АКАДЕМІЯ ТЕХНІЧНИХ НАУК УКРАЇНИ

IV Міжнародна науково-практична конференція

ПРИКЛАДНІ НАУКОВО-ТЕХНІЧНІ ДОСЛІДЖЕННЯ

1-3 квітня 2020

У двох томах

Том 1

АКАДЕМІЯ ТЕХНІЧНИХ НАУК УКРАЇНИ
ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. ВАСИЛЯ СТЕФАНИКА
ІВАНО-ФРАНКІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ НАФТИ І ГАЗУ
УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ
НАЦІОНАЛЬНИЙ ЛІСОТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
CONNECTIVE TECHNOLOGIES LTD (ВЕЛИКОБРИТАНІЯ)

ПРИКЛАДНІ НАУКОВО-ТЕХНІЧНІ ДОСЛІДЖЕННЯ

APPLIED SCIENTIFIC AND TECHNICAL RESEARCH

Матеріали IV міжнародної науково-практичної конференції

(1–3 квітня 2020 р., м. Івано-Франківськ)

У двох томах
Том 1

Партнер конференції:

ІВФ “Темпо”
http://tempo-temp.com.ua/

Івано-Франківськ
ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»
2020

УДК 60
ББК 30
П75

ПРИКЛАДНІ НАУКОВО-ТЕХНІЧНІ ДОСЛІДЖЕННЯ

Матеріали IV міжнародної науково-практичної конференції

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ:

П75 **Прикладні** науково-технічні дослідження : матеріали IV міжнар. наук.-прак. конф., 1–3 квіт. 2020 р., м. Івано-Франківськ / Академія технічних наук України. Івано-Франківськ : ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», 2020. Т. 1. 236 с.
ISBN 978-966-640-483-4

У збірнику надруковано матеріали IV міжнародної науково-практичної конференції «Прикладні науково-технічні дослідження».

Для студентів, аспірантів, викладачів ЗВО та наукових організацій.

УДК 60
ББК 30

ISBN 978-966-640-483-4

УДК 621.391

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

д.т.н. ***Штомпель М.А.****, Український державний університет залізничного транспорту, м. Харків*

Вступ. Перехід до інформаційного суспільства в Україні вимагає постійного розвитку телекомунікаційної інфраструктури шляхом удосконалення методів передавання, обробки та захисту інформації. При цьому суттєво зростає роль захищених телекомунікаційних мереж, що забезпечують задані показники конфіденційності, цілісності, надійності тощо. Побудова даних мереж повинна здійснюватися на основі системного підходу на нормативно-законодавчому, адміністративному, процедурному та програмно-технічному рівнях для забезпечення високого ступеню інформаційної безпеки. Однією з важливих задач при реалізації програмно-технічного комплексу захищених телекомунікаційних мереж є створення ефективних механізмів та засобів аналізу виявлення вторгнень на основі різноманітних правил та принципів, зокрема математичного апарату нейронних мереж.

Виклад матеріалу. При виявленні вторгнень у телекомунікаційних мережах можна використовувати такі підходи: виявлення аномальної поведінки; виявлення зловмисної поведінки; комбінований підхід. У першому випадку ворожа дія (аномалія) розглядається як відхилення від нормальної (типової) поведінки, наприклад, збільшення трафіку у мережі, зростання навантаження на мережевий вузол тощо. Для реалізації систем виявлення аномальної поведінки необхідно створити профіль об’єкту та визначити граничні значення характеристик та параметрів об’єкту. З іншого боку, системи виявлення зловмисної поведінки засновані на порівнянні поточних показників об’єкту з наявним набором сигнатур вторгнень, що дозволяє значно знизити складність їх технічної реалізації.

При побудові сучасних систем виявлення вторгнень разом з традиційними методами (статистичний аналіз, експертні системи тощо) застосовуються інтелектуальні методи (нейронні мережі, генетичні алгоритми тощо), що є універсальними через можливість їх використання як у системах першого, так і другого виду.

Проведений аналіз показав, що нейронні мережі як механізм виявлення вторгнень характеризується гнучкістю, швидкодією, здатністю до навчання (адаптивністю), можливістю роботи з неповними та/або неточними даними. При цьому існує проблема вибору конкретної моделі, параметрів та методу навчання нейронної мережі в залежності від типу системи виявлення вторгнень та наявних вимог до неї. Некоректний вибір даних складових може привести до неповного та/або неточного навчання нейронної мережі, зниження збіжності, потрапляння в локальні мінімуми обраної цільової функції тощо.

При реалізації систем виявлення аномальної поведінки нейронні мережі навчаються заданий період часу шляхом аналізу нормальної роботи телекомунікаційної мережі, після чого використовується режим розпізнавання (класифікації) та у випадку наявності нетипової поведінки об’єкту фіксується факт вторгнення.

У системах виявлення зловмисної поведінки нейронні мережі навчаються на обраних сигнатурах вторгнень різних класів. У подальшому у режимі розпізнавання (класифікації) нейронна мережа здійснює аналіз поведінки об’єкту та його віднесення до деякого класу вторгнень.

Висновки. Для підвищення ефективності систем виявлення вторгнень доцільно використовувати нейромережеві методи, що виступають у ролі універсального класифікатору. Якість роботи нейронної мережі залежить від обраних параметрів, методу навчання та обраної навчальної множини, що містить зразки типової поведінки телекомунікаційної мережі або обрані сигнатури вторгнень. Перспективним напрямом подальших досліджень є порівняння ефективності різних моделей нейронних мереж при побудові систем виявлення вторгнень у телекомунікаційних мережах різного призначення.

Наукове видання

Мови видання: українська, англійська

ПРИКЛАДНІ НАУКОВО-ТЕХНІЧНІ ДОСЛІДЖЕННЯ

Матеріали IV міжнародної науково-практичної конференції

(1–3 квітня 2020 р., м. Івано-Франківськ)

Доповіді друкуються у авторській редакції.

Організаційний комітет не завжди поділяє позицію авторів.

За точність викладеного матеріалу відповідальність покладається на авторів.

Головний редактор *В.М. Головчак*
Оформлення і комп'ютерна верстка *М.В. Кузь*

Підп. до друку 30.03.2020 р. Формат 60x84/16.
Папір офс. Друк цифровий. Гарн. Times new Roman.
Умовн. друк. арк. 10,46. Наклад 400 пр.

Видавець
Прикарпатський національний університет
імені Василя Стефаника
76025, м. Івано-Франківськ,
вул. С. Бандери, 1, тел.: 71-56-22
E-mail: vdvcit@pu.if.ua
Свідоцтво суб'єкта видавничої справи ДК № 2718 від 12.12.2006

Виготовлювач
ФОП Семко Я.Ю.
76019, м. Івано-Франківськ, вул. Крайківського, 2
тел. +38-067-342-56-46
Свідоцтво суб'єкта видавничої справи ДК № 3312 від 12.11.2008

ISBN 978-966-640-483-4