***Быценко Алексей***,
Студент Инжинирингового колледжа
НИУ «БелГУ» Россия, г. Белгород
***Bytsenko Alexey,***
College of Engineering student
NRU "BelGU" Russia, Belgorod
***Гончаров Дмитрий Викторович***,
Ассистент кафедры информационных робототехнических систем
НИУ « БелГУ» Россия, Белгород
***Goncharov Dmitry Viktorovich,***
Assistant Department Information Robotic Systems
NRU BelGU" Russia, Belgorod
***Подпругин Александр Ильич***,
Преподаватель СПО Инжинирингового колледжа
НИУ «БелГУ» Россия, Белгород
***Podprugin Alexander Ilyich***,
VET Teacher at the College of Engineering
NRU "Be lG U" Russia, Belgorod
***Свиридова Ирина Вячеславовна***,
Ассистент кафедры прикладной информатики и информационных технологий
НИУ «БелГУ» Россия, г. Белгород
***Sviridova Irina Vyachesavovna***,
Assistant of the Department of Applied Informatics And information technology
NRU «BelGU» Russia, Belgorod

# РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РЕАЛИЗАЦИИ АЛГОРИТМОВ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ

# DEVELOPMENT OF SOFTWARE FOR THE IMPLEMENTATION OF ALGORITHMS FOR ENCODING AND DECODING TEXT INFORMATION

***Аннотация***: в данной статье рассматриваются алгоритмы реализации кодирования и декодирования информации, а также рассматриваются достоинства и недостатки алгоритмов.

***Annotation***: this article discusses the algorithms for the implementation of encoding and decoding information, as well as discusses the advantages and disadvantages of algorithms

***Ключевые слова***: кодирование, декодирование, алгоритмы.

***Keywords***: encoding, decoding, algorithms

Актуальность работы подтверждается потребностью в защите информации от третьих лиц, в связи с развивающимся уровнем угроз. Людям важна конфиденциальность данных, как личных, так и рабочих, однако, в связи с развитием технологий, развивается и уровень опасности потери конфиденциальности. С данной проблемой помогает справиться шифрование данной информации, ведь даже при условии попадания зашифрованных данных в руки злоумышленника, возможности прочесть или изменить информацию должным образом нет, так-как в шифротексте отсутствует смысловая нагрузка. Шифрование — это обратимое преобразование информации таким образом, чтобы полностью убрать смысловую нагрузку сообщения, тем самым ограничив доступ злоумышленников к исходному сообщению. Алгоритмы шифрования делятся на симметричные и ассиметричные [2].

Симметричные — это алгоритмы шифрования, использующие единый закрытый ключ. Обеим сторонам, обменивающимся сообщениями, необходимо заранее договорится об используемом алгоритме, ключе и о запрете его разглашения третьим лицам [4].

Достоинствами таких алгоритмах являются: скорость, простота реализации, небольшая длина ключа для сопоставимой стойкости.

Недостатками таких алгоритмов являются: изученность (за счёт большого возраста); сложность управления ключами в большой сети, сложность обмена ключами (необходимость защищённого канала).

Ассиметричные — это алгоритмы шифрования, использующие открытый и закрытый ключи. Первый применяется для шифрования, второй — для дешифрования. Данный подход позволяет избавиться от повторного отправления зашифрованного текста, что обеспечивает меньшую затрату ресурсов [5]. Ассиметричные алгоритмы применяются гораздо чаще в силу большей криптостойкости, по сравнению с симметричными алгоритмами.

Достоинствами таких алгоритмах являются: отсутствие необходимости в секретном канале, для дешифрования секретный ключ нужно знать лишь одной стороне, в больших сетях количество ключей значительно меньше.

Недостатками таких алгоритмов являются: сложность внесения изменений в алгоритм, длина ключа в несколько раз выше, чем в симметричных алгоритмах.

В ходе выполнения работы будет разработано ПО, реализующее такие алгоритмы шифрования как:

1. Шифр «Цезаря», использующий метод простой перестановки.
2. Шифр «Виженера», использующий метод простой перестановки.
3. «RSA» (аббревиатура от фамилий Rivest, Shamir и Adleman)
4. «Схема Эль-Гамаля»
5. Комбинированный алгоритм «Шифр Цезаря» и «RSA»

Следует выделить основные объекты разрабатываемого ПО, которые в дальнейшем будут являться классами [3]: главное окно (Main Class) — класс, отвечающей за логику главного окна программы, выполняет роль связующего звена между пользовательским и системный интерфейсом; окно информации о программе (About Info); шифровальщик (Crypto) — класс, отвечающий за обработку(шифрование/дешифрование) текстовой информации, получаемой от пользователя путём ввода с клавиатуры и/или из файла. Таким образом, при помощи контекстной диаграммы нотации IDEF3, описывающей бизнесс-процесс обработки информации, а также логику взаимодействия подсистем в приложении, будет выглядеть следующим образом (Рис. 1). Диаграмма декомпозиции первого уровня представлена

далее (Рис. 2).

