация пользователей;
- г) функции создания, просмотра, редактирования и удаления сделок;
- д) удобная навигация по сделкам;
- е) возможность применения фильтров для списков элементов;
- ж) функции для поиска пользователей;
- з) уведомления;
- и) сохранение истории операций по сделке;
- к) возможность передачи файлов, необходимых для осуществления сделки.

Диаграмма вариантов использования представлена на рисунке 1.2.

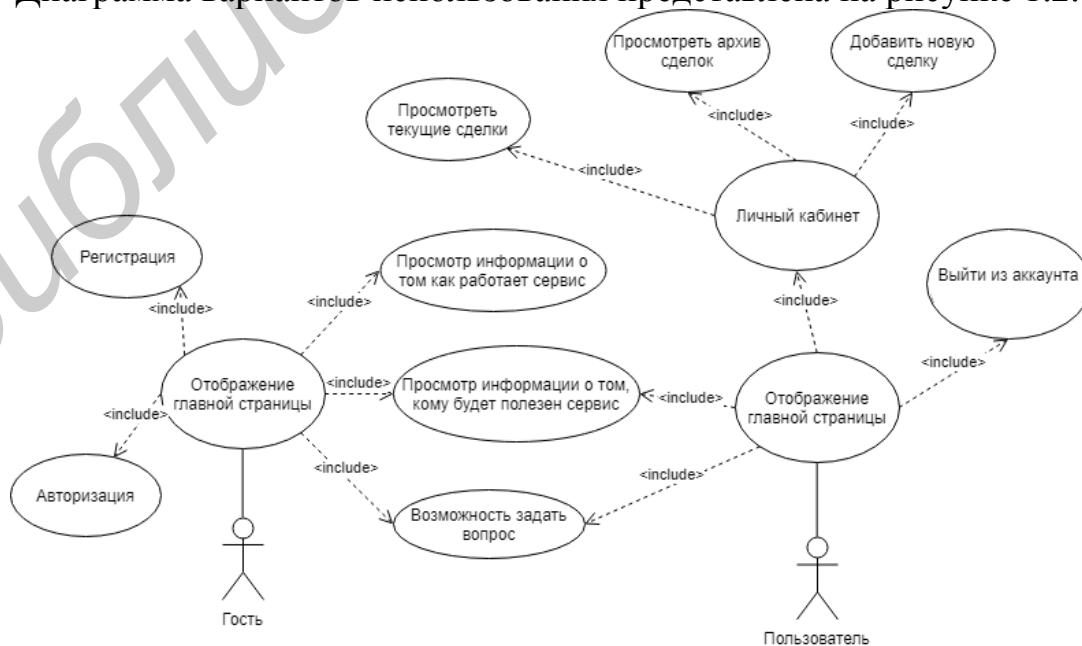


Рисунок 1.2 Диаграмма вариантов использования

Схема клиент-серверной архитектуры изображена на рисунке 1.3.

