УДК 004.514.6
DOI 10.18101/978-5-9793-1497-6-62-69

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И МЕНЕДЖЕР ПАРОЛЕЙ

© Жаркой Сергей Александрович
студент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: matem19961404@gmail.com

© Цыбикова Туяна Сандаликовна
кандидат педагогических наук, доцент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: cts2001@mail.ru

Актуальность обусловлена ростом числа атак на компоненты распределенных систем и возникающих от их реализации ущербов, а также вариантностью и непредсказуемостью таких атак. На данный момент в современном обществе Интернет стал центром развития новых технологии, в корне меняющий методы взаимодействия с информацией. В статье изучены основные понятия защиты информации, виды шифрования, а также кратко описано создание программы «Менеджер паролей».
Ключевые слова: менеджер, пароль, информация, безопасность, программа, данные, шифрование.

На сегодняшний день информация имеет цифровой формат. С помощью выхода в интернет можно получить практически любую услугу. Естественно сервисы нуждаются в аутентификации пользователя, и самый распространенный способ аутентификации является использование связки логин – пароль.

Но отсюда вытекает проблема, что надо запоминать все большее и большее количество комбинации логина и пароля, причем разные для каждого сервиса для безопасности. Плюсом ко всему пароли должны быть сложные, состоять из символов верхнего и нижнего регистров, иметь цифры, специальные символы и достаточно длинные и должны меняться как минимум раз в полгода. Данные пароли крайне трудны для запоминания, и пользователь начинает использовать простые незамысловатые пароли или вовсе хранить в небезопасных местах, например, в текстовом документе на персональном компьютере.

Информационная безопасность подразумевает совокупность методов и средств обеспечивающие конфиденциальность, целостность и доступность определенной информации от незаконного ознакомления, модификации, уничтожений и преобразования, а также защита от воздействий, предполагающие нарушение работоспособности [1].

Информационная безопасность достигается обеспечением трех состоянии: доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры. [1]

Доступность - состояние информации, при котором субъекты, имеющие доступ к ней, могут реализовывать его без ограничения [1].

Целостность - состояние информации, при котором отсутствует любое изменение. Изменение допускается только субъектами, имеющие право на это.

Конфиденциальность подразумевает состояние информации, при котором доступ к ней могут осуществить только субъекты, которые имеют на это право. Для остальных субъектов информация обязана быть неизвестной [1].

Для защиты информации должны достигаться следующие цели [2]:

- предотвращение утечки, хищения, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действии по уничтожению, модификации, копированию, блокированию информации, предотвращение других форм незаконных действии в отношении информационных ресурсов и информационных систем, обеспечение правового режима как объекта собственности;
- защита конституционных прав граждан по сохранению личной тайны, конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Для рядового пользователя будет трудно запомнить связки логин пароль для аккаунта, для таких целей предусмотрено специализированное программное обеспечение для хранения таких данных называемые менеджеры паролей. Менеджеры паролей помогают создавать надежные уникальные пароли при регистрации на веб-сайтах и хранят их на своих серверах или локально на жестком диске. Чтобы зайти на ресурс или в приложение, можно скопировать нужный пароль из менеджера и вставить в соответствующее поле. Часто эти программы позволяют не только запоминать, но и автоматически вводить пароль на сайте. Данное программное обеспечение использует шифровальные средства для безопасности.

Менеджеры паролей делятся на следующие основные категории:

- Десктопные. Пароли к программному обеспечению хранятся на жестком диске компьютера.
- Портативные. Пароли хранятся на мобильных устройствах.
- Сетевые. Пароли сохраняются на веб-сайтах.

Менеджеры паролей, существующие на данный момент:

1. LastPass – менеджер паролей, имеющий возможность сохранять пароли как в облачном хранилище, так и в локальном. Способен изменять их автоматически, если сервис, для которого он предназначался, был взломан. Поддерживает двухфакторную аутентификацию для хранилища паролей с помощью Google Authenticator, USB-устройства или Yubikey. Можно делиться паролями с коллегами и близкими, выбирая, увидят ли они код или просто получат доступ к сервису на определённое время. LastPass сам авторизует пользователя на сайтах с сохранёнными паролями. Также способен генерировать безопасные пароли, хранить и автозаполнять формы для авторизации. Базовая версия – бесплатна, максимум функций – $12 в год.

