Сумський державний університет
Навчально-науковий інститут бізнес-технологій «УАБС»

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ФІНАНСОВО-КРЕДИТНОЇ СИСТЕМИ УКРАЇНИ

МАТЕРІАЛИ
IV Всеукраїнської науково-практичної on-line-конференції
(Суми, 21–22 листопада 2019 року)

У двох частинах

Частина 2

Суми
Сумський державний університет
2019

допомогою комбінування таких форм можна досягти майже будь-якого рельєфу.

Подальше дослідження має сенс у двох ракурсах: по-перше, як імітація руху часток у створеному умовному просторі, по-друге, як динамічна модель в ракурсі різних форм рельєфу і різних скупчень суб'єктів взаємодії.

Практична користь даного дослідження полягає у тому, що дана модель дозволяє виявити і формально описати закони поширення інформації в натовпі за існуючими емпіричними даними.

Список використаних джерел

1. William J. Reilly. The Law of Retail Gravitation [Online]. URL:https://babel.hathitrust.org/cgi/pt?id=uc1.$b50138&view=2up&seq=6.

УДК 330.43(075)

Братушка Сепргій Миколайович,
к.ф.-м.н., доцент,
Сумський державний університет, м. Суми
Лосина Євгеній Сергійович,
студент,
Сумський державний університет, м. Суми

СТАТИСТИЧНИЙ АНАЛІЗ ДИНАМІКИ КІБЕРАТАК НА ФІНАНСОВІ УСТАНОВИ

Банки завжди привертали злочинців, що бажали здійснити пограбування. З розвитком технологій зробити це стало простіше: адже не потрібно вриватися в офіс банку зі зброєю і вимагати відкрити сховище. Інформаційні технології відіграють ключову роль у підвищенні конкурентоспроможності кредитно-

фінансових установ, які функціонують в умовах мінливого ринкового середовища, сприяють його розвитку і зростанню прибутковості. Разом з цим можна виділити і новий напрямок загроз для таких установ. Високі доходи і незначний ризик затримання привели до бурхливого зростання кількості кіберзлочинів. І хоча учасників окремих угруповань час від часу затримують, на їх місце приходять все нові і нові зловмисники, які застосовують все більш витончені методи кібератак.

Кібератака, або хакерська атака, - це атака на комп'ютерну мережу, мета якої - захопити контроль над системою, порушити нормальне її функціонування або змусити її виконувати різні шкідливі завдання. За даними Allianz та WEF, кібер-ризики посідають 2 місце серед усіх бізнес-загроз та входять в ТОП-10 ризиків людства. Відповідно до даних FBI’s Internet Crime Complaint Center, збитки завдані кіберзлочинністю у світі за останні 5 років склали 12 трлн доларів. [1]

За даними дослідження Positive Technologies, сім з десяти кібератак в 2017 році були здійснені з метою отримання прямої фінансової вигоди, наприклад, для виведення грошей з банківських рахунків жертви. Більш того, протягом останніх років спостерігається зростання кібератак саме на банківські установи (Рис. 1).

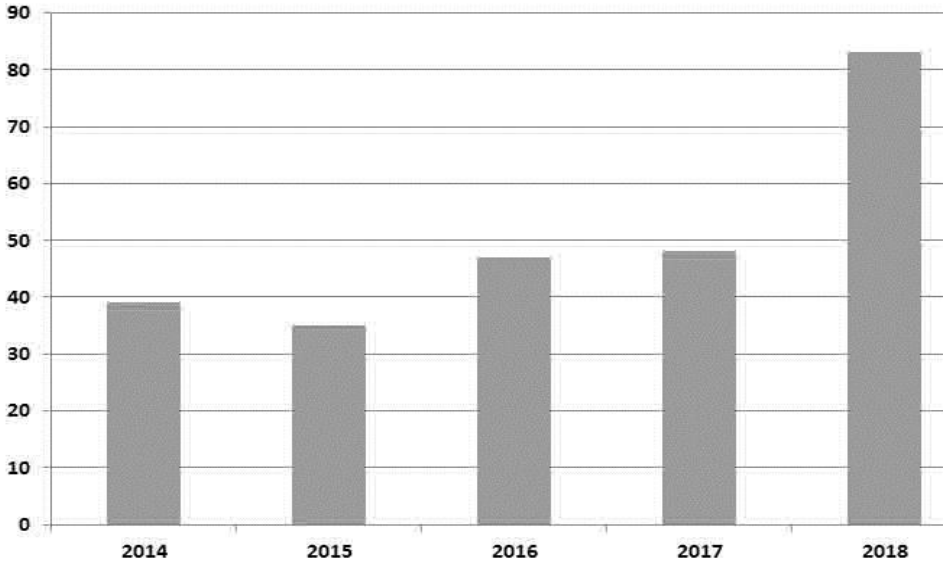

Рисунок 1. – Динаміка кібератак на банківські установи у світі, за даними [2]

У вересні 2019 року компанія Accenture представила результати дослідження, в якому виявила основні загрози інформаційній безпеці бізнесу в 2019 році. За оцінкою Accenture, ринок сервісів кібербезпеки зростає темпами, аналогічними ринків Digital і IT. Accenture прогнозує, що до 2021 року обсяг світового ринку інтернет-бізнесу збільшиться на 66% і складе $ 202 млрд. При цьому сукупний світовий збиток від кібератак може вирости до 2021 року на 39% до $2,1 млрд.

