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-

ботника на обработку данных, непосредственно связанных с его трудовой деятельностью. Такое условие может быть включено в трудовой договор. В результате информация, полученная с использованием DLP-системы, может быть использована в качестве доказательств по уголовному делу, а также служить основанием для привлечения к дисциплинарной ответственности.

Средства конфигурирования DLP-системы позволяют оптимизировать процессы поиска и анализа действий сотрудников, что позволяет своевременно реагировать на угрозы несанкционированной передачи данных рамках настроенной политики. Специализированные инструменты детектируют передачу документов по настраиваемым шаблонам и фильтрам. Документ с потенциально нежелательной информацией проходит проверку, соотносится с уровнем угрозы, после чего, либо пропускает файл, либо прерывает его отправку с оповещением о нарушении.

Совершаемые операции протоколируются. Анализ лог-файлов позволяет получить информацию о характере происшествия – время совершения, устройство и учётная запись пользователя, с которых пытались отправить данные. Найденные улики входят в состав доказательной базы и могут использоваться в суде. В дальнейшем это позволит модифицировать систему для повышения ее эффективности.

Учебный стенд DLP-системы позволяет эффективно демонстрировать технологии защиты компании от внутренних угроз, связанных с утечками данных и нарушениям трудовой дисциплины.

Д. Е. Киселев, М. В. Москалева
(*ГГУ им. Ф. Скорины, Гомель*)

РАЗРАБОТКА ВЕБ-СЕРВИСА ДЛЯ РЕМОНТА ВЕЛОСИПЕДОВ «BICYCLE COMPANY»

В настоящее время почти у каждого был или есть велосипед. К сожалению, как и все вещи, которыми пользуется человек, велосипед может ломаться, к тому же в самый неподходящий момент. Веб-сервис позволяет оставить заявку на ремонт велосипеда, и мастер отправится к пользователю для устранения поломки.

Веб-сервис разработан с использованием платформы ASP.NET Core[1]. Данная платформа позволяет делать веб-приложения, не от-