Поддерживаемые платформы: Web, Android, iOS, macOS, Windows [3].

2. Dashlane. Менеджер паролей с двойной авторизацией, генератором паролей и системой предупреждения взлома аккаунтов, который позволяет удобно хранить пароли, так чтобы вы быстро могли посмотреть какой-то пароль от какого-то сайта. Присутствует также и платная версия. Приложение не требовательно к аппаратной и программной части, потребляет минимум ресурсов и никак не влияет на быстродействие системы и работу компьютера в целом.

Поддерживаемые платформы: Android, iOS, macOS, Windows [3].

3. 1Password. Предоставляет возможность хранить различные пароли, данные банковских карт, лицензии на программное обеспечение и другую конфиденциальную информацию в защищённом мастер-паролем виртуальном хранилище, заблокированном с использованием стандарта PBKDF2. Данные шифруются алгоритмом AES 256 GCM.

Поддерживаемые платформы: Android, iOS, macOS, Windows [3].

4. Sticky Password – менеджер паролей от разработчиков антивирусного программного обеспечения AVG. Умеет захватывать данные даже со старых форм и управлять паролями приложений. Поддерживает прямую синхронизацию по Wi-Fi. Не предоставляет доступ к паролям онлайн, что повышает уровень безопасности.

Поддерживаемые платформы: Android, iOS, macOS, Windows [3].

5. EnPass - это кроссплатформенное приложение для управления паролями, которое позволяет безопасно хранить пароли и другие учетные данные в виртуальном хранилище, заблокированном мастер-паролем. В отличие от большинства других популярных менеджеров паролей, Enpass является автономным менеджером паролей.

Поддерживаемые платформы: Android, iOS, macOS, Windows [3].

Шифровка данных является ключевым элементом для менеджера паролей.

Существуют два основных метода шифрования:

1. Симметричное шифрование.
2. Асимметричное шифрование.

Симметричное шифрование – один из способов шифрования, в котором для шифрования используется один ключ, ключ обязан сохранятся в тайне для осуществления мер по защите доступа.

Классическим примером алгоритмов являются симметричные криптографические алгоритмы, перечисленные ниже:

- Простая подстановка
- Одиночная перестановка по ключу
- Двойная перестановка
- Перестановка «Магический квадрат»

Ассиметричное шифрование – шифрование, использующее два ключа для шифровки и расшифровки: Публичный (Открытый) ключ и приватный (Закрытый) ключ. Эти ключи образуют так называемую ключевую пару и представляют собой большие числа, которые связаны некоторой зависимостью, но отличаются друг от друга.

Самым ярким примером данного типа шифрования является алгоритм RSA.

Самым популярным алгоритмом для шифрования таких данных, как пароль, является AES, также известный как Rijndael. Данный алгоритм является

симметричным и трудно расшифровываемым, так как для расшифровки требуется ключ. Ключ чаще всего в программе генерируется от пароля входа в программу или заданного слова пользователем, зависит от кода написанной программы и самого пользователя.

Для создания подобной программы требуется определить на каком языке она будет создаваться. В качестве выбранного языка выступает C#.

Программа состоит из сборок:

- PasswordManager.App – Главная сборка программы, состоящая из окон программы и исполняющего класса Program.cs.
- PasswordManager.Data – Сборка программы для изменения данных в базе данных. Состоит из классов:
  - PasswordOptionsData.cs – Позволяет изменить данные в таблице данных PasswordOptions предназначенный для изменения настроек генерации паролей.
  - PasswordsData.cs — многофункциональный класс, позволяющий изменять, добавлять или удалять информацию о паролях в базе данных.
  - SettingsData.cs – Класс для изменения настроек внутри программы. Данные настроек хранятся в таблице данных Settings.
  - UsersData.cs – Позволяет изменить данные для входа в программу.
- PasswordManagerDatabase – Сборка состоящая из одного класса DB.cs которая совершает операции с базами данных.
- PasswordManager.Entities – Сборка для определения переменных, состоящая из геттеров и сеттеров. В сборке 4 класса.
- PasswordManager.Filer состоящий из одного класса Filer.cs позволяющий собрать или прочитать данные для импорта и экспорта.
- PasswordManager.Globals – Сборка для настроек по умолчанию, их вариации, а также идентификации пользователя. Состоит из 5 классов:
  - DatabaseConnection.cs – Класс для соединения с базой данных.
  - Defaults.cs – Настройки по умолчанию.
  - Information.cs – Класс с информацией о программе.
  - Variables.cs – Класс для настройки отображения формата даты в программе.
  - Verifier.cs – Класс для проверки правильности ввода данных.
- PasswordManager.Gulipso – Основная сборка, состоящая из одного класса Gulipso.cs в которой определен метод шифрования (AES/Rijndael).
- PasswordManager.Services – Сборка с исполняющими классами. Состоит из 6 классов:
  - BearPassService.cs – Исполняющий файл импорта и экспорта.
  - CryptoService.cs – Исполняющий класс состоящий из функции для шифрования. Шифрование определено в Gulipso.
  - PasswordsService.cs – Позволяет получить доступ к паролям, в зависимости от пользователя, вошедшего в программу, также генерирует пароль в соответствии с установленными параметрами пользователем.
  - SettingsService.cs – Позволяет привязывать определенный набор настроек программы для конкретного пользователя.

