Національний університет оборони
Азербайджанської республіки

Національний технічний університет
"Харківський політехнічний інститут"

Харківський національний
університет радіоелектроніки

Національний аерокосмічний університет
імені М. Є. Жуковського
"Харківський авіаційний інститут"

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей одинадцятої міжнародної
науково-технічної конференції

16 – 17 листопада 2023 року

Том 4: секції 3, 4

(додаткові тези)

Баку – Харків – Бельсько-Бяла –2023

УДК 004 : 681.3 doi: https://doi.org/10.32620/PI.23

У збірнику подано тези доповідей одинадцятої міжнародної науково-технічної конференції "Проблеми інформатизації". Розглянуті питання за такими напрямами: інформатизація навчального процесу; застосування, експлуатація та безпека функціонування телекомунікаційних систем та мереж; комп'ютерні методи і засоби інформаційних технологій та управління; методи швидкої та достовірної обробки даних в комп'ютерних системах та мережах; цивільна безпека (інформаційна підтримка); сучасні інформаційно-вимірювальні системи.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Azerbaijan National Defence University

National Technical University
Kharkiv Polytechnic Institute

Kharkiv National University
of Radio Electronics

National Aerospace University
Kharkiv Aviation Institute

University of Bielsko-Biala

PROBLEMS OF INFORMATIZATION

Proceedings of 11-th international
scientific and technical conference
November 16 – 17, 2023

VOLUME 4: SECTIONS 3, 4

Baku – Kharkiv – Bielsko-Biala –2023

UDC 004 : 681.3 doi: https://doi.org/10.32620/PI.23

The collection presents abstracts of reports of the eleventh international scientific and technical conference "Problems of Informatization". Issues in the following areas are considered: informatization of the educational process; application, operation and safety of telecommunication systems and networks; computer methods and means of information technology and management; methods of fast and reliable data processing in computer systems and networks; civil security (information support); modern information and measurement systems.

ORGANIZING COMMITTEE

Одинадцята міжнародна науково-технічна конференція "Проблеми інформатизації" проводиться 16 та 17 листопада 2023 року в режимі ONLINE.

Тези доповідей доступні в INTERNET.

ТОМ 1

СЕКЦІЯ 1. Інформатизація навчального процесу.

Керівник секції: д.т.н. проф. В. М. Рудницький, ДНДІ ВС ОВТ, Черкаси.
Секретарка секції: к.т.н. Н. В. Лада, ДНДІ ВС ОВТ, Черкаси.

СЕКЦІЯ 2. Застосування та експлуатація телекомунікаційних систем та мереж.

Керівниця секції: д.т.н. проф. Н. Г. Кучук, НТУ «ХПІ», Харків.
Секретар секції: к.т.н. доц. С. С. Бульба, НТУ «ХПІ», Харків.

СЕКЦІЯ 5. Методи швидкої та достовірної обробки даних в комп'ютерних системах та мережах.

Керівник секції: д.т.н. проф. В. А. Краснобаєв, ХНУ, Харків.
Секретарка секції: к.т.н. О. М. Бельорін-Еррера, НТУ «ХПІ», Харків.

СЕКЦІЯ 7. Сучасні інформаційно-вимірювальні системи.

Керівник секції: д.т.н. проф. О. В. Коломійцев, НТУ «ХПІ», Харків.
Секретар секції: к.т.н. доц. А. О. Подорожняк, НТУ «ХПІ», Харків.

ТОМ 2

СЕКЦІЯ 3. Безпека функціонування телекомунікаційних систем та мереж.

Керівник секції: д.т.н. проф. О. О. Можаєв, ХНУВС, Харків.
Секретар секції: к.т.н. доц. О В. Сєвєрінов, ХНУРЕ, Харків.

СЕКЦІЯ 6. Цивільна безпека та захист критичної інфраструктури.

Керівник секції: д.т.н. доц. О. В. Третьяков, НАУ, Київ.
Секретар секції: к.т.н. доц. Є В. Доронін, НАУ, Київ.

ТОМ 3

СЕКЦІЯ 4. Комп'ютерні методи і засоби інформаційних технологій та управління.

Керівники секції: д.т.н. проф. І. В. Рубан, ХНУРЕ, Харків.
д.т.н. проф. А. А. Коваленко, ХНУРЕ, Харків.
Секретар секції: к.т.н. доц. О. С. Ляшенко, ХНУРЕ, Харків.

ТОМ 4

СЕКЦІЇ 3, 4. Додаткові тези.