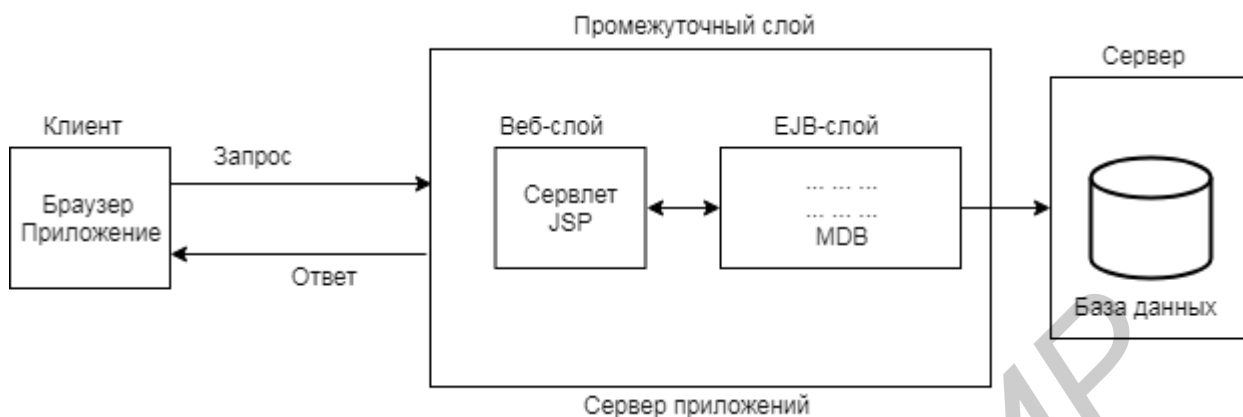


Рисунок 1.3 Схема клиент-серверной архитектуры

В качестве паттерна проектирования использовался паттерн MVC, который схематично изображен на рисунке 1.4.

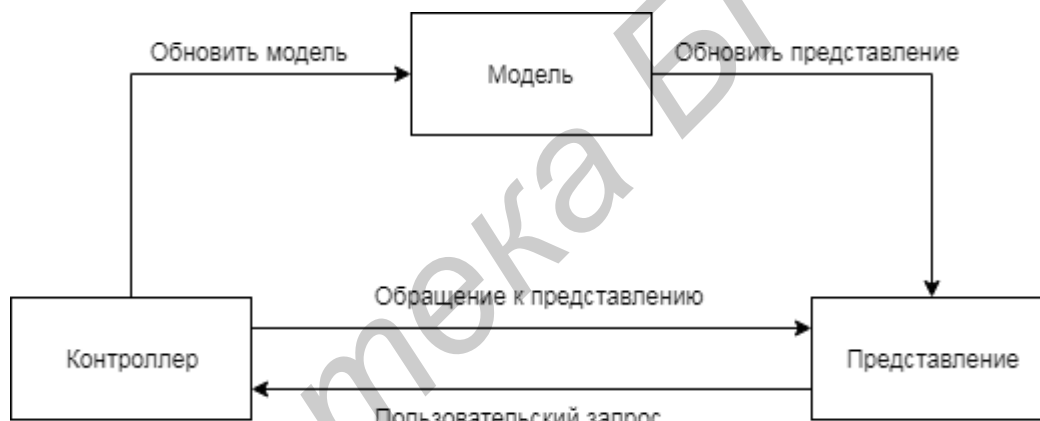


Рисунок 1.4 Паттерн MVC

В целях безопасности для хранения локального таких данных, как пароли пользователей, адреса электронной почты пользователей и т. д. использовался алгоритм хеширования md5, для передачи же данных на сервер использовался алгоритм шифрования aes-128.

MD5 является одним из алгоритмов хеширования на 128-битной основе. Под хешированием понимают преобразование входных данных по определенному алгоритму в битовую строку определенной длины. При этом полученный в ходе вычислений результат представлен в шестнадцатеричной системе исчисления. Она называется хешем, хеш-суммой или хеш-кодом.

Процесс хеширования широко применяется в программировании и веб-индустрии. В основном для создания уникальных значений в ассоциативных массивах, идентификаторов.

AES - симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит).

Алгоритм AES представляет блок данных в виде двумерного байтового массива размером 4x4. Все операции производятся над отдельными байтами массива, а также над независимыми столбцами и строками.

В каждом раунде алгоритма выполняются следующие преобразования:

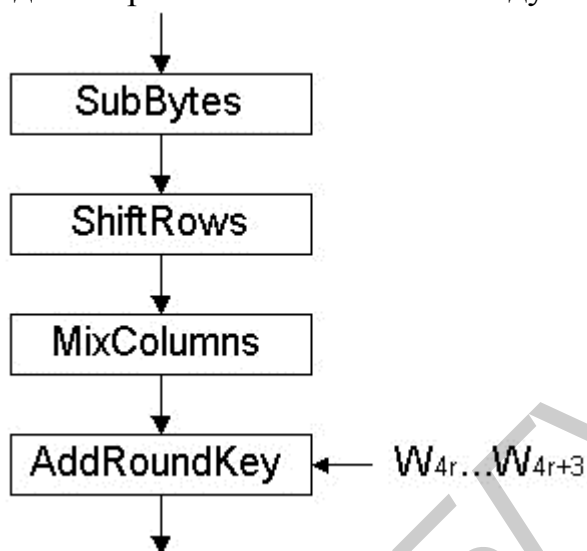


Рисунок 1.5 Схема раунда шифрования

1) Операция SubBytes представляет собой табличную замену каждого байта массива данных.

