teller machine), являются наиболее уязвимым элементом системы дистанционного банковского обслуживания.

В настоящее время номенклатура средств обеспечения безопасности банковских терминалов достаточно широкая и при проектировании таких систем, специалист должен уметь обоснованно выбирать технические средства защиты, позволяющие противодействовать соответствующим угрозам безопасности для такого типа оборудования. Таким образом, обучение специалистов по защите информации и повышение их квалификации является актуальной проблемой, для решения которой, в части обеспечения безопасности АТМ терминалов, разработан программный комплекс (ПК).

В качестве среды разработки указанного комплекса использовался программный пакет Macromedia Flash, отличительной особенностью которого является наличие собственного языка программирования ActionScript. Проектирование системы безопасности АТМ, с использованием разработанного ПК выполняется с учетом места установки банковского терминала, исходя из чего пользователь из предлагаемого перечня угроз выбирает наиболее вероятные. На втором этапе выбираются средства обеспечения безопасности, которые, по мнению пользователя, позволяют противодействовать угрозам, определенным на предыдущем этапе. Выбор средств усложняется тем, что учитывается лимит денежных средств, доступных для приобретения таких средств защиты. Пользователь не может завершить проектирование системы безопасности, в случае если лимит денежных средств исчерпан. По завершению проектирования, ПК проводит анализ правильности действий пользователя в части перечня угроз, которые он определит и выбранных средств защиты. По завершению анализа программа формирует отчет, в котором отмечаются ошибки совершенные пользователем на этапе проектирования, для исправления которых необходимо вновь выполнить вышеуказанные этапы 1 и 2.

Разработанный ПК позволяет получить практические навыки при проектировании системы безопасности АТМ терминалов с учетом различных вариантов их установки, а так же выделяемого лимита денежных средств на приобретение средств обеспечения безопасности АТМ.

ВИЗУАЛЬНОЕ ШИФРОВАНИЕ СЕГМЕНТИРОВАННЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПЕРЕСТАНОВОК БИТОВЫХ ПЛОСКОСТЕЙ

Х.М. Альзаки, В.Ю. Цветков, М.Б.М. Махммуд, С.Х. Карбалаи, Ф.Р. Алиханов

Сегментация находит широкое применение в задачах обработки изображений. Сегментированное изображение представляет собой матрицу, совпадающую с размером исходного изображения, каждый элемент которой имеет номер сегмента, которому он принадлежит. Возможно представление сегментированного изображения в виде набора битовых плоскостей, содержащих соответствующие разряды элементов [1]. Предлагается алгоритм визуального шифрования сегментированных изображений на основе перестановок битовых плоскостей. Алгоритм применяет операции поворота на 90 град, зеркальные повороты и диадные сдвиги к каждой битовой плоскости согласно секретным ключевым параметрам. В результате данных операций искажаются значения элементов матрицы сегментации, что приводит к эффекту визуального шифрования, затрудняющего или делающего невозможным восприятие видеоинформации, содержащейся в исходном изображении. Предложенный алгоритм является обратимым и симметричным. Для повышения его стойкости предлагается применять независимо формируемые ключевые последовательности к каждой битовой плоскости.

Литература

1. *Конопелько В.К.* Текстурная сегментация изображений на основе классификации контурных элементов / В.К. Конопелько, С.Н. Касанин, В.Ю. Цветков, Х.М. Альзаки // Вестник сувязі. 2016. № 1. С. 48–52.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

К.М. Бердимырадов

Среди основных требований к проведению коммерческих операций — конфиденциальность, целостность, аутентификация, авторизация, гарантии и сохранение тайны. Для противодействия этим угрозам используется целый ряд методов, основанных на различных технологиях, а именно: шифрование — кодирование данных, препятствующее их прочтению или искажению; цифровые