Автор:
Ігнатов Микита Сергійович
студент 42ІПЗ групи
Науковий керівник:
кандидат фізико-математичних наук,
доктор педагогічних наук, доцент кафедри
комп'ютерної та програмної інженерії
Малежик Петро Михайлович

ДЕСКТОПНИЙ ДОДАТОК ДЛЯ СИМЕТРИЧНОГО ШИФРУВАННЯ ДАНИХ

Анотація: Щороку зростає кількість правопорушень пов'язаних з порушенням конфіденційності даних. Причиною таких випадків є поширення інформатизації на нові сфери діяльності та, як наслідок, збільшення кількості користувачів інформаційних систем. Проте, незважаючи на розвиток сфери захисту цих систем слабкою ланкою залишається їх користувач. Якщо для співробітників компаній проводяться спеціалізовані тренінги по інформаційній безпеці, то звичайні користувачі менш захищені в цих питаннях. Саме тому важливим є популяризація засобів захисту від подібного роду загроз. Таким елементом захисту може бути використання додатків для шифрування даних [1].

Ключові слова: інформаційна безпека, шифрування, розшифрування, ключ.

Вступ. Інформаційна безпека - захищеність інформації від навмисних або випадкових дій, що призводять до нанесення шкоди користувачам. Зазвичай це передбачає запобігання або зменшення ймовірності несанкціонованого/неналежного доступу до даних або незаконного використання, розкриття, порушення, видалення, пошкодження, модифікацію, перевірку, запис або знецінення інформації [1]. Інформаційна безпека також передбачає дії, спрямовані на зменшення негативного впливу вище перерахованих інцидентів. Саме прийняття запобіжних заходів щодо забезпечення конфіденційності, цілісності, а також доступності інформації і є найбільш правильним підходом у створенні системи інформаційної безпеки [2].

Мета роботи полягає в наступному: створити десктопний додаток для симетричного шифрування даних.

Виклад основного матеріалу. Для того щоб надати користувачу можливість вільно користуватися функціями додатка без знань в області криптографії було виділено перелік основних можливостей.

Десктопний додаток для шифрування та розшифрування має включати в себе такі функціональні можливості:

1. Меню, яке дозволяє вибрати режим роботи програми – шифрування чи розшифрування.
2. Меню шифрування, яке дозволяє:
   - ✓ Вибрати ім'я вхідного файлу (шлях до файлу, являє собою рядок символів, який може містити символи латиниці та кирилиці і цифри, обов'язково необхідно вказати розширення файлу) – це обов'язковий параметр.
   - ✓ Вибрати ім'я вихідного файлу (шлях до файлу, являє собою рядок символів, який може містити символи латиниці та кирилиці і цифри, обов'язково необхідно вказати розширення файлу) – це необов'язковий параметр.
   - ✓ Вибрати ключ, використовуючи який буде проводитись шифрування (шлях до файлу, являє собою рядок символів, який може містити символи латиниці та кирилиці і цифри, обов'язково необхідно вказати розширення файлу) – це необов'язковий параметр.
   - ✓ Видалити файл після шифрування
   - ✓ Почати процес шифрування.
   - ✓ Повернутися до головного меню.

3. Меню розшифрування, яке дозволяє:
   - ✓ Вибрати ім'я вхідного файлу (шлях до файлу, являє собою рядок символів, який може містити символи латиниці та кирилиці і цифри, обов'язково необхідно вказати розширення файлу) – це обов'язковий параметр.
   - ✓ Вибрати ім'я вихідного файлу (шлях до файлу, являє собою рядок символів, який може містити символи латиниці та кирилиці і цифри, обов'язково необхідно вказати розширення файлу) – це необов'язковий параметр.
   - ✓ Вибрати ключ, використовуючи який буде проводитись розшифровування (шлях до файлу, являє собою рядок символів, який може містити символи латиниці та кирилиці і цифри, обов'язково необхідно вказати розширення файлу) – це необов'язковий параметр.
   - ✓ Видалити файл після розшифрування
   - ✓ Почати процес розшифрування.
   - ✓ Повернутися до головного меню.

Після завершення роботи з файлом має бути можливість ввести новий файл, змінити режим роботи програми (шифрування/розшифрування) або завершити роботу програми.

До цільової аудиторії можна віднести будь-якого користувача комп'ютера, який хоче забезпечити конфіденційність своїх даних.

Відмінність даного додатку від інших це мінімалістичний дизайн, швидкість роботи, можливість шифрувати будь-які дані та використання власного симетричного алгоритму шифрування.

Висновок. У сучасному інформаційному просторі виникає велика потреба в забезпеченні інформаційної безпеки користувача, шляхом усунення наслідків від тих атак, що вже відбулися та попередження можливих потенційних атак. Для попередження слід використовувати низку рівнів захисту, серед яких: організаційні заходи, програмно-технічні заходи та просвітницька діяльність серед користувачів. Для підвищення захищеності може бути корисним, розробка та провадження нових засобів шифрування даних, що сприятиме підвищенню як програмо-технічного боку, так і буде популяризувати засоби шифрування серед користувачів.

Список використаних джерел

1. Інформаційна безпека людини як споживача телекомунікаційних послуг: Монографія / І. В. Арістова, Д. В. Сулацький ; НДІ інформатики і права НАПрН України. — К. : Право України ; Х. : Право, 2013. — 184 с.
2. Дмитрий Ганжело о хакерах, защите гаджетов и кибербезопасности в Украине. URL: https://web.archive.org/web/20191018180031/https://indevlab.com/ru/blog-ru/dmitrij-ganzhelo-o-hakerah-zashhite-gadzhetov-i-kiberbezopasnosti-v-ukraine/. (дата звернення: 20.04.2022)
3. Мао В. Современная криптография: Теория и практика / пер. Д. А. Клюшина — М.: Вильямс, 2005. — 768 с. — ISBN 978-5-8459-0847-6
4. Symmetric vs Asymmetric Encryption – Which is More Secure? URL: https://www.cheapsslshop.com/blog/symmetric-vs-asymmetric-encryption-whats-the-difference. (дата звернення: 17.04.2022)
5. Шнайер Б. Глава 16. Генераторы псевдослучайных последовательностей и потоковые шифры // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
6. eSTREAM: быстрые и стойкие поточные шифры. URL: https://lib.itsec.ru/articles2/Oborandteh/estream_bystrye_i_st. (дата звернення: 18.04.2022)