Рисунок 4 – Построение графовой модели на примере карты кампуса Самарского университета

Литература

1. Бугаевский, Л.М., Цветков, В.Я. Геоинформационные системы [Текст]: учебное пособие для вузов/Л.М. Бугаевский, В.Я. Цветков. – М.: Златоуст, 2000. -222 с., ил.

2. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста [Текст]. – М.: ДМК-Пресс, 2013. -656 с.

С.Ю. Самароков

ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА ДАННЫХ НА МОБИЛЬНЫХ УСТРОЙСТВАХ ОС ANDROID

(Самарский университет)

Мобильные устройства являются неотъемлемой частью современного мира. В настоящее время сложно представить современного человека, который бы существовал без портативного устройства – телефона, смартфона, планшета, умных часов – подключенного к сети Интернет. На сегодняшний день мобильные устройства предназначены не только для ведения телефонных переговоров и отправки сообщений, они способны создавать, обрабатывать, хранить и передавать огромное количество информации.

Как и любая информационная система, мобильные системы связи подвержены атакам нарушителей информационной безопасности, реализующим угрозы и уязвимости [3]:

– кража или утеря мобильного устройства;

– несанкционированный доступ;

– целенаправленная кража мобильного устройства с целью получения доступа к данным;

– атака вредоносного ПО;

– фишинговая атака.

В целях обеспечения безопасного хранения конфиденциальной информации на мобильном устройстве рекомендуется использовать такие методы как [5]:

– блокировка экрана;
– использование PIN кодов и паролей;
– использование всевозможных антивирусных средств защиты;
– обновление ПО мобильных устройств;
– шифрование данных.

Однако они не всегда достаточны.

Одним из наиболее эффективных методов защиты конфиденциальных данных является применение шифрования [6]. Современные мобильные ОС поддерживают функцию шифрования приватной информации [2]. Однако не все производители мобильных устройств позволяют пользователю в полной мере использовать данный функционал. В этом случае возникает необходимость в использовании сторонних приложений для защиты данных. Однако, часто это бывает неудобным, либо даже невозможным. Поэтому возникает потребность в интеграции используемой системы с системой, обеспечивающей защиту данных.

Одним из решений данной проблемы является разработка мобильного приложения, которое будет, в общем виде, позволять пользователям: создавать информационный файл, шифровать данные для хранения или предачи по незащищенному каналу, производить дешифрование данных для отображения.

Мобильные устройства оперируют широким набором данных разного формата и типа. Однако наиболее распространенными в использовании являются аудиофайлы. Их можно легко создать с помощью встроенного в систему диктофона, передать по сети Интернет, неоднократно использовать для прослушивания на различных типах устройств.

В качестве решения разработана автоматизированная система защиты данных на мобильных устройствах, реализующая следующие функции:

– создание аудио файла средствами встроенного в систему диктофона;
– генерирование хеш-функции ключа шифрования по алгоритму MD5;
– шифрование аудиоданных алгоритмами TEA и RC4;
– сохранение данных в файл зашифрованного формата;
– дешифровка зашифрованных файлов;
– проверка целостности данных.

Наиболее рациональным применением для шифрования данных на мобильных устройствах является применение криптоалгоритмов с засекреченным ключом шифрования. Поскольку алгоритмы криптографии с открытым ключом обычно требуют дополнительной вычислительной мощности, их стоит использовать рационально, чтобы избежать быстрого разряда АКБ мобильного устройства.

Особенность симметричных криптосистем состоит в том, что для шифрования информации и ее последующего дешифрования используется один и тот же ключ. Алгоритм воздействия на передаваемые данные может быть известен посторонним, однако он зависит от секретного ключа (рисунок 1). Для предотвращения несанкционированный доступа к зашифрованной информации ключ должен быть засекречен.

В качестве алгоритмов шифрования автоматизированной системы криптографической защиты данных выбраны алгоритмы RC4 и TEA [1,4]. Так как данные алгоритмы легко реализуемы и обладают высокой скоростью шифрования за счет того, что основаны на простых математических операциях (побитового сдвига, xor и т.д.).

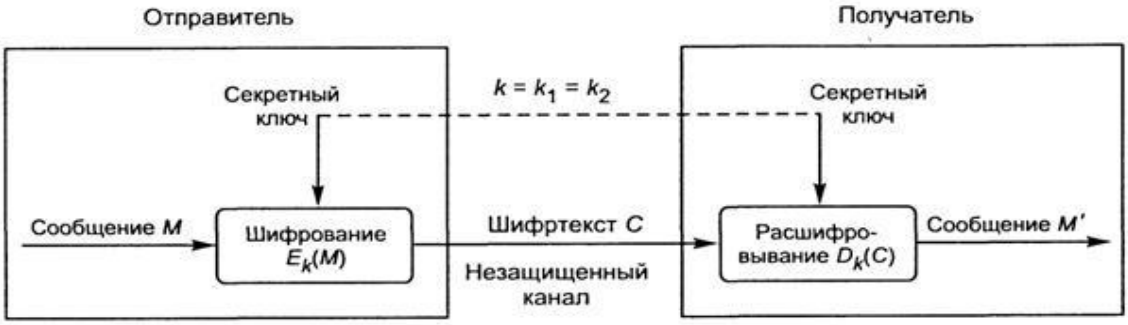

Рисунок 1 – Обобщенная схема симметричной криптосистемы шифрования

Система выполняет функции по шифрованию аудио данных. Следовательно, имеет место потребность в наличии файла, содержащего закодированную информацию, который должен отвечать требованиям системы. Для этого была разработана структура файла, построенная на основе структуры WAV-файла (рисунок 2).

