www.konferenciaonline.org.ua

Міжнародна наукова інтернет-конференція

Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення

Випуск 94

ISSN 2522-932X

Google Scholar

AKADEMIA NAUK STOSOWANYCH
WYŻSZA SZKOŁA ZARZĄDZANIA I ADMINISTRACJI W OPOLU

11-12 грудня 2024 р.

м. Тернопіль, Україна – м. Ополе, Польща
2024

УДК 001 (063)

Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 94)*:* матеріали Міжнародної наукової інтернет-конференції, (м. Тернопіль, Україна, м. Ополе, Польща, 11-12 грудня 2024 р.) / редкол. : О. Патряк та ін. ГО “Наукова спільнота”, WSZIA w Opolu. Тернопіль : ФО-П Шпак В.Б. 2024. 154 с. – ISSN 2522-932X

Збірник доповідей підготовлено за матеріалами Міжнародної наукової інтернет-конференції (випуск 94) 11-12 грудня 2024 р. на сайті www.konferenciaonline.org.ua

Наша адреса: Оргкомітет МНІК "Конференція онлайн"
а/с 797, м. Тернопіль 46005
тел. моб. 068 366 0 525
e-mail: inetkonf@ukr.net

URL Інтернет-конференції: http://www.konferenciaonline.org.ua/
ISSN 2522-932X

Environmental Technology, 2021, 22 (6), P. 1-10. DOI: https://doi.org/10.12912/27197050/141895 (дата звернення: 30.11.2024).
5. Пацев І. С., Барабаш О. В., Пацева І. Г. Вплив воєнних дій на лісові екосистеми Житомирщини. *Екологічні науки*. 2023. Вип. 5 (50). С. 114-118.
6. Барабаш О. В. Екологія земноводних та плазунів Опілля : автореф. дис. … канд. біол. наук : 03.00.16. Чернівці, 2002. 20 с.
7. Літопис природи Національного природного парку «Синьогора»: у Томі ІІ, 2023. 370 с.

Хома Надія Григорівна,
кандидат фізико-математичних наук, доцент,
Західноукраїнський національний університет, м. Тернопіль

Цинайко Василь Петрович, *студент,*
Західноукраїнський національний університет, м. Тернопіль

БЕЗПЕКА В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Інтернет-адреса публікації на сайті:
http://www.konferenciaonline.org.ua/ua/article/id-1999/

Інформаційна безпека є однією з ключових складових сучасних інформаційних систем. З огляду на стрімкий розвиток технологій та зростання обсягів цифрових даних, питання інформаційної безпеки набувають критичного значення. Такі загрози, як шкідливе програмне забезпечення, несанкціонований доступ, соціальна інженерія та кібератаки, постійно змінюються та ускладнюються, створюючи нові виклики для організацій та користувачів. Як наслідок, з'являються нові методи та засоби захисту для збереження конфіденційності, цілісності та доступності даних. Роль інформаційної безпеки виходить далеко за межі технічних аспектів і включає в себе управління ризиками, побудову корпоративної культури безпеки та навчання користувачів. Особливе значення має людський фактор, оскільки навіть найсучасніша система безпеки схильна до людських помилок і недбалості. Тому ефективний захист інформації вимагає комплексного підходу, який охоплює як технічні, так і організаційні заходи.

Загрози інформаційній безпеці існують у різних формах, з різним впливом і наслідками для користувачів та організацій. Однією з найпоширеніших загроз є шкідливе програмне забезпечення, або те, що часто називають вірусами. Іншою важливою загрозою є фішинг – техніка соціальної інженерії, яка використовується для того, щоб обманом змусити користувачів розкрити конфіденційну інформацію, таку як паролі, номери банківських карток або особисті дані. Шахраї часто видають себе за представників державних органів, надсилаючи фальшиві повідомлення або створюючи підроблені веб-сайти, які виглядають як справжні. Фішинг залишається одним з найефективніших методів шахрайства, оскільки багато користувачів не перевіряють достовірність джерел.

DDoS-атаки (Distributed Denial of Service – розподілена відмова в обслуговуванні) є одним з найнебезпечніших видів атак. Їхньою метою є перевантаження серверів та іншої мережевої інфраструктури величезною кількістю запитів, що призводить до відмови в обслуговуванні та тимчасової недоступності сервісів у відповідь. Такі атаки часто здійснюються для того, щоб порушити роботу компанії чи організації або відвернути увагу від інших видів хакерських атак. Злом паролів та інші форми несанкціонованого доступу також становлять серйозну загрозу інформаційній безпеці. Зловмисники можуть використовувати прості і складні паролі та незахищені мережі, щоб отримати доступ до облікових записів користувачів. Це особливо актуально для організацій, де використання надійних паролів і багаторівневої автентифікації залишається недостатнім. Багато даних втрачається саме через те, що користувачі не можуть захистити свої облікові записи. Таким чином, загрози інформаційній безпеці численні і продовжують змінюватися з розвитком технологій. Важливо розуміти ці ризики і мінімізувати потенційні втрати, впроваджуючи відповідні захисні заходи [1, 2].

