



Министерство науки и высшего образования Российской
Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

Студент _____

Группа _____

Тема _____.

Студент:

_____ _____
подпись, дата Фамилия, И.О.

Преподаватель:

_____ _____
подпись, дата Фамилия, И. О.

Преподаватель:

_____ _____
подпись, дата Фамилия, И. О.

Москва — 2022 г.

Оглавление

Введение	3
1 Анализ предметной области	4
1.1 Вывод	4
2 Конструкторская часть	5
2.1 Вывод	5
Заключение	6
Список литературы	7

Введение

Информация - самый ценный ресурс 21 века. Кто владеет информацией - владеет миром. Поэтому ее защита является важнейшей задачей.

Криптография занимается поиском и исследованием методов преобразования информации с целью ее шифрования. В настоящее время существует множество криптографических алгоритмов (КА) обеспечивающих защиту информации. Каждый КА имеет свои не только сильные, но и слабые стороны, позволяющие злоумышленнику осуществить процесс криптоанализа с последующим раскрытием исходного шифртекста.

Существует множество техник, позволяющих проверить (протестировать) устойчивость КА к криптоанализу. К таковым можно отнести: дифференциальный анализ, линейный анализ и т.д. Зачастую, процесс криптоанализа требует больших затрат вычислительных ресурсов, что приводит к усложнению проверки стойкости КА к криптоанализу.

Одной из наиболее перспективных техник оптимизации криптоанализа является применение адаптивных алгоритмов – нейронных сетей, генетических алгоритмов, искусственных иммунных систем и т.д.

Целью данной работы является исследования генетических алгоритмов в области защиты информации.

1 | Анализ предметной области

1.1 Вывод

2 | Конструкторская часть

2.1 Вывод

Заключение

В рамках выполнения работы были решены следующие задачи:

- 1.

Литература

- [1] Visual Studio Code [Электронный ресурс], режим доступа: <https://code.visualstudio.com/> (дата обращения: 02.10.2020)
- [2] Windows [Электронный ресурс], режим доступа: <https://www.microsoft.com/ru-ru/windows> (дата обращения: 02.10.2020)
- [3] Linux [Электронный ресурс], режим доступа: <https://www.linux.org.ru/> (дата обращения: 02.10.2020)
- [4] Руководство по языку python [Электронный ресурс], - режим доступа: <https://pythonworld.ru/samouchitel-python> (дата обращения: 26.11.2020)
- [5] Ubuntu 18.04 [Электронный ресурс], режим доступа: <https://releases.ubuntu.com/18.04/> (дата обращения: 02.10.2020)