  - UsersService.cs – Привязывает к аккаунту только те данные, которые пользователь добавил в базу данных. Просмотр этих данных с другого аккаунта недопустима.
  - ValidationService.cs – Обеспечивает проверку для различных объектов.
- PasswordManager.Theme – Сборка, состоящая из двух классов Colors.cs и Messenger.cs, позволяющая улучшать цветовую составляющую программы и определять текст по умолчанию выводимых сообщении в случае ошибки, предупреждения или информации.

Были реализованы окна программы такие как:

- Главное окно, позволяющее видеть всю информацию и имеющее функциональные кнопки.

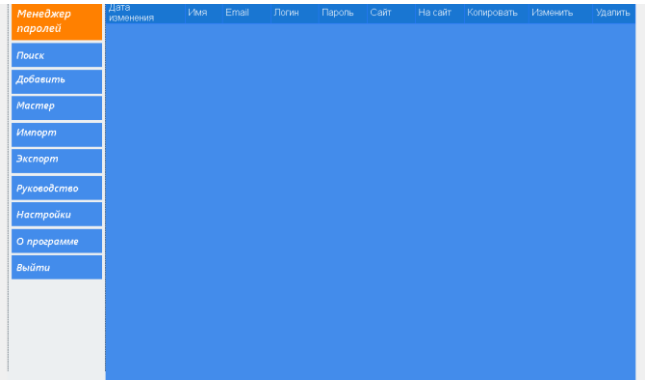

Рис 1. Главное окно программы

- Окно авторизации для входа в программу

Рис 2. Окно авторизации

- Окно добавления записи

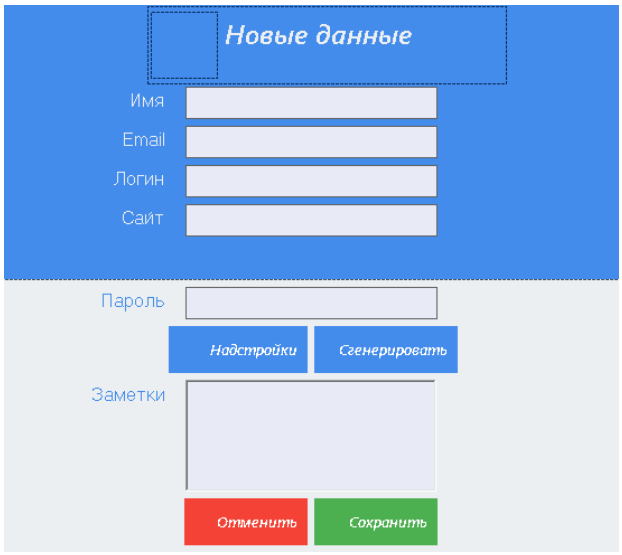

Рис 3. Окно для добавления новой записи

- Окно изменения мастера пароля

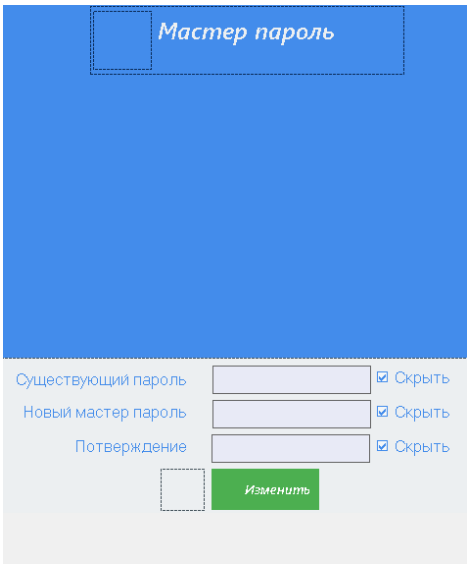

Рис 4. Окно для изменения мастера пароля

- Окно настроек программы

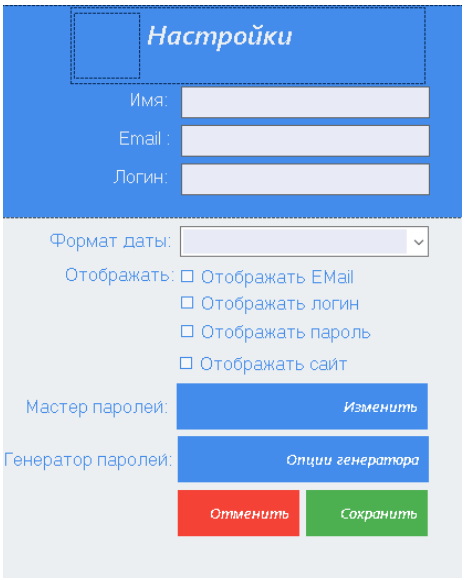

Рис 5. Окно параметров программы

- Окно «О программе»
- Окно «Руководство», в котором описаны рекомендованные действия для хранения и использования паролей.
- Окно редактирования данных, похожее на окно добавления записи

Также была создана база данных, которая содержит четыре таблицы. Таблица Users предназначена для хранения данных авторизованных пользователей программы, Passwords предназначена для хранения записи паролей, Settings для хранения настраиваемых параметров программы и PasswordOptions для хранения параметров генерации паролей.

Рис 6. Таблицы базы данных

Связка логин пароль используется практически на каждом сайте, будто форум, почта и т. д., для доступа. При регистрации это обязательные элементы для заполнения. Пароль в нашем времени является ценным ресурсом, благодаря нему можно получить доступ к важным данным. Конечно, можно придумать один сложный пароль на множество сайтов, где необходима авторизация, однако если этот пароль узнает мошенник, то у него будет полный доступ ко всем сайтам со всеми вашими данными. Хранение всех логинов и паролей в голове практически нереально, а хранить на бумажном носителе или в обычном

