МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кіберзахист об’єктів критичної інфраструктури

Лабораторний практикум №1

Оцінювання дієвості політики безпеки на основі аналізу динаміки ризиків

Перевірив:
Войцеховський А. В.

Виконав:
студент І курсу
групи ФБ-41мп
Сахній Н. Р.

Київ 2024

Мета роботи: Опанувати підходи до оцінки дієвості політики безпеки об’єкта критичної інфраструктури. Реалізувати на практиці підхід щодо аналізу поведінки ризиків.

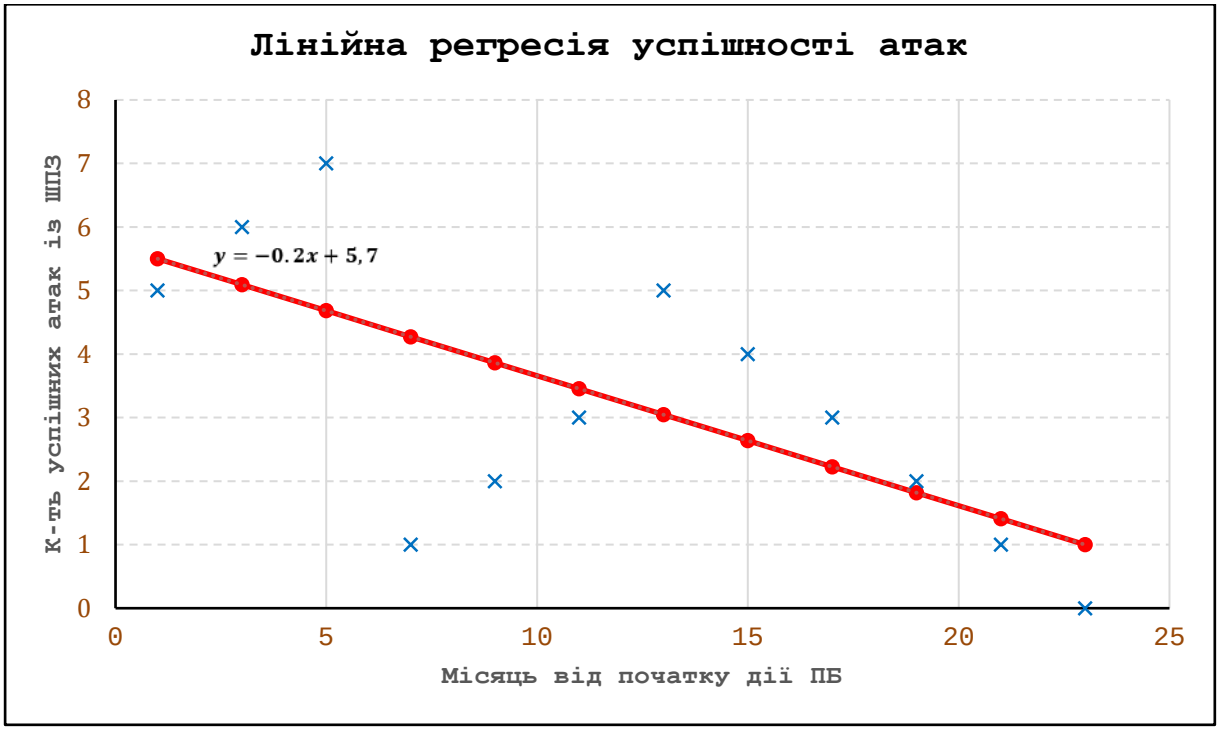
Завдання до виконання:

1. Використовуючи таблицю згідно з варіантом, побудувати залежність у вигляді лінійної регресії (графік) та обчислити відповідні параметри (1)-(6). Обчислити коефіцієнт детермінації та похибку апроксимації (7), (8), зробити висновки про адекватність моделювання та точність.

x – місяць від початку використання політики безпеки, яка оцінюється.

Варіант №5. y – кількість успішних атак з використанням шкідливого ПЗ.

x	1	3	5	7	9	11	13	15	17	19	21	23
y	5	6	7	1	2	3	5	4	3	2	1	0



Параметри лінійної регресії:

(1) $\boldsymbol{a}_{\text{МНК}} = \frac{cov_{x,y}}{\sigma^2} =$ **-0,2**

(2) $\boldsymbol{b} = \acute{y} - a_{\text{МНК}} =$ **5,7**

(3) $\boldsymbol{\acute{x}} = \frac{\sum_{i=1}^{T} x_i}{T} =$ **12 –** середнє значення x

(4) $\boldsymbol{\acute{y}} = \frac{\sum_{i=1}^{T} y_i}{T} =$ **3,25 –** середнє значення y

(5) $\boldsymbol{\sigma^2} = \frac{\sum_{i=1}^{T}(x_i - \acute{x})}{T-1} =$ **52 –** дисперсія

(6) $\boldsymbol{cov_{x,y}} = \frac{\sum_{i=1}^{T}(x_i - \acute{x})(y_i - \acute{y})}{T-1} =$ **-10,64 –** коваріація змінних x та y

Перевірка адекватності моделі:

