

Симбиоз SIEM и DLP многократно повышает уровень информационной защиты организации и упрощает работу службе безопасности.

### **Литература**

1. Исследование утечек конфиденциальной информации в 2016 году [Электронный ресурс] – Режим доступа: <https://www.infowatch.ru/analytics>. – Дата доступа: 19.05.2017.

## **АНАЛИЗ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОГРАММНЫХ ПРОДУКТАХ ДЛЯ ПОЛИКЛИНИК**

Е.Д. Антонов, И.С. Гречко, Ю.Ю. Григорьева

Развитие компьютеризации здравоохранения [1] в Беларуси в последние годы может заметить каждый белорус, и в первую очередь, в своей поликлинике. Программные продукты (ПП) для белорусских поликлиник (ПП для поликлиник, ППдМ) разрабатывают в основном 3 минских организации: частное ЗАО «Мапсофт» [1], Белорусский центр медицинских технологий и информатизации (БелЦМТ) [3] и Объединенный институт проблем информатики (ОИПИ) [4] АН РБ. При этом доля минских поликлиник, компьютеризированных каждой организацией, имеет примерно следующий вид: «Мапсофт» – 35 %, БелЦМТ – 25 %, ОИПИ и другие – 40 %. Все ППдМ имеют примерно одинаковую структуру и решают примерно одинаковый круг задач – автоматизация деятельности врача, автоматизация структурных подразделений поликлиники (бухгалтерия, снабжение, статистика и др.).

Однако защита персональных данных пациентов в ППдМ всех разработчиков находится на уровне разграничения прав доступа к данным и контроля за доступом путем анализа логов. В условиях наличия в каждой минской поликлинике неавтоматизированной регистратуры, где хранятся бумажные амбулаторные карты пациентов, вышеописанная защита теряет смысл: зачем злоумышленнику преодолевать сложности доступа к электронным данным, когда проще получить эти данные у низкооплачиваемого работника регистратуры поликлиники. В этих условиях надежная защита персональных данных пациентов в ППдМ будет реализована только после внедрения организационных мероприятий по компьютеризации существующих в поликлиниках регистратур с бумажными амбулаторными картами пациентов.

### **Литература**

1. Демидов, А.В. Информатизация организаций здравоохранения Республики Беларусь // Вопросы организации и информатизации здравоохранения / А.В. Демидов. – 2014. – № 3. – С. 20–25.

2. «МАПСОФТ» – разработка, внедрение и обслуживание ПО [Электронный ресурс]. – Режим доступа: [www.mapsoft.by/of](http://www.mapsoft.by/of) AWG-based WDM-PON Architecture with Multicast Capability. – Дата доступа: 19.05.2017.

3. БелЦМТ [Электронный ресурс]. – Режим доступа: [www.belcmt.by/](http://www.belcmt.by/). – Дата доступа: 19.05.2017.

4. Объединенный институт проблем информатики [Электронный ресурс]. – Режим доступа: [iip.bas-net.by/](http://iip.bas-net.by/). – Дата доступа: 19.05.2017.

## **МЕТОДИКА КАТЕГОРИЗАЦИИ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БД НА ОСНОВЕ АЛГОРИТМА КЛАСТЕРНОГО АНАЛИЗА SOM**

Э.В. Артемьев

Понимание характера уязвимостей информационной безопасности имеет решающее значение для анализа угроз, которые они представляют. В значительной мере это касается таких информационных систем, как базы данных (БД), которые имеют ряд характерных особенностей, свойственных хранилищам данных: двойственная природа систем управления базами данных (СУБД), зависимость уязвимостей и механизмов управления от данных и описывающей их организацию модели, угрозы логического вывода, различная значимость сочетаний данных. Все это определяет специфический характер уязвимостей информационной безопасности БД. Поэтому для повышения эффективности защиты при выборе методов

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 расширения малых и средних текстов, а также может применяться при комплексных методах криптоанализа, в качестве предварительной прогонки перед основным ходом метода.