МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»
Кафедра дискретной математики и информационных технологий

БЕЗОПАСНОСТЬ ХРАНЕНИЯ ЛИЧНОЙ ИНФОРМАЦИИ В ИНТЕРНЕТЕ. РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ ХРАНЕНИЯ УЧЕТНЫХ ДАННЫХ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы
направления 09.03.01 — Информатика и вычислительная техника
факультета КНиИТ
Карташова Фёдора Сергеевича

Научный руководитель
доцент, к. ф.-м. н. _____ О. В. Мещерякова

Заведующий кафедрой
доцент, к. ф.-м. н. _____ Л. Б. Тяпаев

Саратов 2022

ВВЕДЕНИЕ

Век цифровых технологий дал огромное количество полезных сервисов человеку. Нашу жизнь уже невозможно представить без социальных сетей, электронной почты, мессенджеров, интернет-магазинов. С каждым годом количество таких сервисов и услуг становится только больше.

Каждый день человек заказывает одежду и продукты через такие сервисы Ozon, Самокат, Wildberries, Delivery club. Это стало возможным благодаря переходу к цифровым технологиям. За январь-февраль 2021 года рынок интернет-торговли в России вырос на 44% до 431.3 миллиардов рублей. Все больше граждан РФ оплачивают покупки банковскими картами. Информация о банковских картах и переводах переходит на хранения этим сервисам, а значит должна быть максимально защищена.

Помимо роста числа сервисов растет и количество данных, которые компании собирают и хранят о человеке. Центры хранения и обработки данных (в дальнейшем ЦОД) — специализированные здания для размещения серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет по всему миру становятся больше. Разработка переходит на облачные платформы — происходит отказ от развертывания серверов на базе ресурсов компании, производящей программное обеспечение и переход на аренду серверного оборудования в огромных ЦОД, принадлежащих таким гигантам в сфере информационных технологий как Google, Amazon, Microsoft.

Эксабайты данных, которые собирают эти компании, представляют огромную ценность и содержат в себе весьма чувствительную информацию. Такой информацией могут быть наши сообщения, место жительства, учетные данные, номер банковской карты.

Пользователям обещают безопасность хранения полученных данных. Государства вводят законы и нормы, регулирующие хранение и использование информации о пользователях.

Но всегда есть, была и будет третья сторона, которая найдет способ украсть, повредить, продать и использовать данные в недобросовестных целях.

Как много бы компании не тратили денег на защиту информации о пользователях, всегда будут существовать пути взлома, возможности физически украсть данные, либо же воспользоваться методами давления на людей.

Каждая новая информация о пользователе постепенно, как пазлы, собирается в единое целое, образуя уникальный цифровой след. На основе цифрового следа возможно создать психологический портрет. Можно понять использует ли человек правила безопасного формирования паролей. Если нет, то чаще всего в качестве пароля, человек использует какое-то конкретное слово в его основе, либо, что еще хуже, использует один и тот же пароль в множестве сервисов.

Такое поведение пользователей является ожидаемым, ведь устойчивый пароль является уникальным и не должен содержать в себе конкретного смысла. Такие пароли трудно запомнить даже специалисту в мнемонике.

Целью данной дипломной работы является создание приложения для удобного хранения и генерирования устойчивых паролей.

Для достижения данной цели требуется решить следующие задачи:

- систематизировать знания о способах хранения информации о пользователях, знания известных утечек баз данных популярных сервисов;
- сравнить существующие решения в области менеджеров паролей на рынке;
- на основе сравнения выбрать основные функции, особенности и вектор развития менеджера паролей;
- разработать архитектуру приложения, выбрать способ хранения данных и алгоритм шифрования
- создать приложение, выполняющее функции, хранения учетных данных и создания устойчивых паролей.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе «Информация и цифровой след» рассмотрены основные понятия информационной безопасности, а именно: информация, ее свойства и цифовой след.

Федеральный закон №149 ФЗ от 27.07.2006 "Об информации, информационный технологиях и о защите информации" дает следующее определение: "Информация — это сведения (сообщения, данные), независимо от формы их представления" .

