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].

Рассмотрены основные способы защиты данных в AWS от возможной реализации наиболее распространенных классов сетевых атак, таких как: «Распределенный отказ в обслуживании» (DDoS), «Человек посередине» (MITM), IP Spoofing, PortScanning, защита от перехвата пакетов другими подписчиками облака. Также рассмотрен вопрос актуальности разработки методики составления модели угроз безопасности для информационных систем, построенных на основе технологий облачных вычислений, при определении требований для обеспечения безопасности данных в облаке.

СПИСОК ЛИТЕРАТУРЫ:

1. About AWS. URL: http://aws.amazon.com/what-is-aws/ (дата обращения 13.11.2012).
2. Amazon Web Services: Overview of Security Processes — May 2011. URL: aws.amazon.com/whitepapers/ (дата обращения 13.11.2012).

М. М. Тараскин, Ю. И. Коваленко

ВЕРБАЛЬНАЯ ФОРМУЛИРОВКА ПОДХОДА К ПОСТРОЕНИЮ ОПТИМАЛЬНОЙ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Отличительной особенностью современного периода является переход от индустриального общества к информационному. Это формирует повышенные требования к защите информационных ресурсов. Достижение необходимого уровня информационной безопасности в организациях должно, прежде всего, базироваться на исследовании источников угроз для информации, уязвимостей в ее защите и проистекающих из их соотношений рисков.

При разработке и создании системы комплексной защиты информации в организации основное внимание должно быть уделено ее оптимальности. Оптимальность системы защиты заключается в том, что она должна обеспечить требуемый уровень защиты информации при минимальном расходовании ресурсов (финансовых, технических, информационных и др.) на ее создание, организацию и обеспечение функционирования или при заданном объеме ресурсов обеспечить максимально возможный уровень защищенности информации.

При оптимизации системы защиты ключевым исходным моментом является формирование полного множества функций защиты, так как надлежащим распределением ресурсов для осуществления каждой из функций можно оказывать воздействие на уровень защищенности информации, создавая таким образом объективные предпосылки для разработки оптимальной системы защиты.

Полное множество должны составлять семь функций защиты:

— создание таких условий, при которых угрозы безопасности информации не могли бы проявляться;

— предупреждение появления угроз, даже если для этого есть объективные предпосылки;

— обнаружение появления угроз;

— предупреждение воздействия появившихся угроз на защищаемую информацию;

— обнаружение воздействия угроз на защищаемую информацию;