Это приводит к увеличению лояльности, привлечению новых клиентов и, в конечном счете, росту прибыли. Более того, Big Data может помочь оптимизировать внутренние процессы, выявить узкие места и повысить эффективность работы.

Однако, внедрение инструментов Big Data для МСБ сопряжено с рядом трудностей. Главная из них – высокая стоимость. Приобретение необходимого оборудования, программного обеспечения и наем квалифицированных специалистов могут оказаться неподъемными для малого бизнеса. Кроме того, для эффективного использования Big Data необходимо уметь грамотно собирать, обрабатывать и интерпретировать данные, что требует определенных знаний и навыков.

Не стоит забывать и о вопросах конфиденциальности. Сбор и хранение больших объемов данных о клиентах требует соблюдения строгих правил безопасности и защиты персональной информации. Нарушение этих правил может привести к серьезным юридическим последствиям и потере репутации. Таким образом, перед внедрением Big Data необходимо тщательно взвесить все «за» и «против» и убедиться, что компания готова к решению возникающих проблем.

Использование анализа данных становится все более доступным для малого и среднего бизнеса благодаря развитию технологий и снижению стоимости инструментов. Применение Big Data позволяет компаниям лучше понимать своих клиентов, повышать эффективность операций и оставаться конкурентоспособными на рынке. В условиях растущей цифровизации экономики этот подход становится ключевым фактором успеха для любого бизнеса, независимо от его размера.

Список использованных источников:

1. Что такое Big Data? Простыми словами о сложном. – URL: https://bluescreen.kz/chto-takoie-big-data-prostymi-slovami-o-slozhnom/ (дата обращения: 04.03.2025). – Текст: электронный.

2. Big Data. – URL: https://okocrm.com/glossary/big-data/?ysclid=m6yqxmaeg6180073301 (дата обращения: 04.03.2024). – Текст: электронный.

3. Исследование MarketsandMarkets. – URL: https://www.marketsandmarkets.com/Market-Reports/big-data-market-1068.html (дата обращения: 04.03.2025). – Текст: электронный.

4. Объем данных в мире: Прогноз IDC. – URL: https://www.idc.com/getdoc.jsp?containerId=prUS46881420 (дата обращения: 04.03.2025). – Текст: электронный.

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ РАБОТЫ С ХЕШЕМ ФАЙЛОВ, ИХ СИММЕТРИЧНОГО И АСИММЕТРИЧНОГО ШИФРОВАНИЯ НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ PYTHON

А.И. Галицкий[a], студент гр. 17В21,
Научный руководитель: Разумников С.В., к.т.н., доц.
Юргинский технологический институт (филиал)
Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail: [a]tosha-1-9@mail.ru.

Аннотация: В работе представлен процесс разработки программы для работы с хешем файлов, их симметричного и асимметричного шифрования на языке программирования Python. Подробно описаны этапы создания данного ПО. В результате разработки получена и апробирована программа, имеющая инструментарий для работы с хешем файлов, а также их шифрования (симметричного и асимметричного). Были рассмотрены и нивелированы проблемы аналогичных программных продуктов, и введены новые функции. Определены области применения разработанного ПО и намечены векторы дальнейших улучшений. Описаны возможности дальнейшей технической поддержки.

Ключевые слова: Программа, Python, программирование, криптография, хеш, симметричное шифрование, асимметричное шифрование.

Abstract: The paper presents the process of developing a program for working with a hash of files, their symmetric and asymmetric encryption in the Python programming language. The steps of creating this program are described in detail. As a result of the development, a program has been obtained and tested that has tools for working with file hashes, as well as their encryption (symmetric and asymmetric). The problems of similar software products were reviewed and eliminated, and new functions were introduced.

The areas of application of the developed software have been identified and the vectors of further improvements have been outlined. The possibilities of further technical support are described.

Keywords: Program, Python, programming, cryptography, hash, symmetric encryption, asymmetric encryption.

Введение.

