[6] Купревич Т. С. Международные грузоперевозки в условиях цифровой экономики: факторы и направления развития. автореф. дис. ... канд. екон. наук: 08.00.14. Минск, 2020. 23 с.

[7] Волков Д. В. Впровадження digital-технологій на транспорті. *«Digitalization of the economy as a factor of sustainable development» Materials of International scientific-practical conference,* (Mariupol, May 25-26, 2021). Маріуполь, 2021. С. 137-139.

УДК 004.415+004.42+004.056.5

ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ ПРОГРАМИ-ТРЕНАЖЕРА ДЛЯ ВИВЧЕННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Сєркін Р. О., Шапошнікова О.П., Мнушка О.В.

Харківський національний автомобільно-дорожній університет

Захист інформації відноситься до актуальних задач сьогодення внаслідок надзвичайно широкого розповсюдження систем обробки інформації, розширення локальних та глобальних комп’ютерних мереж, якими передаються величезні об’єми інформації державного, військового, комерційного та приватного характеру, а також поступового втілення ідей «цифрової держави», коли всі послуги держава має надавати онлайн. Використання комп’ютерів і автоматизованих технологій обробки інформації спричиняє появу низки проблем, пов’язаних із проблемами захисту даних, зумовлених наданням доступу більшому колу користувачів до конфіденційних чи персональних даних. Збільшується кількість комп’ютерних злочинів, що врешті решт може призвести до економічних втрат. Поширення технологій Інтернету речей також тісно пов’язане із питаннями безпеки даних [1].

Метою роботи є аналіз основних проблем, пов'язаних із обробкою та захистом інформації, а також розробка програмного забезпечення – тренажеру для вивчення криптографічних алгоритмів.

Навчаючі програми до яких відноситься і наша програма-тренажер мають ряд особливостей, що були розглянуті у [2, 3], серед основних – урахування вікових обмежень та особливостей сприйняття інформації.

Аналіз показує, що до переліку основних загроз для цілісності та конфіденційності інформації слід віднести:

– перехоплення інформації – цілісність інформації зберігається, але її конфіденційність порушена;

– модифікацію інформації – вихідне повідомлення змінюється або повністю підміняється іншим і відсилається адресату;

– підміна авторства інформації, що призводить до репутаційних та матеріальних втрат.

Захист інформації здійснюють за рахунок організаційних заходів, програмних, апаратних, програмно-апаратних заходів із використанням криптографічних алгоритмів.

Метою розробки програми-тренажера є створення допоміжного інструменту для викладачів, студентів та будь-кого, хто цікавиться історією розвитку криптографічного захисту даних та має на меті вивчити поширені методи шифрування.

Симетричне шифрування (шифрування із закритим ключем) використовує один і той же ключ, який обидві сторони інформаційного обміну зберігають в секреті від противника. Всі відомі з історії шифри, наприклад, шифр Цезаря - це шифри з закритим ключем. Асиметричне шифрування (шифрування із відкритим ключем) використовує два типи ключів – відкритий та закритий. Відкритий ключ може передаватися незахищеними каналами зв'язку.

Як правило, симетричні алгоритми шифрування вимагають менше обчислень, ніж асиметричні, тобто якісні асиметричні алгоритми повільніші

та вимогливіші до апаратних ресурсів. Недоліком симетричних алгоритмів є необхідність мати секретний ключ з обох боків передачі інформації. Для компенсації недоліків симетричного шифрування в даний час широко застосовується комбінована (гібридна) криптографічна схема, де за допомогою асиметричного шифрування передається сеансовий ключ, що використовується сторонами для обміну даними за допомогою симетричного шифрування.

Визначимо функціональні вимоги до програмного забезпечення виконавши вертикальне трасування. Функціональні вимоги визначають набір корисних функцій ПЗ, що складають цінність продукту. Під час реалізації програми використано принципи організації робочого процесу на основі Agile [4].

Розглянемо приклад реалізації функціоналу тренування. Для тренування доступно 4 шифри: шифр Цезаря, шифр Віженера, Атбаш та Скитала. Візуально форми для тренування шифрів схожі між собою. На формі знаходиться поле в яке потрібно ввести текст. Також є поле куди потрібно ввести ключ. При натисканні на кнопку «Закодувати» відбувається кодування тексту, введеного в текстове поли, використовуючи введений ключ. При натисканні на кнопку «Розкодувати» відбувається подія відбувається розкодування тексту, введеного в текстове поли, використовуючи введений ключ. Текст можна завантажити з текстового файлу. Для цього потрібно натиснути кнопку «Завантажити текст з файлу» та обрати текстовий файл. Текст, який знаходиться в текстовому полі можна зберегти натиснувши кнопку «Зберегти текст у файл» та ввести в діалоговому вікні назву файлу.

Кожен шифр використовує в якості словника – український алфавіт, тому текст для кодування та декодування повинен бути українською мовою. Всі інші символи будуть пропускатися.

Головне вікно додатку (рис. 1) забезпечує доступ до всіх функцій програми.