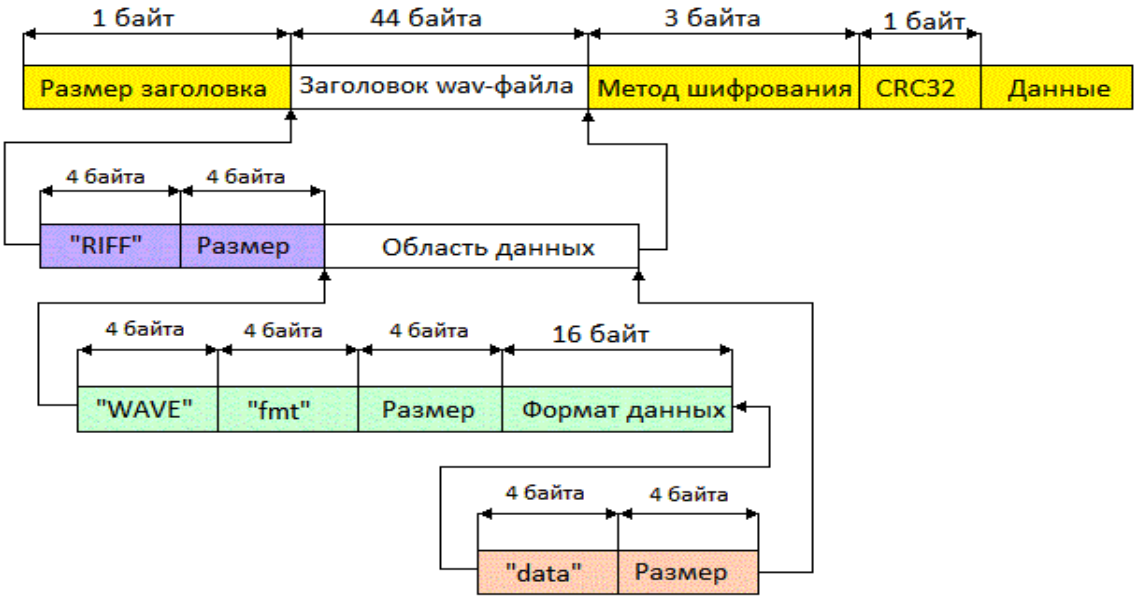

Рисунок 2 – Структура зашифрованного файла

В дальнейшем планируется реализация возможности сокрытия зашифрованных данных посредством алгоритмов стеганографии, а также внедрение в систему функции добавления в зашифрованный файл скрытых цифровых водяных знаков. В итоге, конечный круг реализованных функций позволит снизить вероятность несанкционированного доступа к данным, и как следствие, повысить уровень её защищенности.

Литература

1. Панасенко, С. Алгоритмы шифрования. Специальный справочник [Текст] / С. Панасенко. – Санкт-Петербург: БХВ-Петербург, 2009. – 578 с.

2. Глухих, В.И. Информационная безопасность и защиты данных [Текст] / В.И. Глухих. – ИГТУ, 2011. – 248 с.

3. Блог Лаборатории Касперского [Электронный ресурс]. – URL: https://blog.kaspersky.ru/encryption-reasons/879/

4. Криптография и защита данных [Электронный ресурс]. – URL:http://www.crypto.com/report.html

5. Мобильная безопасность: Защита мобильных устройств в корпоративной среде [Электронный ресурс]. –URL: https://xakep.ru/2011/10/13/57058/

6. Шнайер, Б. Прикладная криптография [Текст] / Брюс Шнайер. – Триумф, 2012. – 815 с.

А.А. Сытник, И.В. Гвоздюк

ОБ ОДНОМ ПОДХОДЕ К АВТОМАТНОМУ МОДЕЛИРОВАНИЮ ПОВЕДЕНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ

(Саратовский государственный технический университет имени Гагарина Ю.А)

Конечные автоматы составляют один из важнейших классов математических моделей для дискретных систем с конечным множеством состояний. Практическое и теоретическое значение автоматных моделей в решении задач проектирования и эксплуатации информационно-коммуникационных систем, формальных языков и трансляторов стало причиной интенсивных исследований по теории автоматов. Конечные автоматы, по сути, являются, практически, единственной математической моделью, способной эффективно использоваться при ппопытках формализации сложных информационных систем и программного обеспечения. Разнообразие возникших задач, подходов к их решению, научных позиций исследователей привело к выделению классов автоматов (автоматы типов Мили и Мура, автоматы Медведева, автономные автоматы, автоматы с конечной глубиной памяти, (n, m, l) – автоматы и т.д.), а также к разработке различных математических способов их задания (табличное задание, графы автоматов, автоматные матрицы, логические уравнения, формулы языка регулярных выражений, задание автомата композицией автоматов).