АНАЛІЗ СИСТЕМ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ У КОМП'ЮТЕРНІ МЕРЕЖІ

Онищенко Ю. М., Амельницька А. М.
Харківський національний університет внутрішніх справ, Харків, Україна

Ми живемо в епоху інформаційного суспільства, коли інформаційні технології охоплюють усі сфери нашого життя. З появою новітніх технологій, зокрема мережі Інтернет, ми стали вразливі до всілякого роду кібератак[1]. Системи виявлення вторгнень (СВВ) допомагають виявляти атаки та запобігати їх розвитку. Їх можна класифікувати за такими критеріями, як характер відповідної реакції, методиками аналізу та рівнем виявлення атак [2]. В теперішній час найбільше застосування мають такі три групи методів виявлення атак:

- сигнатурні методи;
- методи виявлення аномалій (поведінковий);
- комбіновані методи (використовують спільно алгоритми, визначені в сигнатурних методах і методах виявлення аномалій).

Метою доповіді є аналіз систем виявлення несанкціонованого доступу у комп'ютерні мережі.

В доповіді наводяться результати аналізу СВВ та приклади різноманітних методів виявлення атак на комп'ютерні мережі. [3]. Встановлена основна послідовність дій при виявленні кібератак на комп'ютерні мережі та системи.

Загалом, слід зазначити, що системи виявлення вторгнень допомагають виявити потенційні атаки, які можуть включати в себе вторгнення в мережу, спроби несанкціонованого доступу до системи тощо. Вони відіграють важливу роль у забезпеченні безпеки інформаційних систем та мереж, допомагаючи вчасно реагувати на загрози, попереджати атаки та виявляти їх.

Список літератури

1. Система виявлення вторгнень. Веб-сайт. URL: https://uk.wikipedia.org/wiki/Система_виявлення_вторгнень
2. В. І. Мєшков, В. О. Віролайнен, Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. URL: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf
3. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему / В.В. Бєрковський, О.С. Безсонов. URL: http://nbuv.gov.ua/UJRN/suntz_2017_3_17