**Васильєв М. В.**

**РОЗРАХУНОК РИЗИК-МОДЕЛЕЙ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ**

Аналіз можливих погроз та аналіз ризиків є основою для обґрунтування вибору заходів щодо забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем, що повинні бути використані для зниження ризику до необхідного рівня. Для отримання адекватних імовірнісних характеристик реалізації досліджуваних погроз необхідно отримати математичні моделі процесів виникнення та реалізації даних погроз. Динаміка реалізації погроз безпосереднього та віддаленого доступу до елементів інформаційно-телекомунікаційної системи (ІТКС) в сучасних умовах являє собою складний динамічний процес, з зв’язку з тим, що в ІТКС присутня множина паралельних процесів, виконання яких впливає на реалізацію даних дій. Тому для опису процесу реалізації погроз, що досліджуються, доцільніше використовувати моделі, побудовані на базі мереж Петрі-Маркова, в основі яких лежать теорія мереж Петрі та напівмарківські процеси, що дозволяє розглядати реалізацію паралельних процесів з визначенням часових та статистичних характеристик.

Окремі аспекти аналізу та управління ризиками досліджувались у роботах О.Г. Корченко, В.Г. Криволапова, Д.О. Котенко, Є.Г. Новицького, Пітера Стефенсона, в тому числі з позиції теорії штучного інтелекту, експертних та нечітких систем.

В роботі розглянута ІТКС як об'єкт атак, пов'язаних з безпосереднім і віддаленим доступом до її елементів, виділений перелік найбільш актуальних атак для ІТКС, що функціонують на основі стека протоколів TCP/IP, досліджені алгоритми їх реалізації, а також приведені найбільш адекватні заходи протидії цим атакам. З використанням апарату теорії мереж Петрі-Маркова розроблені аналітичні моделі реалізації атак, пов'язаних з безпосереднім і віддаленим доступом до елементів ІТКС. На основі аналітичного моделювання зроблений розрахунок імовірнісних і часових характеристик реалізації даних атак, а також досліджений вплив на динаміку реалізації атак застосування відповідних заходів і засобів захисту.

Розглянуті основні види збитку ІТКС при реалізації цих атак. За основний закон розподілу вірогідності кількості реалізованих атак на основі відповідних висновків прийнятий закон розподілу Пуассона. Досліджена взаємна залежність виникнення віддалених атак, виходячи з якої розраховані інтенсивності їх виникнення, а потім вірогідність їх реалізації. Розроблена методика аналізу ризиків при реалізації даних атак, що завдають збитку різної величини і побудовані відповідні розподіли збитків і ризиків для заданого набору значень інтенсивностей атак.

Розроблена методика застосована для вирішення завдання управління ризиками ІТКС. Розрахована вірогідність реалізації атак з урахуванням використання заходів і засобів захисту, і побудовані відповідні розподіли ризиків.

Отримані ризик-моделі дозволяють здійснити підвищити зручність, швидкість, точність та інформативність оцінки ризиків інформаційної безпеки, спростити процес обрання варіанта обробки ризиків шляхом побудови моделей процесу управління ризиками інформаційної безпеки.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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