



# БОЛЬШИЕ ВЫЗОВЫ

ВСЕРОССИЙСКИЙ КОНКУРС  
НАУЧНО-ТЕХНОЛОГИЧЕСКИХ ПРОЕКТОВ



Региональный трек  
Всероссийского конкурса  
научно-технологических проектов

**«БОЛЬШИЕ ВЫЗОВЫ»**

направление

**Умный город и безопасность**

название работы

Разработка расширения для  
браузера PassChain для  
хранения логинов и паролей на  
компьютере с использованием  
хэш-функций

участник(и)

**Василевский Владимир Игоревич**

#большиевызовы  
#МГК

г. Москва  
2021

[mgk.olimpiada.ru](http://mgk.olimpiada.ru)



# Актуальность моего проекта



Данная проектная работа посвящена распространенной в наше время проблеме хранения логинов и паролей от учетных записей в Интернете. Актуальность моей работы обусловлена тем, что в наше время люди активно пользуются разными сайтами, где требуется регистрация и создание учетных записей. К сожалению, сегодня часто происходят взломы учетных записей и утечка личных данных. Именно поэтому мной принято решение разработать расширение для браузера, которое обеспечит хранение логинов и паролей от различных веб-сайтов на компьютере пользователя. Наличие подобного расширения позволит существенно повысить безопасность хранения логинов и паролей.

# Цели проектной работы

- Целью моей проектной работы была разработка расширения для браузера, которое позволит хранить логины и пароли от учетных записей пользователя на его компьютере с использованием хэш-функций и технологии Blockchain.

# Задачи проектной работы

- Выявление и анализ главных проблем, связанных с безопасностью хранения логинов и паролей от учетных записей в Интернете.
- Изучение хэш-функций и технологии Blockchain для их применения в рамках разрабатываемого мной расширения.
- Изучение различных видов шифрования.
- Создание алгоритма для разработки расширения, основанного на указанной технологии.
- Разработка и тестирование расширения для хранения логинов и паролей на компьютере пользователя.

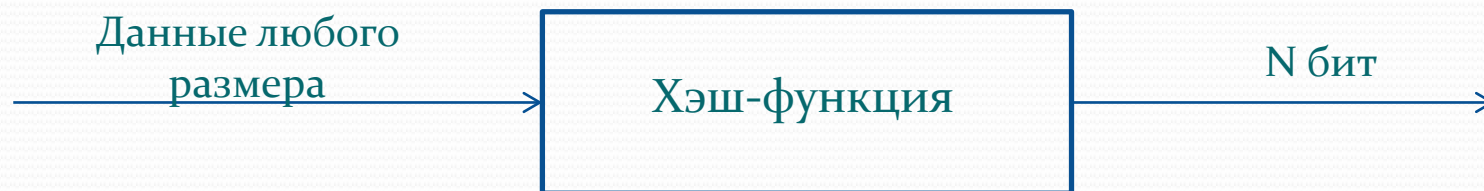
# Преимущества Passchain

В настоящее время существуют различные программы и приложения для хранения паролей. Это LastPass, Dashlane, Splikity, 1Password и многие другие. Они используют технологию, предусматривающую хранение соответствующих данных пользователя на серверах. Это потенциально может быть небезопасно. Предлагаемое мною расширение обеспечивает хранение паролей на компьютере пользователя и осуществляет автозаполнение соответствующих полей при заходе на сайт, что позволяет пользователю использовать любые, даже очень сложные пароли, так как необходимость в их запоминании отпадает.



# Что такое хэш-функция и для чего она применяется?

- Хэш-функция преобразует входные данные в битовую последовательность фиксированной длины. Соответствующая последовательность или строка называется хэшем или хэш-суммой.
- Ключ хэширования – это данные, отправляемые на вход хэш-функции.
- Хэш-функция является однонаправленной и необратимой и обычно используется для проверки целостности файлов и хранения паролей.



# Что такое Blockchain и для чего он применяется?



- Технология Blockchain – это выстроенная по определенным правилам цепочка блоков, содержащих информацию.
- Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хэш-сумму и хэш-сумму предыдущего блока.
- В случае изменения информации в блоке придется редактировать и все последующие блоки.



# Алгоритм работы расширения

Формируется нулевой блок блокчейна.



Пользователь осуществляет регистрацию на веб-сайте: вводит свой логин и пароль и нажимает на кнопку «Зарегистрироваться» или аналогичную кнопку.



Расширение Passchain предлагает пользователю сохранить пароль, проверив соответствующую пару (логин и пароль)



После нажатия на кнопку «Сохранить» формируется очередной блок блокчейна после шифрования пароля с помощью технологии AES и хэша предыдущего блока.



При повторном заходе пользователя на сайт, где он ранее зарегистрировался, происходит автозаполнение соответствующих полей.



