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;

— локализация воздействия угроз на информацию;

— ликвидация последствий воздействия угроз.

На основе вышесказанного и с учетом состояния аналитической базы решения задачи оптимизации систем защиты может быть реализован следующий подход к построению оптимальной системы комплексной защиты информации:

— проводится анализ структурного построения и принципов функционирования организации и выделяются на основе анализа уязвимые элементы, которые влияют на безопасность объекта;

— определяются и анализируются возможные угрозы выделенным элементам и формируется перечень требований к системе защиты;

— на основе опыта создания систем защиты информации определяются наиболее подходящие варианты набора средств и мер защиты, использованием которых может быть реализована каждая из функций защиты, и для этих вариантов методами экспертных оценок определяются показатели их эффективности;

— на основе технико-экономических оценок средств и мер защиты определяются размеры ресурсов, необходимых для практического использования различных средств и мер;

— решается задача синтеза оптимальной системы защиты информации математическими методами, в частности на основе аксиоматики алгебры логики.

Необходимым условием разработки системы защиты информации является соблюдение следующих принципов:

— учет требований защиты информации при построении организации и разработке технологии автоматизированной обработки информации;

— комплексность использования средств и методов защиты; обеспечение непрерывности процесса защиты;

— обеспечение периодического контроля правильности функционирования всех подсистем защиты.

Разработка системы комплексной защиты информации может выполняться как без использования каких-либо ранее созданных средств защиты, так и с их использованием в качестве элементов системы.

Применение данного подхода к построению оптимальной системы комплексной защиты информации в организации обеспечит интегральность учета угроз, уязвимостей и рисков и тем самым обеспечит требуемый уровень информационной безопасности в организации.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями от 27 июля 2010 г., 6 апреля, 21 июля 2011 г., 28 июля 2012 г.).

2. *Асфаль Р.* Роботы и автоматизация производства / Пер. с англ. М. Ю. Евстегнеева и др. М.: Машиностроение, 1989.

3. Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст).