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

подписи, проверяющие подлинность личности отправителя и получателя; Stealth технологии с использованием электронных ключей; брандмауэры; виртуальные и частные сети. Принципиально новый подход заключается в немедленной авторизации и шифровании финансовой информации в сети Internet с использованием схем SSL (Secure Socket Layer) и SET (Secure Electronic Transaction). Протокол SSL предполагает шифрование информации на канальном уровне, а протокол SET исключительно финансовой информации. Применяются методы шифрования, основанные на "открытых ключах", в том числе и российский стандарт электронной подписи. Алгоритм SET позволяет добиться того, что покупатель не может расшифровать платежные реквизиты продавца, но может расшифровать все данные заказа. С другой стороны, банк не может получить данные по структуре заказа, но имеет доступ к платежным реквизитам продавца и покупателя. Это достигается с использованием двойной электронной подписи: банку посылается одна часть сообщения, а покупателю — другая.

Однако проведенный анализ существующих решений по защите информации в электронной коммерции показывает, что ни один из методов защиты не является универсальным. Не существует абсолютно надежного способа противодействия взлому используемой защиты, и ее взлом — это лишь вопрос времени.

Литература

1. Электронная коммерция: основы организации и ведения бизнеса / А.Л. Денисова, Н.В. Молоткова, М.А. Блюм. Тамбов, 2012.

2. *Юрасов А.В.* Электронная коммерция. М., 2014.

РАСПОЗНАВАНИЕ И АНАЛИЗ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ МУРАВЬИНЫХ АЛГОРИТМОВ

А.И. Бобров

Муравьиный алгоритм — один из эффективных полиномиальных алгоритмов для нахождения приближённых решений задач поиска оптимальных маршрутов на графах. Суть подхода заключается в анализе и использовании модели поведения колонии муравьёв, ищущих пути от колонии к источнику питания.

Примерами задач, которые эффективно решаются при использовании муравьиных алгоритмов, являются задача коммивояжера, маршрутизации автотранспорта, задача о назначениях, задача планирования. Также к ним относятся и задачи классификации, решение которых лежит в основе многих систем обнаружения сетевых вторжений на информационные ресурсы.

Целью данной работы является разработка системы обнаружения атак, которая основана на муравьином алгоритме, а также её тестирование на различных стрессовых выборках, чтобы доказать её эффективность.

Традиционно для решения задач классификации используют различные алгоритмы и модели на основе нейронных сетей и конечных автоматов. В данной работе для решения задач классификации вторжений была использована система, в основе которой лежит модель на основе муравьиных алгоритмов.

Разработанная система, состоит из трех компонент: анализатора, сканнера и базы. База системы — совокупность правил, которые разграничивают сетевые атаки, сканнер — модуль, который собирает данные с информационной системы, а анализатор - модуль, отвечающий за определение соответствия данных из базы и данных, предоставляемых сканнером.

Построенная таким образом система обнаружения атак, основанная на муравьином алгоритме, является качественным аналогом классических систем обнаружения атак. Проведенные тесты показали достаточную эффективность ее работы на различных выборках.

ОЦЕНКА СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ НА ТЕЛЕКОММУНИКАЦИОННЫХ ПРЕДПРИЯТИЯХ С УЧЕТОМ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ БЕЛАРУСЬ

В.А. Бойправ, Л.Л. Утин

Приступая к решению любых вопросов в информационной сфере целесообразно проанализировать следующие документы, определяющие основные термины, используемые в области защиты информации:

– Закон Республики Беларусь «Об информации, информатизации и защите информации»;