3. Foody G., See L., Fritz, S., Mooney P., Olteanu-Raimond A.-M., Fonte C. C., Antoniou V. Mapping and the Citizen Sensor. Ubiquity Press. URL: http://www.jstor.org/stable/j.ctv3t5qzc

4. Official website OpenStreetMap. URL: https://www.openstreetmap.org/

ВИБІР ФАКТОРІВ ПРИ СТАТИСТИЧНОМУ ДОСЛІДЖЕННІ РИЗИКУ КІБЕРАТАК

***Густера Олег Михайлович*,**
кандидат економічних наук, асистент кафедри статистики,
інформаційно-аналітичних систем та демографії;
Київський національний університет імені Тараса Шевченка

Управління ризиком може базуватись на використанні даних з різних інформаційних джерел, одним з найбільш поширених з яких є статистичний аналіз що дозволяє отримати відомості про фактори що впливають на ризик, ступінь на напрямок зв'язку між різними факторами, тісноту зв'язку між різними факторами та можливість побудування математичної моделі що буде використовуватись для отримання достовірного прогнозу.

Основні параметри ризикової ситуації які можуть бути корисними для прийняття рішення та управління ризиком на прикладі ризику кібератаки для підприємства – кількість атак (загальна або у розрізі конкретної галузі підприємства) та відповідно до цього масиву кількості наслідки що можуть бути при настанні ризикової події (максимальний, мінімальний та середній збиток). Використання лише середнього значення збитків від кібератаки не може повністю охоплювати ступінь ризику для даної події. Так, наприклад, деякі атаки не приносять суттєвих збитків тому що направлені на виявлення незакритих портів або інших незахищених місць та використовуються зловмисниками не для комерційних цілей. В той же час, інші атаки при їх невеликій кількості можуть призводити до суттєвих збитків – видалення або спотворення інформації, викрадання конфіденційних даних. Найчастіше для розділення на більш або менш суттєві ризики використовують категоризацію ризиків за ступенем потенційних збитків або не враховують атаки які не призводять до збитків.

При цьому також потрібно враховувати загальну кількість пристроїв що підключені до мережі та потенційно можуть бути атакованими, так як вони визначають генеральну сукупність та відносно до неї може бути визначена імовірність атаки з урахуванням фактичної кількості кібератак.

До параметрів що можуть бути використані при статистичному дослідженні оцінки ризику можна віднести:

- загальна кількість кібератак,
- сфера діяльності підприємства,
- розміщення інформаційної інфраструктури підприємства,
- наявність захисту від найбільш поширених атак,

- потужність кібератаки (кількість атакованих пристроїв),
- загальна кількість пристроїв у мережі, що можуть бути атаковані.

Використання пасивних інструментів захисту від кібератак у дата центрах може як позитивно, так і негативно впливати на імовірність атаки зловмисниками. Так, наприклад, зловмисник може втратити інтерес через те що не може обійти захист, або навпаки проявляти більший інтерес до захищених інформаційних інфраструктур як потенційно більш цінних.

Сфера діяльності підприємства також достатньо суттєво впливає на можливу кількість атак. Більшість підготовлених та цілеспрямованих атак використовуються для отримання комерційної вигоди, тому направлені на організації що використовують цінну інформацію або здатні сплачувати за неї кошти. Також у галузях з високим рівнем конкуренції кількість атак може збільшуватись через недобросовісні дії інших організацій.

Розміщення інформаційної інфраструктури підприємства - в окремому дата центрі, у провайдера послуг або безпосередньо в організації, може визначати ступінь захисту а також імовірність атаки. Як правило, спеціалізовані дата центри з системами захисту рідше стають цілями кібератак. При проведенні статистичного аналізу окремо оцінюються як кількісні та якісні показники кібератаки – до якісних можна віднести ступінь збитків від кожної атаки, до кількісних – кількість атак, частота атак, кількість атакованих пристроїв.

Список використаних джерел

1. Wilkens S., Predescu M. Default risk charge: modeling framework for the «Basel» risk measure. Journal of Risk. 2017. Vol. 19, № 4. pp. 23–50

2. Ivanchenko N. Development of the system for prediction of security state of an enterprise using semantic–frame fuzzy models of knowledge base. Східно-Європейський журнал передових технологій. 2017. Vol 6, № 3 (90). С. 58-65