2) Операция ShiftRows выполняет циклический сдвиг влево всех строк массива данных, за исключением нулевой. Сдвиг i -ой строки массива (для $i = 1, 2, 3$) производится на i байт.

3) Операция MixColumns. Выполняет умножение каждого столбца массива данных на фиксированный полином $a(x) : a(x) = 3x^3 + x^2 + x + 2$. Умножение выполняется по модулю $x^4 + 1$.

4) Операция AddRoundKey выполняет наложение на массив данных материала ключа. А именно, на i -ый столбец массива данных ($i=0...3$) побитовой логической операцией «исключающее или» (XOR) накладывается определенное слово расширенного ключа W_{4r+i} , где r – номер текущего раунда алгоритма, начиная с 1.

Перед первым раундом алгоритма выполняется предварительное наложение материала ключа с помощью операции AddRoundKey, которая выполняет наложение на открытый текст первых четырех слов расширенного ключа $W_0...W_3$.

Последний же раунд отличается от предыдущих тем, что в нем не выполняется операция MixColumns.

Расшифрование выполняется применением обратных операций в обратной последовательности. Соответственно, перед первым раундом расшифрования выполняется операция AddRoundKey (которая является обратной самой себе), выполняющая наложение на шифртекст четырех последних слов расширенного ключа, т.е. $W_{4R}...W_{4R+3}$. Затем выполняется R

раундов расшифрования, каждый из которых выполняет следующие преобразования:

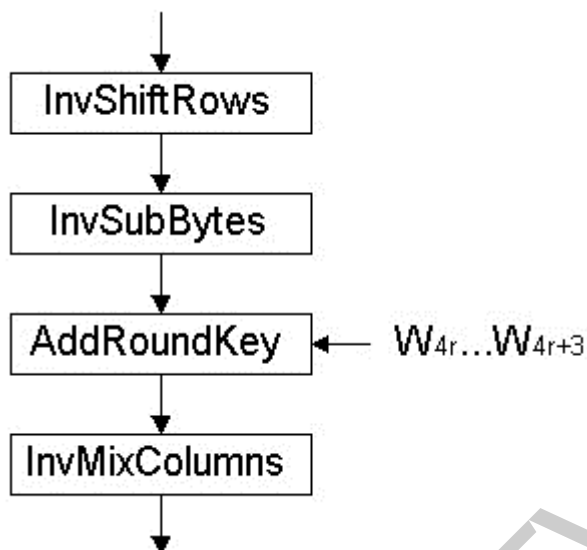


Рисунок 1.6 Схема раунда расшифрования

1) Операция `InvShiftRows` выполняет циклический сдвиг вправо трех последних строк массива данных на то же количество байт, на которое выполнялся сдвиг операцией `ShiftRows` при зашифровании.

2) Операция `InvSubBytes` выполняет побайтно обратную табличную замену.

3) Операция `AddRoundKey`, как и при зашифровании, выполняет наложение на обрабатываемые данные четырех слов расширенного ключа $W_{4r...W_{4r+3}}$. Однако, нумерация раундов r при расшифровании производится в обратную сторону – от $R-1$ до 0 .

4) Операция `InvMixColumns` выполняет умножение каждого столбца массива данных аналогично прямой операции `MixColumns`, однако, умножение производится на полином $a^{-1}(x)$, определенный следующим образом: $a^{-1}(x) = B_x^3 + D_x^2 + 9_x + E$.

Аналогично зашифрованию, последний раунд расшифрования не содержит операцию `InvMixColumns`.

В третьей главе было проведено юзабилити-тестирование разработанного веб-сервиса. В процессе тестирования отслеживались следующие метрики:

- интуитивность этапа создания сделки;
- степень достижения поставленной цели;
- время на выполнение основных этапов (от момента создания сделки, до момента попадания в чат).

По итогам первичного юзабилити-тестирования было выявлено, что пользователи имели проблемы в понимании этапа создания сделки, для решения данной проблемы была добавлена возможность просмотреть экран помощи.

В следствие проведенного первичного юзабилити-тестирования веб-сервис был доработан, что было доказано улучшившимися результатами в повторном юзабилити-тестировании.

Библиотека БГУИР

ЗАКЛЮЧЕНИЕ

В рамках магистерской диссертации решены следующие задачи:

а) Проведён аналитический обзор аналогов и технологий разработки интернет-площадок электронной коммерции.

В рамках данной задачи проведён аналитический обзор таких сервисов, как Escrow.com, Skydeal и Boulverad Escrow. Далее, для составления требований к интернет-площадке для совершения сделок в сфере электронной коммерции, произведено исследование рассмотренных аналогов на предмет динамики популярности. Исходя из результатов данного исследования составлены требования, которыми должна обладать интернет-площадка для совершения сделок в сфере электронной коммерции:

- а) должна присутствовать автоматизация проведения сделки;
- б) желательно наличие внутреннего чата;
- в) желательно наличие неограниченного типа товаров, которые могут использоваться в сделке.

Также в рамках данной задачи изучены такие важные понятия, как юзабилити, эргономика, escrow-счет, escrow-агент, защищенная (безопасная) сделка, инженерная психология, система "человек-машина", инженерно-психологическое проектирование, эргономическое проектирование и составлены дальнейшие задачи на магистерскую диссертацию.

б) Реализована интернет-площадка для совершения сделок в сфере электронной коммерции.

При реализации интернет-площадки для совершения сделок в сфере электронной коммерции составлены функциональные требования, разработана диаграмма вариантов использования, разработана архитектура веб-сервиса и база данных, использовался язык программирования Java, контейнер сервлетов Tomcat и реляционная система управления базами данных MySQL. Для обеспечения принципов безопасности в качестве алгоритма хэширования использовался алгоритм md5, а в качестве алгоритма фишрования – алгоритм AES.

в) Апробирована реализованная интернет-площадка.

В рамках подготовки к проведению юзабилити-тестирования разработанной интернет-площадки для совершения сделок в сфере электронной коммерции сделано следующее:

- 1) составлен портрет потенциального пользователя;
- 2) разработана система метрик;

Далее проведено юзабилити-тестирование среди людей, которые соответствуют всем параметрам, входящих в составленный портрет пользователя, по разработанной системе метрик.

В результате первичного тестирования была выявлена проблема с этапом создания сделок. Для решения данной проблемы интернет-площадка была модифицирована дополнительной функцией - экраном помощи.

В результате повторного тестирования, которое проводилось среди людей, которые не участвовали в первоначальном тестировании, но имеют похожие сферы деятельности, стало понятно, что после внедрения дополнительного функционала пользователем стало гораздо понятнее, какие действия должны быть при создании сделки, общее время выполнения основных этапов уменьшилось, а степень достижения поставленной цели увеличилась.

По материалам диссертационной работы представлен доклад на научной конференции.

Библиотека БГУИР

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А.) Новак П.С. Инженерно-психологические требования к интернет-площадке для совершения сделок в сфере электронной коммерции / П.С. Новак. Мн.: 56 Научная Конференция Аспирантов, Магистрантов и Студентов БГУИР, 2020.

2-А.) Новак П.С. Принципы программной реализации интернет-площадки для совершения сделок в сфере электронной коммерции / П.С. Новак. Мн.: 56 Научная Конференция Аспирантов, Магистрантов и Студентов БГУИР, 2020.

Библиотека БГУИР