СЕКЦІЯ 3
БЕЗПЕКА ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н. проф. О. О. Можаєв, ХНУВС, Харків
Секретар секції: к.т.н. доц. О В. Сєвєрінов, ХНУРЕ, Харків

БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ У СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Показій К. О., Лященко В. О., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний розвиток телекомунікаційних мереж характеризується стрімким зростанням кількості підключених пристроїв та обсягу передаваних даних. Це створює нові виклики для забезпечення безпеки та конфіденційності інформації. Основні загрози безпеці включають несанкціонований доступ, витоки даних, атаки типу «людина посередині» та інші [1]. З ростом цифрової інтеграції та глобалізації, телекомунікаційні мережі стають основою для багатьох аспектів нашого повсякденного життя, від особистого спілкування до бізнес-операцій. Наприклад, зловмисники можуть використовувати слабкі місця в мережевій інфраструктурі для проведення масштабних DDoS-атак або для отримання доступу до конфіденційної інформації. Тому, поряд з технологічними рішеннями, важливо розглядати і людський фактор: навчання персоналу, формування культури безпеки серед користувачів та розуміння потенційних загроз може стати ключем до забезпечення надійності та безпеки в сучасних телекомунікаційних мережах.[2].

Метою доповіді є аналіз сучасних загроз безпеки в телекомунікаційних мережах та розробка рекомендацій щодо їх протидії. Особлива увага приділяється питанням конфіденційності передаваних даних та захисту від несанкціонованого доступу.

У доповіді висвітлено рекомендовані стратегії безпеки для розширення телекомунікаційних мереж, що враховують зростання кількості підключених пристроїв та об'ємів передачі даних. Ключова увага надається використанню інтегрованого підходу у захисті, який охоплює криптографію, аутентифікацію та стратегій реагування.

Список літератури

1. Петров О. О. Методи захисту інформації в телекомунікаційних системах. Телекомунікаційні технології / О. О. Петров, В. І. Литвиненко. – 2017. – №2. – С. 45–50.

2. Левченко І. П., Сергієнко А. В. Системи ідентифікації та аутентифікації користувачів в сучасних телекомунікаційних мережах. Безпека інформації. 2019. Т. 7, № 3. С. 33–38.

ВПЛИВ СОЦІАЛЬНО-ІНЖЕНЕРНИХ АТАК НА БЕЗПЕКУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Лященко В. О., Показій К. О., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Соціально-інженерні атаки стають все більш поширеними у сучасному цифровому світі, цілеспрямовано впливаючи на людський фактор для отримання несанкціонованого доступу до інформаційних систем. Телекомунікаційні системи, які є важливою частиною інфраструктури будь-якої країни, не є винятком і можуть стати мішенями для таких атак [1]. Аналіз сучасних методів соціально-інженерного обману, таких як фішинг, відмова в обслуговуванні, імітація особи, дозволяє розробляти ефективні стратегії захисту та протидії цим загрозам [2].

Однією з основних причин успіху соціально-інженерних атак є недостатнє інформування та освіта користувачів щодо потенційних загроз та способів їх виявлення.

Незважаючи на технологічний прогрес та розвиток захисних систем, людина залишається найбільш уразливим елементом в будь-якій інформаційній системі. Тому важливо не лише вдосконалювати технічні засоби захисту, але й проводити регулярні навчальні семінари та тренінги для співробітників.

Залучення персоналу до процесу забезпечення безпеки, формування у них культури цифрової обережності та розуміння основних принципів кібергігієни може стати ключовим фактором у протидії соціально-інженерним атакам.

Такий підхід дозволить не лише знизити ризик компрометації систем, але й підвищити загальний рівень кібербезпеки в організації.

Метою доповіді є вивчення механізмів реалізації соціально-інженерних атак та розробка рекомендацій для підвищення рівня безпеки телекомунікаційних систем.

В доповіді представлені результати досліджень з вивчення методів соціально-інженерного обману, а також практичні рекомендації щодо їх виявлення та нейтралізації.

Список літератури

1. Гончарук О. В. Безпека інформації. / О. В. Гончарук // Соціальна інженерія як загроза безпеці інформаційних систем. / О. В. Гончарук., 2019. – (2). – С. 35–40.

2. Сергієнко І. М., Черненко Ф. О. Методи захисту від соціально-інженерних атак в телекомунікаційних мережах. Кібербезпека: освіта, наука, техніка. 2020. Т. 3, № 1. С. 44–49.

