

Материалы XXV Республиканской научной конференции студентов и аспирантов «Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях», Гомель, 21–23 марта 2022 г.

лей, так же сталкиваются с растущим спросом на транскрибирование, а конкретнее, субтитры в реальном времени. Ярким примером готового продукта, дающего возможность транскрибировать речь в режиме реального времени, является устройство Eriphan LiveScrypt. Раньше такие субтитры были дорогостоящим удовольствием, требующим от организаторов включать в бюджет мероприятия расходы на профессионального транскрибера, однако с появлением устройств, транскрибирующих речь, расходы значительно сократились.

Актуальность работы обусловлена повышенным спросом общества на решение проблем в различных сферах деятельности, необходимостью изучения систем подобного рода студентами профильной специальности, формирования в обществе адекватного отношения к проблемам информационной безопасности.

### Литература

1 Researchgate.net: бесплатная социальная сеть и средство сотрудничества учёных всех научных дисциплин [Электронный ресурс]. – Режим доступа: [https://www.researchgate.net/publication/228738432\\_Speech\\_Transcription\\_Services](https://www.researchgate.net/publication/228738432_Speech_Transcription_Services). – Дата доступа: 25.11.2021.

**Д. И. Кардаш, А. В. Лубочкин**  
(ГГУ им. Ф. Скорины, Гомель)

## **РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ШИФРОВАНИЯ И ХРАНЕНИЯ ДАННЫХ МНОГИХ ПОЛЬЗОВАТЕЛЕЙ**

На протяжении всех времен люди старались скрыть важную информацию от посторонних глаз. Для этого они всячески пытались зашифровать свои письма и иные источники информации. С развитием новых областей математики возможности шифрования существенно расширились, а после создания первых ЭВМ, не говоря уже о современных компьютерах, открылись совершенно новые возможности для защиты информации [1]. Многие люди, использующие персональные компьютеры (смартфоны и другие подобные, с точки зрения рассматриваемой проблемы, устройства), каждый день сталкиваются с шифрованием данных, но не замечают этого, так как компьютер делает все сам. Однако в нынешнее время любому человеку может понадо-

биться защитить личную информацию, например, для хранения на каком-либо носителе. Для этого и была создана программа шифрования и хранения данных многих пользователей.

Разработанное приложение позволяет без особых усилий и понимания принципов криптографии, зашифровать файлы для последующего их хранения. Данное приложения создано с использованием языка программирования Python и некоторых его библиотек [2]. Для реализации программы использованы библиотеки PySide и Cryptography. PySide позволяет создать графический интерфейс для данного приложения, а модуль Cryptography значительно упрощает реализацию шифрования и дальнейшего его использования.

Программное средство позволяет:

- шифровать и расшифровывать файлы любого типа;
- сохранять файлы для последующего хранения, удалять, редактировать их.

### **Литература**

1 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер ; под ред. А. Б. Васильева. – М. : Триумф, 2002. – 816 с.

2 Лутц, М. Изучаем Python / М. Лутц. – СПб. : Символ-Плюс, 2011. – 1280 с.

**Д. Д. Кибанов**

*(ГрГУ им. Я. Купалы, Гродно)*

## **ИСПОЛЬЗОВАНИЕ СИСТЕМ МОНИТОРИНГА В РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ**

Системы защиты от утечек данных (англ. Data Leak Prevention, DLP) традиционно применяются для мониторинга взаимодействий информационных систем для пресечения незаконной деятельности в рамках политики безопасности компании.

В работе, на примере работы учебного стенда системы Infowatch Traffic Monitor, рассматриваются методы эффективного использования DLP-систем в задачах расследования инцидентов безопасности и киберпреступлений, связанных с утечками данных.

Основополагающим требованием является учет нормативно-законодательной базы. Организация должна заручиться согласием ра-