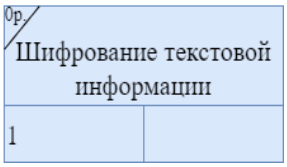


Рис. 1. Диаграмма IDEF3 [A-0]

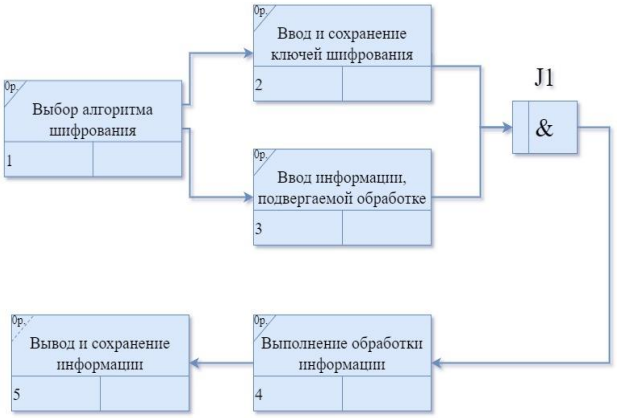


Рис. 2. Диаграмма IDEF3 [A0]

Контекстная диаграмма DFD будет иметь следующий вид (Рис. 3).


Рис. 3. Диаграмма DFD [A-0]

Диаграмма декомпозиции первого уровня представлена далее (Рис. 4).

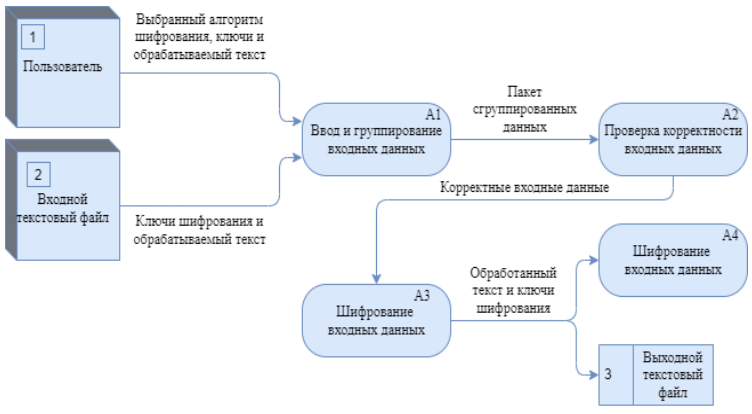


Рис. 4. Диаграмма DFD [A0]

Возможность создания комфортного пользовательского интерфейса с помощью XAML подтверждается большими функциональными возможностями языка. В работе будут использованы таковые: margin (отступы от границ окна или элементов управления), padding (внутренний

отступ контента от элемента управления), content (свойство, содержащие какой-либо объект любого типа) и другие.

Таким образом главное окно ПО будет иметь следующий вид (Рис. 5).

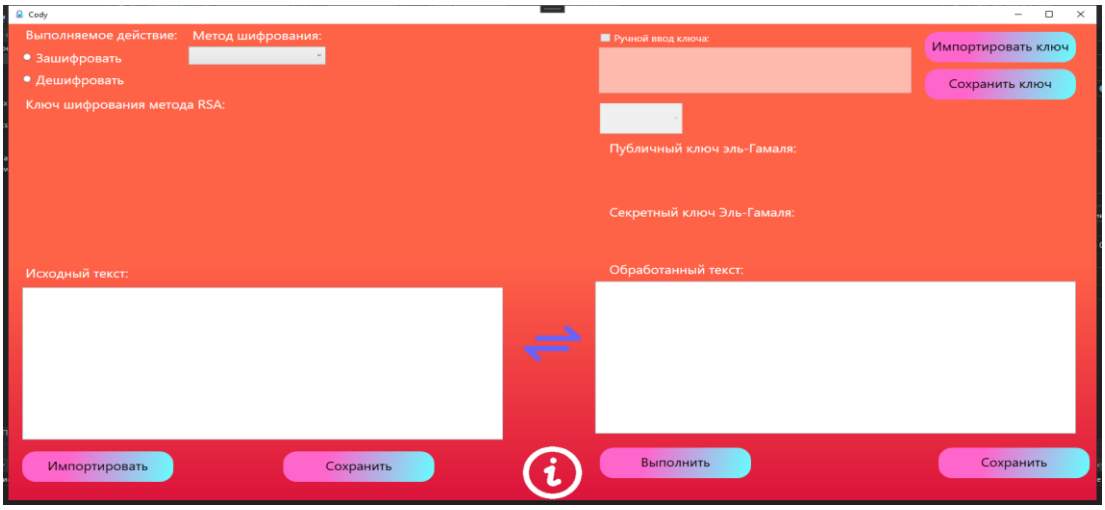


Рис. 5. Внешний вид главного окна программы

Подводя итоги, стоит отметь следующее: было создано ПО, демонстрирующее работу как вышедших из эксплуатации, так и актуальных на сегодняшний день, алгоритмов шифрования. С помощью данного ПО можно уберечь информацию от третьих лиц и/или продемонстрировать работу вышеназванных алгоритмов заинтересованным лицам.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. **Васильева, И. Н.** Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489919

2. **Зараменских, Е. П.** Информационные системы: управление жизненным циклом : учебник и практикум для среднего профессионального образования / Е. П. Зараменских. — Москва : Издательство Юрайт, 2022. — 431 с. — (Профессиональное образование). — ISBN 978-5-534-11624-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495987