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»;

Библиотека БГУИР