обеспечения безопасности БД необходимо учитывать указанные особенности.

В настоящий момент существует необходимость в адекватной категоризации уязвимостей БД, принимая во внимание их своеобразие. Применение международного стандарта классификации уязвимостей CVE (Common Vulnerabilities and Exposures) [1], обеспечивает средства для однозначного именования общеизвестных уязвимостей, но при этом не стандартизируются категории уязвимостей, связанных с БД.

Выбор методики кластеризации данных для интеллектуального классифицирования уязвимостей БД обусловлен тем, что кластеризация данных – это способ, применяемый для формирования кластеров объектов, которые имеют похожие признаки. Для таких объектов внутриклассовое подобие максимально, а межклассовое сходство сводится к минимуму, что идеально подходит для категорий уязвимостей. Еще одно преимущество использования кластеризации данных по категориям уязвимостей заключается в том, что требуются минимальные предшествующие знания и предположения. Поэтому целесообразным представляется применение алгоритма кластеризации SOM (Self-organizing map) [2] для категоризации уязвимостей БД. Преимуществом использования SOM в данной методике является возможность получать скрытые сведения из входного набора данных, а также в наглядной визуализации и интерпретации результатов. Категоризация уязвимостей БД с помощью SOM позволит более качественно ранжировать угрозы безопасности БД с целью своевременного реагирования на наиболее критичные из них.

Литература

1. Common Vulnerabilities and Exposures (CVE) [Электронный ресурс]. – Режим доступа http://cve.mitre.org/. Дата доступа 05.02.2017.

2. Kohonen, T., Self-Organizing Maps, Second Edition, Berlin: Springer-Verlag, 1997.

ПРИМЕНЕНИЕ РОЕВЫХ АЛГОРИТМОВ К РЕШЕНИЮ ЗАДАЧ КРИПТОЛОГИИ И ОЦЕНКА ИХ ЭФФЕКТИВНОСТИ

А.И. Бобров

В настоящее время известны применения генетических алгоритмов для оптимизации широкого круга задач, в том числе задач криптоанализа. Различными авторами рассматривались методы организации криптографических атак на традиционные симметричные криптосистемы, использующие шифры перестановки и замены, а также на блочные криптосистемы с использованием методов эволюционной оптимизации и генетического поиска. Недостатком генетических алгоритмов является наличие слепого поиска. В общем случае это приводит к генерации решений с нарушениями и тем самым увеличивает время поиска и требует дополнительного контроля, генерации большого количества одинаковых решений, генерации большого количества плохо приспособленных решений, что может привести к попаданию в локальный оптимум. Поэтому представляют интерес эвристические методы, инспирированные природными системами, в которых осуществляется поэтапное построение решения задачи (то есть добавление нового оптимального частичного решения к уже построенному частичному оптимальному решению).

К таким методам относят и муравьиные алгоритмы, моделирующие поведение колонии муравьев, связанное с их способностью быстро находить кратчайший путь от муравейника к источнику пищи. Колония муравьев рассматривается как многоагентная система, в которой каждый муравей-агент действует автономно на основе простых правил.

Задача поиска алгоритма муравьиных колоний в общем случае заключается в определении позиций для символов из алфавита ключа таким образом, что целевая функция, определяющая оптимальность шифртекста (при заданном открытом тексте) при реализации алгоритма шифрования или оптимальность открытого текста (при заданном шифртексте) при реализации алгоритма криптоанализа, достигает экстремума. Данная задача – частный случай квадратичной задачи о назначениях, традиционно являющейся тестовой задачей для оценки эффективности методов поиска. Метод, построенный на муравьином алгоритме, подходит для расшировки малых и средних текстов, а также может применятся при комплексных методах криптоанализа, в качестве предварительной прогонки перед основных ходом метода.