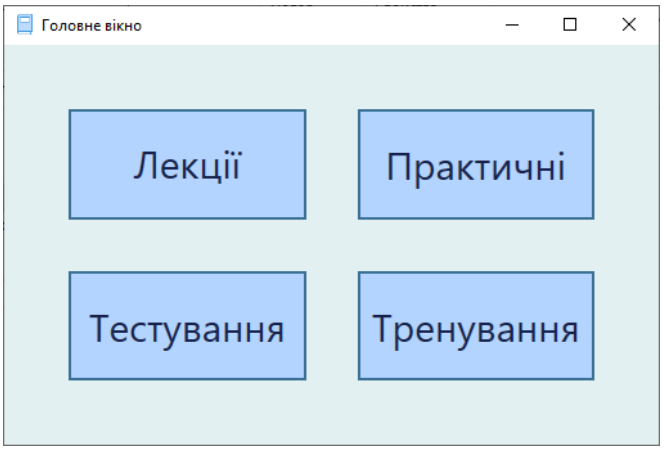
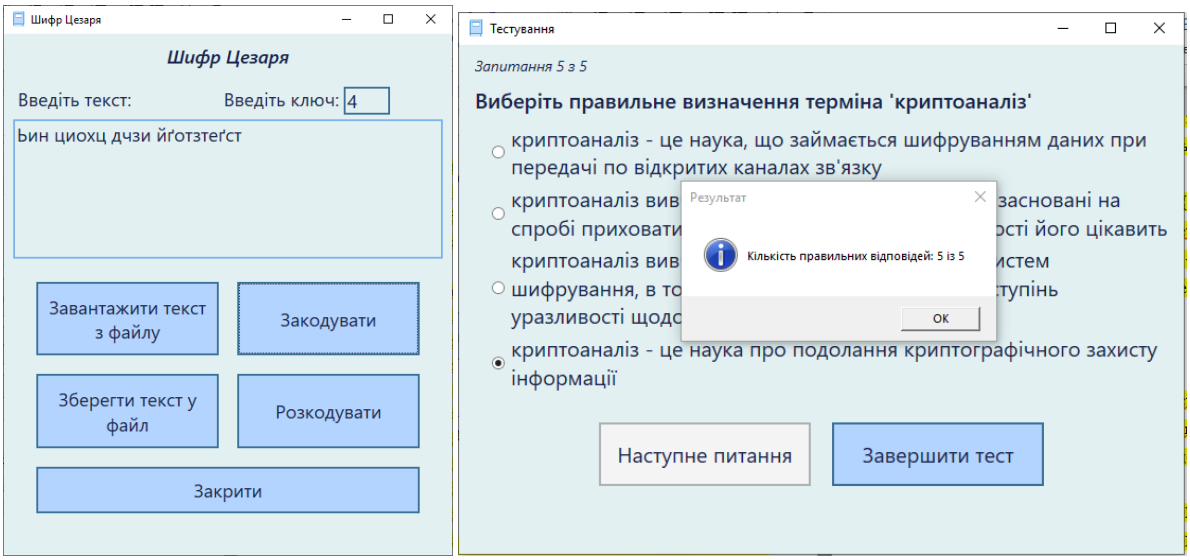


Рисунок 1 – Головне вікно додатку

При натисканні на кнопку «Тренування» відкривається вікно з доступними шифрами для тренування. При натисканні на будь-яку кнопку відкривається вікно, в якому можна наочно попрацювати з обраним шифром (рис. 2 а). Також реалізовано функціонал тестування знань (рис.2 б), що дозволяє оцінити студенту або викладачу рівень засвоєння навчального матеріалу. Гнучкість тестування забезпечується використанням JSON-файлів для завантаження тестів та вивантаження результатів.



а) б)

Рисунок 2 – Форми для тренування та тестування

Проаналізовано потреби у створенні навчальних додатків-тренажерів для вивчення алгоритмів шифрування. Визначено функціональні вимоги до програмного забезпечення та створено архітектуру додатку. Додаток

реалізовано у вигляді додатку Windows із використанням технологій .Net. та мови програмування C#, підхід реалізації криптографічних алгоритмів представлено у [5]. Результати розробки використовуються у курсі «Технології захисту інформації» для студентів спеціальності 121 «Інженерія програмного забезпечення».

Перспективами подальшого дослідження є удосконалення модулів оцінювання знань та формування індивідуальних траєкторій навчання студентів.

Література:

[1] O. Mnushka and V. Savchenko, "Security Model of IOT-based Systems," 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2020, pp. 398-401, doi: 10.1109/TCSET49122.2020.235462.

[2] Б.О. Котенко, О.В. Мнушка, «Об’єктно-орієнтований підхід до дизайну навчаючих програм», Комп’ютерні технології і мехатроніка. Збірник наукових праць за матеріалами міжнародної науково-практичної конференції, Харків, ХНАДУ, 2019, С.125-127.

[3] О.В. Мнушка, Б.О. Котенко, В.М. Савченко, «Аналіз вимог та розробка прототипу навчаючого програмного забезпечення для мобільних платформ», Вісник Харківського національного автомобільно-дорожнього університету : зб. наук. пр., вип. 92, т. 1, Харків, 2021, С. 51-59.

[4] О.П. Шапошнікова, В.В. Кірвас «Застосування методології Agile в практиці проектного навчання при підготовці IT спеціалістів, » Системи обробки інформації. 2020. № 4(163). С. 94-100. https://doi.org/10.30748/soi.2020.163.10.

[5] Р.О. Сєркін, О.В. Мнушка, «Реалізація криптографічних алгоритмів та протоколів мовою програмування C#,» Комп’ютерні технології і мехатроніка : зб. наук. пр. за матеріалами II міжнар. наук.-практ. конф. – Харків : ХНАДУ, 2020. – С. 92–95.