УДК УДК 004.056:004.738.5

Евсеев С. П., Король О. Г.

Serhii.Yevseiev@hneu.net, Olha.Korol@hneu.net

Харьковский национальный экономический университет имени Семена Кузнеца, Харьков

КОНЦЕПТУАЛЬНАЯ СИНЕРГЕТИЧЕСКАЯ МОДЕЛЬОЦЕНКИ БЕЗОПАСНОСТИ БАНКОВСКОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ БАНКОВСКОГО СЕКТОРА

Анализ последних исследований и публикаций показал, что при построении защиты информации сложился подход, основанный на представлении процесса ее обработки в виде абстрактной вычислительной среды, в которой работают множество субъектов (пользователей и процессов) с множеством объектов (ресурсы и наборы данных).

При этом построение системы защиты заключается в создании защитной среды в виде некоторого множества ограничений и процедур, способных под управлением ядра безопасности запретить несанкционированный и реализовать санкционированный доступ субъектов к объектам и защиту последних от преднамеренных и случайных внешних и внутренних угроз. Данный подход опирается на теоретические модели безопасности Хартсона, Белла –Лападулы, MMS Лендвера и Мак Лина, Биба, Кларка – Вилсона и др.

Основным отличием предлагаемого подхода моделирования модели безопасности от известных является, во-первых, использование синергетического подхода при построении модели угроз, что дает эмерджентный эффект получения комплексированной оценки угроз БИн, во-вторых, обеспечению успешности выполнения бизнес-процессов посредством функций безопасности БИн (ФББИн), выделенных элементов АБС, основанных на требованиях: обеспечение конфиденциальности, доступности, целостности, аутентичности и непрерывности бизнес-процессов. сервисов и сетевых, и аппаратных подсистем. На рис. 1 приведены в обобщенном виде компоненты концептуальной синергетической модели безопасности БИн.

Концептуальная синергетическая модель безопасности БИн формируется на основе предложенной методологии и синергетическом подходе к обеспечению безопасности БИн и оцениванию безопасности информационных технологий (ИТ) АБС Украины, а также частных моделей: инфраструктурной модели АБС, синергетической модели угроз и модели проведения оценки защищенности АБС. Предложенная синергетическая модель оценки безопасности банковской информации (БИн) позволяет переосмыслить подход построения политик безопасности БИн на основе выявления эмерджентных свойств с использованием синергетической модели угроз, что позволяет комплексированно подходить к оценке рисков, с учетом главенствования киберугроз. Модель инфраструктуры АБС позволяет связать элементы иерархической структуры с коммуникационными связями с информационными активами БИн, и на основании синергетической модели угроз возможные деструктивные последствия, модель нарушителя позволяет строить типовые модели нарушителя в соответствии с требованиями регуляторов, при этом используется однозначная классификация нарушителей прав доступа, что позволяет избежать привлечения экспертов на этапе предпроектного обследования.