Якщо проводити аналіз напрямків кібератак на банківські установи, основні типи атак наступні:

DDoS - розподілена атака типу «відмова в обслуговуванні». Мережевий ресурс виходить з ладу в результаті безлічі запитів до нього, за короткий проміжок часу відправлених з різних точок.

Malvare - скорочено від англійського «malicious software» - шкідливе програмне забезпечення, що має своєю метою в тій чи іншій формі завдати шкоди користувачу або комп'ютера і його вмісту. Malvare - загальна назва для всіх видів кібер-загроз, таких як: віруси, трояни, шпигунські програми, adware і ін.

Accounting hijacking - це процес, за допомогою якого електронну пошту, обліковий запис комп’ютера чи будь-який інший обліковий запис особи, пов'язаний з обчислювальним пристроєм чи послугою, викрадений або викрадений хакером.

Target attac - цілеспрямована атака, яка відноситься до типу загрози, при якій суб'єкти погрози активно переслідують та компрометують інфраструктуру цільового суб'єкта, зберігаючи анонімність. Цільові атаки часто використовують методи, схожі с тими, які можна знайти в традиційних онлайн-загрозах, таких як шкідливі електронні листи, компрометовані чи шкідливі веб-сайти або використання зловмисного програмного забезпечення.

Поширеність способів кібератак на фінансові установи у світі за 2014/18 роки приведено на рис. 2 та рис. 3.

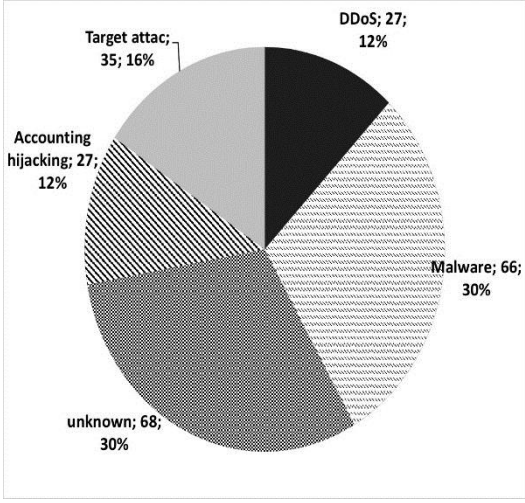

Рисунок 2. – Розподіл типів кібератак на банківські установи у світі, за даними [2]

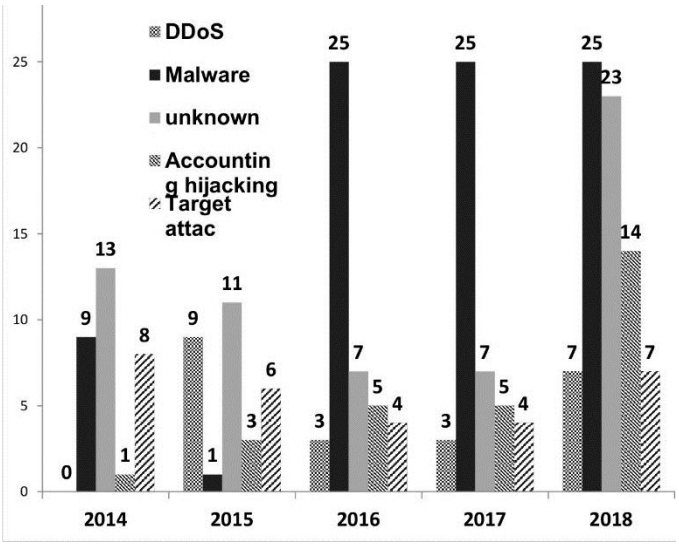

Рисунок 3. – Розподіл типів кібератак на банківські установи у світі по рокам, за даними [2]

Аналізуючи динаміку популярності різних типів атак за останні роки (рис. 3), можна зробити наступні висновки:

— - найбільш поширеними типами кібератак на фінансові установи є атаки, спрямовані на знищення або заволодіння персональних даних клієнтів;

— - останній рік-два спостерігається чітка тенденція, коли метою зловмисників є персональні дані клієнтів.

Такі висновки дають можливість фахівцям з кібербезпеки обгрунтовано формувати стратегії та технології захисту від кібератак для забезпечення стабільної роботи, мінімізації втрат та збереження іміджу кредитно-фінансових установ.

Список використаних джерел

1. Лугановская Е. Противодействие киберпреступности: правила корпоративной защиты [Електронний ресурс] – Режим доступу: https://www.epravda.com.ua/rus/columns/2019/05/15/647756 - Назва з екрану.

2. Сайт терміни та статистика безпеки інформації: HACKMAGEDDON [Електронний ресурс] – Режим доступу: https://www.hackmageddon.com/