(7) $\boldsymbol{R^2} = \frac{\sum_{i=1}^{T}(y_i^* - \acute{y})^2}{\sum_{i=1}^{T}(y_i - \acute{y})^2} =$ **0,46 –** коефіцієнт детермінації

(8) $\boldsymbol{\varepsilon} = \frac{1}{T} \cdot \sum_{i=1}^{T} \left| \frac{y_i - y_i^*}{y_i} \right| \cdot 100 =$ **58,44%** – похибка

Маємо, що коефіцієнт детермінації дорівнює 0,46 – значення далеке від 1. Це свідчить про те, що модель не є адекватною, тобто наявний слабкий лінійний зв'язок між **x** та **y**. Похибка становить 58,44%, тому точність моделювання знаходиться на низькому рівні. Хоч на 2-ий рік кількість успішних атак явно пішла на спад, однак на початку 1-го року вона зростала.

2. Зробити висновки про динаміку ризиків: зростаюча, спадаюча.

Загалом динаміка ризиків **спадаюча**, про що свідчить як графік лінійної регресії, так і кількість успішних атак із використанням ШПЗ під кінець періоду оцінювання. Початковий приріст міг бути спричинений активністю зі сторони хакерів націлених на даний об'єкт критичної інфраструктури.

3. Зробити висновки про дієвість політики безпеки та фактори, які можуть впливати на ефективність заходів захисту.

Зважаючи, що метою впровадження політики безпеки було суттєво зменшити кількість успішних атак із використанням шкідливого ПЗ, то можна робити висновки про **її недієвість** відповідно до вимог. Адже подібні зміни мали б стати дієвими миттєво, а не на кінець періоду оцінювання.

Водночас тими **факторами**, що негативно вплинули на ефективність заходів захисту, могли би бути нові TTP (згідно MITRE ATT&CK) від хакерських угрупувань, які експлуатували невідомі “Zero Day”-вразливості.

4. Дати рекомендації, які заходи треба підсилити для покращення ситуації.

Найперше, що потрібно зробити для покращення ситуації – це перевірити наявні системи захисту на предмет відповідності **моделі “Zero Trust”**. Тим самим, всі застарілі рішення необхідно замінити на нові, які мають змогу приймати рішення про нейтралізацію загроз на базі машинного навчання.

Крім того, слід проводити регулярні навчання співробітників з основ кібергігієни, щоб підвищити їх обізнаність про кібератаки, фішингові повідомлення, надійне управління паролями, безпеку при роботі з електронною поштою та інші базові аспекти інформаційної безпеки.

5. Відповісти на контрольні запитання.

- **Які види атак та яким чином можна зареєструвати?**

Для ефективного захисту необхідно впроваджувати комплексні рішення:

IAM (Identity and Access Management) для відслідковування спроб входу в системи з несанкціонованих облікових записів або невідомих IP-адрес.

DLP (Data Loss Prevention) – для запобігання витоку важливих даних.

XDR (Extended Detection and Response) – для об'єднання даних із різних точок кінцевих пристроїв, щоби централізовано реагувати на загрози.

AntiVirus – для захисту робочих станцій та серверів від шкідливого ПЗ, яке може проникати в системи через зйомні пристрої або фішинг.

AntiBot – для виявлення та нейтралізації ботів, які можуть бути використані у DDoS-атаках або для збору інформації з систем ІС.

IDS/IPS (Intrusion Detection/Prevention Systems) – для виявлення та запобігання вторгненням, зокрема на промислові системи управління.

- **Які види атак, на вашу думку, є найбільш типовими для об’єктів критичної інфраструктури.**

Для об'єктів критичної інфраструктури найбільш типовими є такі види: DDoS-атаки, фішингові атаки із використанням ШПЗ, атаки на ICS/SCADA, несанкціоновані спроби доступу/витоку до даних та використання зйомних пристроїв, а також атаки зі сторони APT-груп.

- **Як перевіряється адекватність та точність моделювання?**

Адекватність перевіряється значенням коефіцієнту детермінації близькому до одиниці, а точність – значенням похибки апроксимації.

- **У яких випадках не можна робити висновки про дієвість політики безпеки по регресійній моделі (навіть за умови коефіцієнту детермінації, близького до одиниці)?**

Якщо значення похибки високе, то висновки про дієвість не можливі.

- **Які фактори впливають на дієвість політики безпеки?**
  - Чіткість вимог і правил, щоб політика була зрозумілою та однозначною для всіх співробітників із підтримкою на рівні вище.
  - Регулярне оновлення політики для адаптації під нові загрози;
  - Навчання співробітників необхідне для підвищення обізнаності серед персоналу, аби на максимум запобігти людським помилкам;
  - Використання відповідних технологічних рішень, таких як SIEM-систем, для постійного збору подій та контролю порушень ІБ.

- **Які додаткові критерії можна розглянути при оцінці дієвості заданої політики безпеки.**
  - Як позначаються фінансові вкладення на поведінці ризиків;
  - Наскільки враховано вимоги наявних чеклістів з безпеки;
  - Якими є результати тестування на проникнення за умов ПБ;
  - Наскільки якісно виконуються необхідні організаційні заходи із забезпечення політики безпеки, що були ініційовані керівництвом об’єкта критичної інфраструктури та вимогами законодавства;