2. *Ручай А. Н.* Разработка комплекса модулей для разграничения прав доступа в ОС Windows XP на основе биометрической аутентификации // Информационные технологии и системы: материалы Первой Международной конференции. Челябинск: ЧелГУ, 2012. С. 75–76.
3. *Ручай А. Н.* Модель атак и защиты на биометрическую систему распознавания диктора // Доклады ТУСУР. 2011. № 1 (23). С. 96–100.

А. Ю. Сенцова, И. В. Машкина

АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

В настоящее время все большее распространение получает *технология облачных вычислений*, при которой данные, программное обеспечение (ПО), прикладные системы, компьютерные ресурсы предоставляются клиентам по запросу как услуга через Интернет [1]. При этом заказчик имеет тот уровень защищенности в облаке, который обеспечивается вендором, поэтому существует необходимость анализа и оценки возможных информационных рисков в системе облачных вычислений (СОбВ).

Облачная модель состоит из сервисов клиентов, управляемого централизованного контента и виртуальной инфраструктуры. Кроме таких компонентов традиционной инфраструктуры информационной системы, как сеть, компьютеры, серверы, в архитектуру облачной системы входят blade-сервер и облачные приложения [2].

В работе рассматривается бизнес-модель продажи и использования *приложения как услуги (SaaS)*. Вендор в этом случае разрабатывает веб-приложение и предоставляет заказчику (клиенту) доступ к ПО через Интернет. На основе анализа технологии клиент-серверного взаимодействия и известных описаний существующих систем разработана *архитектура облачной системы*. Архитектура системы облачных вычислений настолько сложна, что она приобретает новые, неизвестные прежде уязвимости. Переход к облачным средам приводит к появлению *принципиально новых угроз* [3]. Для облачных сред угрозы удаленного взлома и заражения вредоносным кодом весьма значимы из-за параллельного существования множества виртуальных машин. Кроме того, виртуальная машина отличается от физической возможностью ее заражения в *выключенном* состоянии [1, 3], если есть доступ к хранилищу образов виртуальных машин через сеть. Поэтому особое внимание должно быть уделено *политикам безопасности* в виртуальных инфраструктурах.

Опасность возникновения ущерба или убытков в результате использования организацией облачных сред может быть оценена величиной информационного риска в системе облачных вычислений. В данной работе предложена концептуальная модель угроз в виде *нечетких когнитивных карт* (НКК), построенных на основе разработанной системы облачных вычислений, для анализа рисков нарушения информационной безопасности.

Информационный риск обусловлен наличием угроз нарушения безопасности информации. Поэтому необходимо в первую очередь идентифицировать все возможные угрозы и их источники. Каждая угроза должна быть детализирована и оценена с учетом наличия уязвимостей на путях ее распространения.

Применение НКК позволяет произвести моделирование процессов распространения угроз в системе облачных вычислений через используемые уязвимости компонентов ее архитектуры. При этом полученная модель обладает свойством *наглядности*, простотой *понимания и перевода* содержательного знания эксперта на математический язык.

На основе разработанных моделей угроз, реализуемых злоумышленником, внешним и внутренним пользователями Заказчика, пользователем с высокими привилегиями, пользователем вендора в СОбВ, производится оценивание прогнозируемых значений рисков нарушения ИБ в соответствии с методом, приведенным в [4].

Результаты расчета рисков с помощью НКК могут быть использованы с целью формирования множества данных обучающих выборок для обучения искусственной нейронной сети (ИНС). Обучающая выборка для настройки весов ИНС сформирована методом разряжения.

После обучения ИНС в составе системы управления ИБ обеспечит получение динамической оценки информационного риска с учетом актуальных данных, сформированных в процессе мониторинга инфраструктуры СОбВ. На вход ИНС подается информация с выхода модуля анализа событий безопасности, в котором на основе оперативных данных (полученных с сенсоров систем обнаружения вторжений, антивирусов, с межсетевых экранов и других компонентов инфраструктуры) выявляется источник актуальной угрозы. На выходе ИНС формируется динамическая оценка риска нарушения ИБ.

Численное значение риска используется в подсистеме поддержки принятия решений о выборе рационального варианта реагирования на атаку и подается на консоль администратора безопасности.

Большинство типов ИНС может быть использовано для задачи получения численной динамической оценки рисков нарушения ИБ после настройки параметров с помощью НКК.

СПИСОК ЛИТЕРАТУРЫ:

1. Официальный сайт журнала «Компьютер-Пресс» [Электрон. ресурс]. URL: http://compress.ru/article.aspx?id=21238&iid=967 (дата обращения: 18.02.2013).
2. *Lee G.*, N. Antonopoulos, L. Gillam Cloud Computing: Principles, Systems and Applications /. L.: Springer, 2010. — 379 p.
3. *Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях. М.: ДМК-Пресс, 2012. — 592 с.
4. *Гузаиров М. Б., Машкина И. В., Степанова Е. С.* Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. 2011. № 2. С. 37—49.

Д. С. Симоненкова, А. Н. Велигура

ОБ ИНФОРМАЦИОННЫХ СИСТЕМАХ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В работе рассматривается популярная облачная платформа Amazon Web Services (AWS). Описаны сервисы, предоставляемые платформой AWS, такие как: Amazon Relational Database Service (Amazon RDS), Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notifications Service (Amazon SNS), Amazon Elastic MapReduce, Amazon Virtual Private Cloud (Amazon VPC), Amazon Route5, AWS Identity и Access Management (IAM). Детально рассмотрены ключевые сервисы Amazon Simple Storage (AmazonS3), Amazon CloudWatch и Amazon Elastic Compute Cloud (AmazonEC2), описана система обеспечения безопасности данных в каждом из ключевых сервисов AWS. Подробно представлено взаимодействие всех сервисов AWS [1, 2].