УДК 004.77:004.931
Семерюк Т.М.[1], Неласа Г.В.[2]
[1]асп. НУ «Запорізька політехніка»
[2]проф. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

В даний час існує досить багато способів і можливостей отримати управлінням чужим комп'ютеризованим робочим місцем. Написано безліч наукових праць, в яких розглянуті питання виявлення і класифікації атак із застосуванням різних методів. Представляється можливим розділити системи виявлення атак на локальні і мережеві. Виходячи з того, до якого виду належить атака, приймається рішення, який програмний продукт доцільно застосувати в тій чи іншій ситуації. Для мережевих систем виявлення атак характерним є контроль і аналіз трафіку, що циркулює в локальній мережі.

Типова структура інформаційної атаки має комплексну складну організацію, виявлення і розпізнання якої простим способом буває неможливо. В свою чергу в мережевому середовищі кожен проаналізований пакет буде давати деяку корисну частину (порцію) інформації, яку аналітична система виявлення атак може використовувати для оцінки контролю над поточною ситуацією в мережевому середовищі, прогнозування комп'ютерних загроз з метою їх запобігання, можливості припинення дій порушника за результатами виявлених слідів або спроб вчинення зловмисних дій порушника [1].

Для виявлення комплексних атак необхідний аналіз різного роду джерел інформації і пошуку взаємозв'язку між виявленими простими атаками. Як засіб захисту автоматизованих інформаційних систем виступає система виявлення атак (СВА). В якості підстави для формування ознак виявлення атак може бути застосована політика безпеки автоматизованих інформаційних систем. З огляду на особливості таких систем, політика безпеки як описує модель внутрішнього порушника і внутрішніх загроз в мережі, так і містить зовнішній ресурс для інформаційних систем - модель зовнішніх загроз і поведінковий характер автоматизованої інформаційної системи в цілому.

Приватні політики, які входять до складу політики безпеки, описують параметри і критерії безпеки класів ресурсів автоматизованої інформаційної системи, підлягають захисту. Політика безпеки являє інформацію, потрібну для формування ознак виявлення простих атак, враховуючи при цьому особливості автоматизованих інформаційних систем.

Для досягнення поставлених цілей виникають завдання формалізації ознак виявлення атак, які можуть бути отримані з положень політики безпеки, розробки алгоритму виявлення комплексних атак на основі цих ознак. Для вирішення проблеми виявлення мережевих атак можна використовувати такі методи: агентний підхід, розробку спеціального програмного забезпечення, використання штучного інтелекту, впровадження імунних інформаційних моделей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Selin R.N., Churilov S.A. Prognosys method for computer attacks explication // Известия ЮФУ. Технические науки.-2011.-№2 (115). – С. 233-237.