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»;

– СТБ ISO/IEC 27000-2012 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь;

– СТБ ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

Законом Республики Беларусь «Об информации, информатизации и защите информации» определено, что защита информации — это комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации. Из приведенных пяти свойств информации в законе дается определение только термину «конфиденциальность» — требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь. Определения остальных указанных свойств информации в законе не приводятся.

В СТБ ISO/IEC 27000-2012 определение термина «защита информации» отсутствует, а используется только понятие информационная безопасность (information security) — сохранение конфиденциальности, целостности и доступности информации. Стандартом допускается возможность включения требования сохранения других свойств информации, таких как подотчетность, неотказуемость, достоверность. В нем приводятся определения всех указанных свойств информации.

В СТБ ГОСТ Р 50922-2006 определено, что безопасность информации (information security) — это состояние защищенности информации при которой обеспечены ее конфиденциальность, доступность и целостность. В стандарте дается определение защиты информации как деятельности, направленной на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Приводятся определения свойств информации.

На основании проведенного анализа можно сделать вывод, что действующие в нашей стране НТПА не дают однозначных определений базовых терминов, используемых в области защиты информации, а в некоторых случаях вступают в противоречия между собой.

Таким образом, с точки зрения законодательства Республики Беларусь корректнее говорить не о системе информационной безопасности (СИБ), а о системе защиты информации (СЗИ) как комплексе правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

АЛГОРИТМЫ БЫСТРОГО ПРЕОБРАЗОВАНИЯ УОЛША

А.А. Будько, Т.Н. Дворникова

Функции Уолша находят применение в различных областях передачи и обработки информации. Преобразование Уолша осуществляется с помощью быстрых алгоритмов.

К настоящему времени имеется определенное количество таких алгоритмов, которые получены в основном используя факторизации матриц Уолша в различных упорядочений. Возможное количество алгоритмов быстрого преобразования Уолша очень велико. Однако они не равноценны. При рассмотрении алгоритмов быстрого преобразования Уолша выделяются так называемые «замечательные» алгоритмы быстрого преобразования Уолша.

В докладе рассматривается метод получения алгоритмов быстрого преобразования Уолша основанный на представлении элементов матриц Уолша в экспоненциальной или показательной форме. Получено два новых алгоритма в системе упорядочения Уолша-Пэлли, которые как и полученные ранее алгоритмы Кули-Туки, Сэнди, Кроузера-Радера-Рошфора, Андрюса-Кейна относятся к «замечательным» алгоритмам. Эти алгоритмы быстрого преобразования Уолша обладают свойствами симметрии, их граф для любой размерности может быть легко получен. Все алгоритмы быстрого преобразования Уолша требуют одинаковое количество арифметических операций, однако решение об использовании для конкретного применения того или иного алгоритма принимается на основе сравнения. Известно, что алгоритмы Кули-Туки и Сэнди не требуют дополнительной памяти, поскольку вычисления осуществляются на местах. В то время алгоритм Кроузера-Радера-Рошфора не позволяет осуществить вычисления на местах и требует дополнительной памяти. Однако граф быстрого преобразования Уолша (алгоритм Гротера-Рейдера) имеет все одинаковые итерации, что дает определенное преимущество при осуществлении вычислений мгновенного спектра по Уолшу.