На сегодняшний день невозможно представить любую сферу жизни человека без хотя бы частичной информатизации и автоматизации. Производными данных особенностей современного общества являются файлы. Бывают они самыми разными: от видеозаписей и фотографий до специализированных под какие-либо процессы и операции. Количество файлов уже во много миллиардов раз превышает численность населения Земли, но от этого ценность каждого отдельно взятого файла лишь увеличивается. Защитить такой важный и драгоценный ресурс способны алгоритмы хеширования и шифрования. Хеширование представляет собой процесс преобразования информации в уникальную последовательность символов фиксированной длины. Шифрование является инструментом для сохранения конфиденциальности и целостности файлов, посредством преобразования данных таким образом, чтобы их смогли использовать только круг доверенных лиц или те, кому предоставлен подобного рода доступ.

Разработка программы

Хеширование и шифрование являются защитниками информации от изменения злоумышленниками и гарантами того, что вы работаете именно с тем, что вам необходимо, а не навязано. Согласно работе Мебонии М. А. и Федоровой О. В. [1], хеширование позволяет однозначно определить соответствует ли предоставленный файл исходному объекту и избежать работы с поддельными данными. Читая же труд Карпова М. А. и Лимановой Н. И. [2] можно ещё раз убедиться, что именно шифрование позволяет исключить вмешательство в передаваемую или хранимую информацию третьих лиц и сохранить её первозданный вид и наполнение. Было бы актуально и полезно для пользователей со всего мира иметь цифровой продукт, предоставляющий возможность осуществления операций, названных ранее, в удобной форме.

На момент написания данной работы уже существует огромное количество готовых решений, позволяющих осуществлять хеширование и шифрование файлов на достаточно высоком уровне. Но среди них лишь малое количество (по сравнению с их общим числом) способны предоставлять возможность осуществления этих процессов в рамках одного программного продукта. Единицы же могут предложить пользователю простой, интуитивно понятный интерфейс. Именно эти особенности являются их главными недостатками. Их решение, как и создание функционала, описанного выше, будет представлено далее.

Для того, чтобы выполнить целостную разработку ПО была изучена научная литература, необходимая для понимания концепций применения хеширования и шифрования для защиты данных [3]. Чтобы сформировать простой, удобный интерфейс программы и исправить описанные ранее недостатки была изучена соответствующая техническая документация [4].

В результате выполнения работы должно быть получено программное обеспечение, предоставляющее пользователю возможность хеширования и шифрования файлов с необходимыми ему параметрами в одной программе.

При разработке программы использовались стандартные методы Python, а также подключаемые библиотеки, такие как Hashlib, Cryptography и Tkinter. Код был написан в удобном формате, где для каждого окна и его функционала был отведён отдельный класс, в котором каждый ключевой элемент и действие были описаны соответствующими функциями. Это решение позволило не только упростить разработку ПО, но и сделать её удобнее. Также, посредством глубокого анализа собственного кода и алгоритмов аналогов удалось решить проблемы, приведённые выше.

Результатом разработки является программа, осуществляющая работу с хешем файлов, а также их шифрование и дешифрование. Интерфейс выполнен просто и лаконично, не имеет лишних элементов. Навигация по программе осуществляется посредством кнопок меню. При выполнении каждой из операций пользователь имеет возможность, не только выбрать файл для работы, но и задать необходимые параметры (для хеширования – алгоритм, для шифрования и дешифрования – ключи).

Апробация программы осуществлялась в 3 доступных режимах: «Работа с хешем» (рис. 1), «Симметричное шифрование» (рис. 2) и «Асимметричное шифрование» (рис. 3). По её результатам можно сделать вывод о том, что разработка была выполнена успешна.

Данная программа может быть применена при защите своих данных от злоумышленников – достаточно просто зашифровать ту информацию, которую вы бы хотели оставить приватной.

