А. И. Бражук
(*УО «ГрГУ им. Я. Купалы», Гродно)*

ПРИНЦИПЫ МОДЕЛИРОВАНИЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ ОБЛАЧНЫХ СИСТЕМ КЛАССА «ИНФРАСТРУКТУРА КАК УСЛУГА»

Перспективные облачные компьютерные системы класса «Инфраструктура как услуга» (Infrastructure as a Service, IaaS) непосредственно основаны на технологиях виртуализации аппаратных платформ. Кроме угроз информационной безопасности (ИБ), характерных

для традиционных компьютерных систем, внедрение слоя гипервизора и виртуальных машин (ВМ) порождает новые классы угроз (нелегитимные ВМ, хищение данных ВМ, уязвимости гипервизора, атаки на виртуальную сетевую инфраструктуру и т.п.) [1, 2].

Моделирование ИБ систем IaaS должно обеспечивать анализ угроз и уязвимостей для решения задач *синтеза систем ИБ* и *анализа защищенности;* а также осуществляться в соответствии со следующими принципами:

– *Ролевой подход и инвариантность роли к результатам анализа*. Выбранное представление (пользователь, провайдер, разработчик) должно давать корректные результаты моделирования.

– *Интегральность модели*. Полученный набор моделей должен обобщать частные модели ИБ.

– *Многомерность и актуальность данных*. Модель должна обеспечивать анализ данных по ключевым аспектам функционирования системы IaaS. Данные должны постоянно пополняться и отражать текущее состояние теории и практики ИБ.

– *Практическая ориентированность и адаптивность модели.* Модель должна обеспечивать возможность задания различных конфигураций входных данных и их изменения в широком диапазоне.

Литература

1 SP 800-125. Guide to Security for Full Virtualization Technologies / Scarfone K. A. et al. // National Institute of Standards & Technology, Gaithersburg, MD. – 2011. – 35 p.

2 An analysis of security issues for cloud computing / Hashizume K. et al. // Journal of Internet Services and Applications. – 2013. – Т. 4. – № 1. – P. 5 – 8.