# Используемый стандарт шифрования



## AES 256 ENCRYPTION

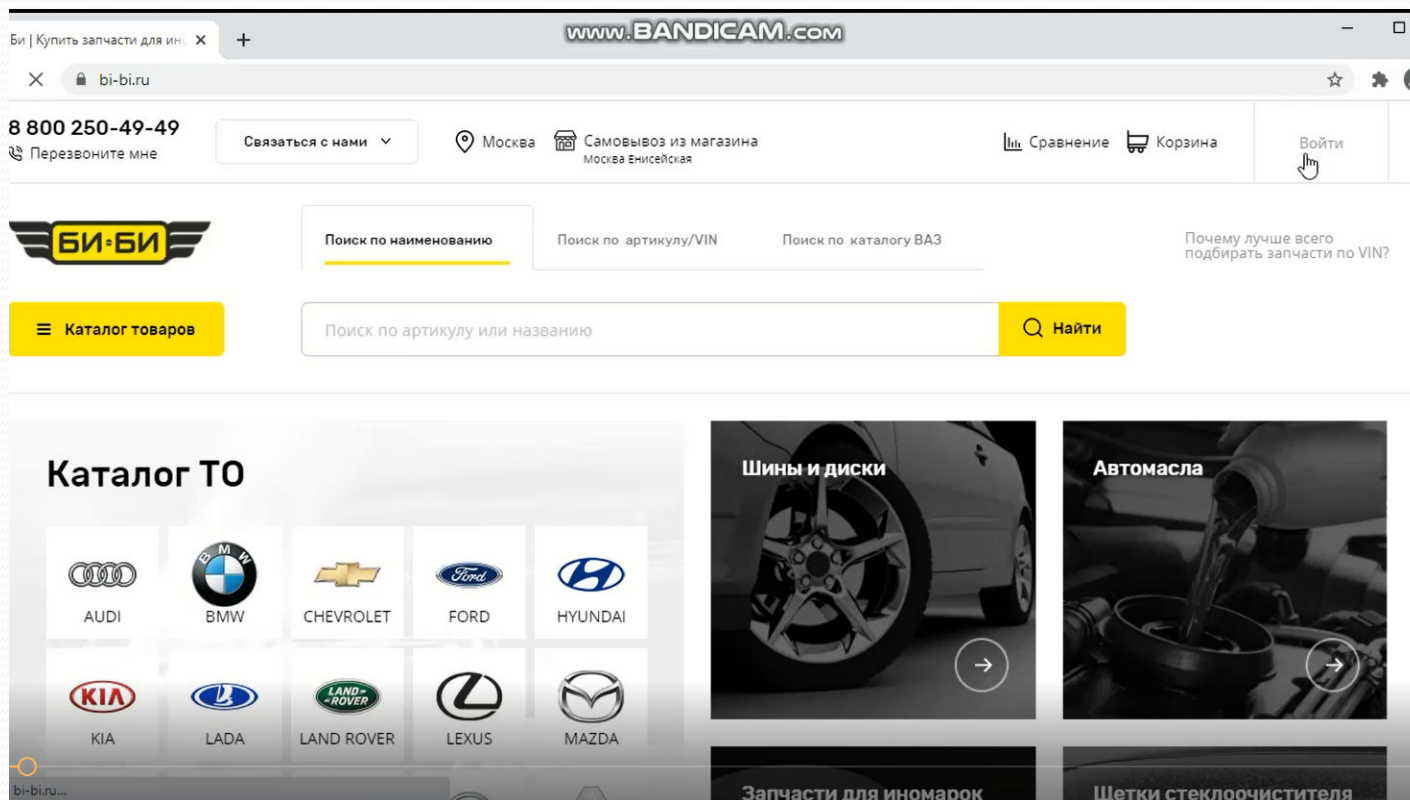
- Для дополнительной защиты пароля использовался стандарт шифрования AES.
- AES (Advanced Encryption Standard), также известный как Rijndael (Рейндал), представляет собой симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется.

# Фрагмент кода

Расширение написано на JavaScript, специально для этого изученного мною. Ниже представлен фрагмент кода моей программы:

```
1  chrome.runtime.onMessage.addListener(  
2  function(request, sender, sendResponse) {  
3  if(request.type==="set"){  
4  var b = request.block;  
5      let k=0  
6      while(localStorage.getItem(k) !== null){  
7          k+=1  
8          //console.log(k)  
9      }  
10     localStorage.setItem(k,b)  
11 }  
12 if(request.type==="get"){  
13     sendResponse({data: localStorage.getItem(request.id),len:localStorage.length });  
14 }  
15 if(request.type==="check"){  
16     var addr=request.addr;  
17     let k=1  
18     let ex=0;  
19     while(localStorage.getItem(k) !== null){  
20  
21         if(JSON.parse(localStorage.getItem(k)).address.hostname===addr){  
22             ex=1;  
23         }  
24         console.log(k)  
25         k+=1  
26     }  
27     sendResponse({data:ex });  
28 }  
29 });
```

# Как работает мое расширение (видео)



После сохранения в Passchain пользователь может увидеть в Панели управления паролями зашифрованный пароль. Расшифрованный пароль там представлен исключительно для цели демонстрации и исключен из финальной версии кода. В видео представлена цепочка из 3 блоков. Регистрация была произведена на веб-сайтах [www.ukazka.ru](http://www.ukazka.ru), [www.220-volt.ru](http://www.220-volt.ru), [www.bi-bi.ru](http://www.bi-bi.ru).



# Итоги и перспективы развития

- Поставленная передо мною цель проектной работы, состоящая в том, чтобы разработать расширение для хранения логинов и паролей от учетных записей в Интернете на компьютере пользователя, была мною выполнена.
- В будущем мною планируется разработать расширения для других браузеров (пока реализовано для Google Chrome), обеспечить синхронизацию для различных устройств, а также предложить пользователю автоматическую смену паролей через установленные им интервалы для целей обеспечения безопасности.

# Использовавшиеся ресурсы

- <https://club.dns-shop.ru/blog/t-57-tehnologii/30931-tehnologiya-blockchain-prostyimi-slovami>
- Математика в кибербезопасности. Kaspersky Academy. <https://stepik.org/course/62247/syllabus>
- [https://ru.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard)
- [www.dashlane.com](http://www.dashlane.com)
- [www.lastpass.com](http://www.lastpass.com)