©Савченко А.Ю.
МОДЕЛЮВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ
 СИСТЕМИ ПРИ РЕАЛІЗАЦІЇ ПОГРОЗ ВІДДАЛЕНОГО ТА БЕЗПОСЕРЕДНЬОГО ДОСТУПУ

Погрози інформаційної безпеки мають імовірнісний характер та змінюються в процесі функціонування інформаційно-телекомунікаційної системи (ІТКС), тому поняття «ризику» необхідно розглядати як деяку імовірнісну категорію, що асоціюється з поняттям збитків від успішної реалізації погроз, а в якості базової моделі взяти імовірнісну модель атак на ІТКС, в якій об’єктивні співвідношення виражені в термінах теорії ймовірностей та математичної статистики.

Одним із шляхів вирішення проблеми оцінки ризиків та вибору оптимального варіанта їх обробки є моделювання. Призначенням моделювання процесів управління ризиками інформаційної безпеки є отримання необхідної інформації для проведення аналізу на доказовій основі з метою прийняття обґрунтованих рішень стосовно того, яким чином краще забезпечувати захист активів організації від певних загроз інформаційної безпеки. На сьогодні методики оцінювання ризиків ІБ можна умовно поділити на стандартизовані та наукові. У перших, як правило, застосовується якісний підхід з використанням різного роду таблиць зі шкалами значень ризику. Найбільш популярними та найчастіше використовуваними на практиці є методики наведені у стандартах ISO/IEC 27005:2011 , NISTSP800-30, OCTAVE та EBIOS. У наукових методиках здійснюється спроба реалізації кількісного аналізу шляхом використання різноманітного математичного апарату, а саме: теорії імовірностей, теорії нечіткої логіки, імовірнісних методів, мереж Петрі, нейронних мереж тощо. Однак перші не дозволяють отримати точні результати, а другі є занадто складними для практичного застосування.

Зазначимо, що у міжнародному стандарті ISO/IEC 31010 наведено понад 30 підходів до аналізу та оцінки ризиків. Отже, розроблювані у цій роботі моделі, мають: відобразити складну структуру інформаційно-комунікаційних систем та мереж, які функціонують в організаціях, та вміти легко пристосовуватись до динамічних змін у їх структурі; надавати відомості, необхідні для прийняття управляючих рішень, за обмеженої кількості відомостей про об’єкт; за короткий проміжок часу та в умовах дефіциту бюджету організації отримувати кількісні вихідні дані.

Для реалізації цілей ми поставили та розв’язали такі задачі: розробили та побудували на основі апарату мереж Петрі-Маркова моделі реалізації загроз безпосереднього та віддаленого доступу до елементів ІТКС без врахування та з урахуванням використання засобів захисту; отримали в результаті аналітичного моделювання часові та ймовірні характеристики реалізації загроз безпосереднього та віддаленого доступу до елементів системи; розробили методику оцінки ризиків та захищеності інформаційно-телекомунікаційної системи; дослідили рух параметрів ризику та захищеності ІТКС при зміні параметрів досліджуваних загроз; розробили алгоритми управління ризиком в ІТКС, що атакується; розробили методику оцінки ефективності мір та засобів захисту ІТКС.

Робота виконана під керівництвом к.т.н., доц. кафедри РКС Федюшина О.І.