блокноте или документе на персональном компьютере – небезопасно. От этого вытекает вывод, что нужно найти альтернативу небезопасным местам для хранения паролей.

Таким образом, традиционные методы хранения паролей имеют серьезные недостатки, которые не позволяют их использовать в современных условиях. В настоящее время, когда безопасность и удобство работы в Интернет во многом определяет успех во всех делах (бизнесе, учебе, науке), очень важно иметь надежную систему хранения и учета паролей. Созданная программа позволит эффективно защитить и систематизировать пароли, а также обеспечит максимально комфортную работу в сети.

Литература

1. Шаньгин В. Ф. Информационная безопасность / В. Ф. Шаньгин – Москва: ДМК Пресс, 2017. – 702 с.
2. Защита информации – [Электронный ресурс]. URL: https://center-yf.ru/
3. Десять лучших менеджеров паролей по версии Lifehacker.com – [Электронный ресурс]. URL: https://lifehacker.ru/

INFORMATION SECURITY AND PASSWORD MANAGER

Sergey A. Zharkoy
student,
DorzhiBanzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: matem19961404@gmail.com

Tuyana S. Tsybikova
Cand. Sci. (Education), A/Prof.,
DorzhiBanzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: cts2001@mail.ru

The relevance of the problem is due to the increase in the number of attacks on components of distributed systems and the damage resulting from their implementation, as well as the variability and unpredictability of such attacks. At the moment in modern society, the Internet has become a center for the development of new technologies, fundamentally changing the methods of interaction with information. In the article the basic concepts of information security, types of encryption are studied and the development of the program "Password Manager" is briefly described.
Keywords. Manager, password, information, security, program, data, ciphering.