Информация как объект в современном мире и как предмет жизнедеятельности и жизнеобеспечения имеет свои специфические особенности. К ним можно отнести:

- Информация в форме сведений всегда связана с физическим лицом, а в форме сообщений и данных — с материальным носителем, на котором она фиксируется, хранится и переносится.
- Информация может быть товаром и объектом рыночных отношений. Право собственности закреплено гражданским законодательством, включает имущественные права. Для реализации права необходимо документирование информации — фиксация на материальном носителе.
- Информация как предмет жизнедеятельности и жизнеобеспечения имеет ценность и важность, которые могут меняться во времени, и приносить доход или другие материальные и нематериальные блага её обладателям. Для сохранения ценности информации необходимо поддерживать её потребительские свойства.

Среди этих потребительских свойств, содержаться свойства безопасности информации, основными из которых являются: конфиденциальность, целостность, доступность. При нарушении хотя бы одного из этих свойств ценность информации снижается либо теряется вообще.

Цифровой след или цифровая тень — это данные, которые пользователь оставляет при использовании интернета [1]. Эти данные включают отправленные электронные письма, сообщения в социальных сетях, посещаемые вебсайты, данные, указанные в онлайн-формах. Пользователи интернета активно и пассивно создают собственный цифровой след. Также по цифровой тени можно отследить действия человека и его устройств в интернете.

Увеличению цифрового следа способствуют оставленные отзывы и покупки в интернете, подписки на информационные рассылки, публикации в социальных сетях.

Цифровой след важен по следующим причинам:

- Носит относительно постоянный характер. Как только информация становятся общедоступной, например, публикация в Вконтакте, пользователь, опубликовавший ее, практически не может контролировать, как она будет использоваться другими людьми.
- Цифровой след может отражать цифровую репутацию человека, которая теперь считается такой же важной, как и репутация за пределами сети.
- Прежде чем принимать решения о найме, работодатели могут проверять цифровые следы своих потенциальных сотрудников, особенно их социальные сети. Колледжи и университеты могут проверять цифровые следы своих будущих студентов перед зачислением на учебу.
- Публикуемые в интернете сообщения и фотографии могут быть неверно истолкованы или изменены.
- Контент, предназначенный для узкой группы, может распространиться на более широкий круг.
- Киберпреступники могут использовать цифровой след в целях фишинга,для доступа к учетной записи или для создания ложных профилей наоснове ваших данных.

Во второй главе «Способы хранения информации о пользователях, утечки данных и их причины» рассмотрены причины перехода к облачным технологиям для хранения данных пользователей и приведены примеры утечек данных в популярных сервисах.

Облачные технологии представляют собой обработку информации, выполнение вычислений, хранение данных на веб-ресурсах, имеющих свои мощности и предоставляемые абонентам Интернета в качестве сервиса.

Облачные технологии имеют следующие достоинства:

- низкая стоимость — снижение расходов на обслуживания виртуальной инфраструктуры, оплата лишь фактического использования ресурсов;
- доступность — облака доступны всем и везде, где есть Интернет, и с любого устройства, где есть браузер;
- гибкость — неограниченность вычислительных ресурсов (память, процес-

сор, диски), виртуализация;

- надежность — специально оборудованные ЦОД имеют дополнительные источники питания, охрану, профессиональных работников, регулярное резервирование данных, высокую пропускную способность интернет-канала, высокая устойчивость к DDoS атакам;
- безопасность — облачные сервисы имеют достаточно высокую безопасность при должном соблюдении правил безопасности на объекте ЦОД;
- большие вычислительные мощности — можно использовать все ее вычислительные способности, заплатив только за фактическое время использования.