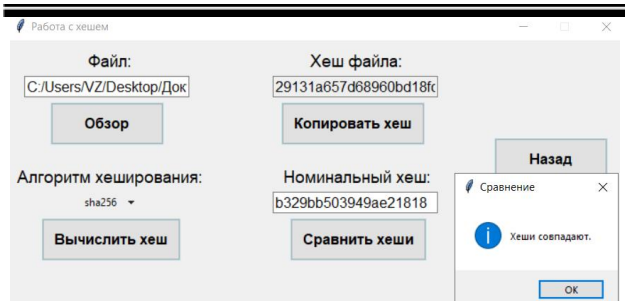

Рис. 1 Работа с хешем

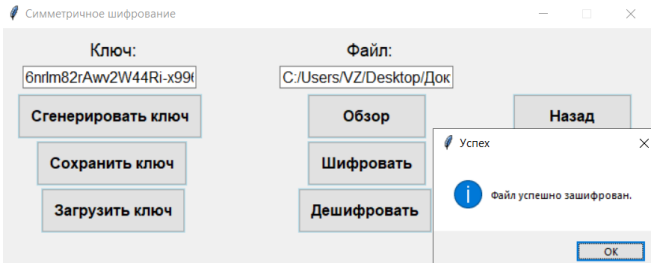

Рис. 2. Симметричное шифрование

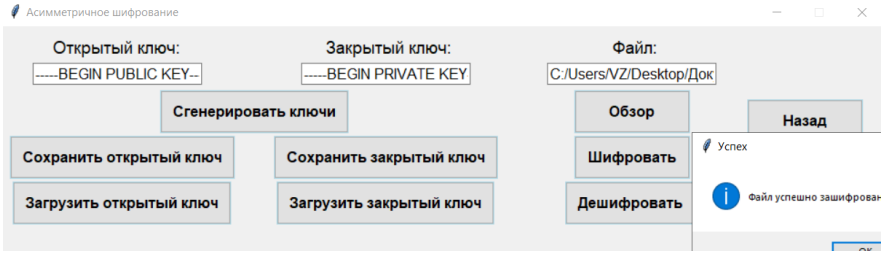

Рис. 3. Асимметричное шифрование

Также имеется возможность интеграции данного ПО в общение между пользователями – можно проверять целостность принятых файлов и осуществлять шифрование и дешифрование принимаемых и отправляемых данных для обеспечения конфиденциальности.

Поддержка данного программного обеспечения возможна во множестве направлений. Одним из таких векторов является добавление новых алгоритмов хеширования и шифрования. Также возможным результатом сопровождения данной программы будет являться добавление возможности шифрования целых папок или дисков. Это будет полезно, если пользователь будет осуществлять работу с большим объёмом файлов.

Заключение

В результате работы была разработана программа для работы с хешем файлов, их симметричного и асимметричного шифрования на языке программирования Python. Были решены проблемы аналогов. Благодаря проведённой апробации были доказаны работоспособность и эффективность разрабатываемого ПО. Также были описаны сферы применения программы и векторы будущих доработок и улучшений.

Список использованных источников:

1. Мебония М.А. Сравнительное исследование хэш-алгоритмов в криптографии / М.А. Мебония, О.В. Федорова // Вестник науки. – 2022. – №12 (57). – URL: https://cyberleninka.ru/article/n/sravnitelnoe-issledovanie-hesh-algoritmov-v-kriptografii (дата обращения: 26.02.2025).
2. Карпов М.А. Вопросы практического применения криптографии для обеспечения безопасности данных / М.А. Карпов, Н.И. Лиманова // Бюллетень науки и практики. – 2023. № 12. – URL: https://cyberleninka.ru/article/n/voprosy-prakticheskogo-primeneniya-kriptografii-dlya-obespecheniya-bezopasnosti-dannyh (дата обращения: 26.02.2025).
3. Пчелинцева Н.В. К вопросу применения криптографии / Н.В. Пчелинцева, И.В. Чепраков, А.А. Гущина // Наука и образование. – 2022. – № 2. – URL: https://cyberleninka.ru/article/n/k-voprosu-primeneniya-kriptografii (дата обращения: 26.02.2025).
4. Графические пользовательские интерфейсы с Tk. Документация Python. – URL: https://translated.turbopages.org/proxy_u/en-ru.ru.7c386e1d-658303e9-ea657aab-74722d776562/https/docs.python.org/3/library/tkinter.html (дата обращения: 26.02.2025).