Методи та засоби інформаційної безпеки є важливими інструментами для боротьби із загрозами, які можуть пошкодити дані або поставити під загрозу конфіденційність та безперервність систем. Одним з найважливіших методів є шифрування даних, яке забезпечує захист даних під час передачі через мережі та зберігання. Шифрування перетворює дані в зашифрований формат, який не може бути прочитаний третіми особами без спеціального ключа. Це важливо як для особистих даних користувача, так і для конфіденційних даних організації. Не менш важливим заходом безпеки є система автентифікації, яка гарантує, що тільки авторизовані особи можуть отримати доступ до даних. Одним з найефективніших методів є багатофакторна автентифікація, яка вимагає декількох рівнів перевірки, включаючи паролі та коди, що надсилаються на мобільні телефони.

Іншим важливим аспектом захисту є брандмауер (або файрволи), який контролює вхідний та вихідний мережевий трафік. Вони блокують небажані запити та доступ до потенційно небезпечних ресурсів. Брандмауери допомагають відстежувати і блокувати шкідливий трафік і знижують ризик атак на систему ззовні [3].

Антивірусне програмне забезпечення також є одним з основних засобів захисту, який допомагає виявляти та нейтралізувати шкідливі програми. Сучасний антивірус завжди може сканувати файли, завантажувані файли та веб-сайти, до яких звертаються користувачі, для роботи в режимі реального часу. Це важливий крок для запобігання зараженню вашої системи вірусами, троянами або шпигунськими програмами.

Окрім технічних засобів, ефективний захист інформації також вимагає навчання персоналу та розробки політики безпеки. Поширені випадки витоку інформації відбуваються через помилки і невігластва співробітників. Саме тому організації проводять навчання з питань безпеки і розробляють чіткі правила поводження з конфіденційною інформацією, використання паролів і реагування на підозрілі дії [4].

Тому для забезпечення інформаційної безпеки необхідний комплексний підхід, що включає як технічні засоби, так і освітні заходи для користувачів, і тому інформаційна безпека є важливим елементом сучасних інформаційних систем, особливо хмарних технологій. Складність загроз даним і системам вимагає багаторівневого підходу до захисту, що поєднує технічні та організаційні заходи. Шифрування даних, багатофакторна автентифікація, контроль доступу та періодичні перевірки безпеки є ключовими компонентами надійного захисту, які ефективно протидіють несанкціонованому доступу, витоку даних та іншим кібератакам.

Література:

1. https://infocom.ua/services-for-business/data-security/infoddos/?gad_source=1&gclid=Cj0KCQiAlsy5BhDeARIsABRc6Zt9ZMHrfg5cQ9gyOz4j_dlzFN1qqrftbUuzSb2dUdfCL1GcJSCBsbkaAo8vEALw_wcB
2. https://thekernel.ua/wp-content/uploads/2023/02/10-поширених-типів-кібератак.pdf
3. https://mediacom.com.ua/rol-brandmauera-v-osobistij-kiberbezpetsi/
4. https://iitd.com.ua/news/najkrashhi-praktiki-zahistu-hmarnih-shovishh/

***Хрунь Христина Богданівна**, магістр,*
Західноукраїнський національний університет, м. Тернопіль

ПРОГНОЗУВАННЯ ФІНАНСОВИХ ПОКАЗНИКІВ ЗА ДОПОМОГОЮ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Інтернет-адреса публікації на сайті:
http://www.konferenciaonline.org.ua/ua/article/id-1991/

Задача прогнозування фінансових показників за допомогою згорткових нейронних мереж (ЗНМ) вимагає комплексного підходу, який поєднує знання з фінансового аналізу, обробки великих даних [1] і глибокого навчання [2]. Концептуальні основи вирішення цієї задачі включають наступні ключові елементи:

1. Аналіз фінансових часових рядів.

Фінансові показники, зокрема ціни акцій, обсяги торгів, індекси та інші ринкові дані, часто є часовими рядами. Такі дані мають складну структуру з прихованими трендами, сезонними коливаннями і випадковими коливаннями. Основним завданням аналізу часових рядів є виявлення цих патернів і використання їх для прогнозування. Фінансові дані часто характеризуються високим рівнем шуму та нестабільністю, що вимагає особливих підходів до обробки і виділення значущих ознак.

2. Використання згорткових нейронних мереж для виділення ознак.

ЗНМ є потужними інструментами для автоматичного виділення ознак з даних, зокрема для часових рядів. Використання ЗНМ дозволяє моделі автоматично вивчати та виділяти складні локальні патерни в часових рядах,

Зміст

Секція 1. Інформаційні системи і технології

Наукове видання

«Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення»
Рік заснування – 2011

Видання виходить 11 разів на рік

Відповідальний за випуск *У.О. Русенко*
Комп'ютерне верстання *О.В. Ковальський*

Підписано до друку 19.12.2024
Формат 60х84/16. Папір офсетний. Друк на дублікаторі.
Умов.-друк. арк. 4,5. Обл.-вид. Арк 4,95.
Тираж 50 прим.

Віддруковано ФО-П Шпак В.Б.
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції серія ДК№7599 від 10.02.2022р.
Тел. 097 299 38 99
E-mail: tooums@ukr.net