Но какими бы привлекательными достоинствами облачные технологии ни обладают, существует ряд недостатков этой платформы:

- постоянное соединение с сетью — для получения доступа к услугам "облака" необходимо постоянное соединение с сетью Интернет;
- программное обеспечение — есть ограничения по ПО, которое можно разворачивать на облаках и предоставлять его пользователю;
- конфиденциальность — в настоящее время нет технологии, которая бы гарантировала 100% конфиденциальность хранимых данных;
- безопасность — облако само по себе является достаточно надежной системой, однако при проникновении на него злоумышленник получает доступ к огромному хранилищу данных;
- дороговизна оборудования — для построения собственного облака необходимо выделить значительные материальные ресурсы.

В качестве примеров утечек данных приведены случаи связаные с сетью магазинов "Красное и Белое" , налоговой службой Росси, банком ВТБ и американской страховой компанией First American Financial Corporation. А также приведены результаты исследования института Ponemon об основных причинах таких утечек.

В третьей главе «Стойкость паролей и рынок ПО для хранения учетных данных» приведены результаты анализа от сервиса разведки утечек данных и мониторинга даркнета DLBI об утекших паролях в российском сегменте интернета [2]. Кроме этого анализа были приведены рекомендации к созданию устойчивых к взлому паролей от компании Sophos. Также в этой главе был проведен сравнительный анализ пяти популярных решений на рынке менеджеров паролей, а именно: 1Password, LastPass, RememBear, Passbolt и KeePass.

В четвертой главе «Разработка менеджера паролей» были описаны основные этапы разработки и полученный программный продукт. Первым этапом разработки стал выбор основых функций приложения, а именно:

- простой интерфейс;
- кроссплатформенность;
- сохранность паролей в зашифрованном локальном хранилище;
- возможность мастер-пароля дать доступ ко всем учетным данным;
- возможность очищения хранилища в случае компрометации устройства;
- использование известных стандартов шифрования.

На следущем этапе разработки были выбраны технологии хранения данных, а именно SQLChipher [3], реализация кроссплатформенных библиотек для взаимодействия с базой данных, классов генерации и шифрования паролей [4,5].

Заключительным этапом разработки стала реализация пользовательского интерфейса при помощи технологии Xamarin.Forms. В результате были созданы следющие страницы:

- страница регистрации и авторизации;
- страница со списком сервисов, в которых зарегистрирован пользователь;
- страница со списком учетных записей пользователя для каждого сервиса.

ЗАКЛЮЧЕНИЕ

Данная работа ставила своей целью разработку приложения для безопасного хранения учетных данных пользователей. Для этого был проведен анализ рынка существующих менеджеров паролей, была выбрана технология хранения данных, найден подходящий алгоритм шифрования, разработан генератор устойчивых паролей и реализован пользовательский интерфейс приложения.

В современных реалиях сложно доверить хранение такой чувствительной информации, как учетные данные, третьим лицам. Рассмотренные в работе случаи утечки данных заставляют задуматься о взятии ответственности за хранение личных данных на себя. Таким образом, развитие отечественных решений в области менеджеров паролей является важной задачей. Разработанное приложение основано на популярных открытых технологиях с использованием современных методов шифрования данных, доступно для ОС Windows. Также, за счет разработанной общей портативной библиотеки, при должных знаниях особенностей ОС Android и iOS, приложение может быть легко перенесено на эти системы.

ОСНОВНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

1 Kaspersky.ru [Электронный ресурс]. — URL: https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint (Дата обращения 4.05.2022). Загл. с экрана Яз. рус.

2 DLBI [Электронный ресурс]. — URL: https://dlbi.ru/five-billion-password-2021/ (Дата обращения 4.05.2022). Загл. с экрана Яз. рус.

3 *Kreibich, J.* Using SQLite / J. Kreibich. — Sebastopol, California, U.S.A: O'Reilly Media, 2010. — 528 с.

4 *Thorsteinson, P.* .NET Security and Cryptography / P. Thorsteinson, G. A. Ganesh. — Hoboken, New Jersey, U.S.A: Prentice Hall Professional, 2020. — 466 с.

5 Habr: Как устроен AES[Электронный ресурс]. — URL: https://habr.com/ru/post/112733/ (Дата обращения 4.05.2022). Загл. с экрана Яз. рус.