КОНЦЕПЦІЯ 'ZERO TRUST' У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙ

Показій К. О., Лященко В. О., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Концепція 'Zero Trust' стає ключовою у сучасних умовах зростання кількості кіберзагроз. Основний принцип цієї концепції полягає у тому, що жоден користувач або пристрій не має довіри за замовчуванням, незалежно від того, звідки вони підключаються до мережі. Це означає, що кожен спроба доступу до ресурсів мережі має бути перевірена, аутентифікована та авторизована.

Впровадження стратегії 'Zero Trust' допомагає підприємствам забезпечити високий рівень безпеки від несанкціонованого доступу, атак та інших загроз.

Основні компоненти цієї стратегії включають ідентифікацію користувача, застосування принципу найменших привілеїв та постійний моніторинг мережевого трафіку.

Однією з ключових переваг концепції 'Zero Trust' є гнучкість та адаптивність до змінних умов кіберзагроз. У традиційних мережевих моделях, внутрішні ресурси часто розглядалися як "довірені", тоді як зовнішній світ був "недовірливим".

Однак з ростом мобільних, хмарних технологій та Інтернету речей, межа між внутрішніми та зовнішніми ресурсами стає все менш визначеною [1].

Метою доповіді є аналіз принципів та методів впровадження концепції 'Zero Trust' у телекомунікаційних системах, а також розгляд її переваг та можливих викликів.

У доповіді розглянуто сучасні технології та інструменти, які допомагають підприємствам впроваджувати стратегію 'Zero Trust'. Вона також містить практичні рекомендації щодо її ефективного застосування. Однією з ключових рекомендацій є постійне оновлення програмного та апаратного забезпечення. Це допоможе мінімізувати ризик виникнення вразливостей, які можуть бути використані зловмисниками для отримання доступу до мережі.

Крім того, підприємствам слід регулярно проводити аудит безпеки для виявлення можливих слабких місць [2].

Список літератури

1. Мельник І. П., Шевченко О. Ю. Аналіз методів аутентифікації в мережах 'Zero Trust'. Безпека інформації. 2021. Т. 7, № 3. С. 22–28.
2. Білоконь А. В., Лисенко О. І. Стратегії захисту в сучасних телекомунікаційних мережах. Телекомунікаційні системи. 2020. Т. 5, № 2. С. 45–50.

РОЗРОБКА МУЛЬТИМЕДІЙНОГО КУРСУ З КІБЕРБЕЗПЕКИ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ

Онищенко Ю. М., Муллалієва Д. С.
Харківський національний університет внутрішніх справ, Харків, Україна

Актуальність кібербезпеки в сучасному світі надзвичайно висока, оскільки кіберзагрози та кібератаки постійно зростають у складності та масштабах. Відсутність належного захисту може призвести до серйозних наслідків для корпорацій, державних структур та громадян. Узагальнена статистика підтверджує цю тенденцію.

За даними Звіту про кібербезпеку Verizon за 2022 рік [1], порівняно з 2021 роком кількість атак програм-вимагачів в 2022 році зросла на 13%, що є значним збільшенням, якщо порівняти цей відсоток з останніми 5 роками разом [2].

Стосовно України, протягом 2022 року Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2021 році.

Кількість подій інформаційної безпеки в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником» зросла у 18,3 та 2,2 рази відповідно [3].

Ця статистика вказує на необхідність надійного навчання та підготовки фахівців у галузі кібербезпеки для подолання зростаючих загроз та ефективного захисту інформації та інфраструктури в сучасному цифровому середовищі.

У цьому контексті розробка мультимедійного курсу з кібербезпеки на платформі вебсайту є актуальним завданням, адже має низку переваг:

1. Збільшення обізнаності: здобувачі вищої освіти можуть швидко ознайомитися зі змінами в кіберзагрозах та відповідних стратегіях захисту, відвідавши даний вебсайт.
2. Реалістичне навчання: мультимедійні ресурси на вебсайті дозволяють створити ситуації, що імітують реальні кібератаки, допомагаючи здобувачам вищої освіти розвивати практичні навички в області кібербезпеки, користуючись вебплатформою.
3. Гнучке навчання: здобувачі вищої освіти можуть навчатися у власному темпі, вибираючи час і місце для навчання, і отримувати доступ до матеріалів з будь-якого пристрою з підключенням до Інтернету.
4. Оновлення змісту: вебсайт можна легко оновлювати, щоб відображати нові загрози та стратегії захисту, забезпечуючи постійно актуальну інформацію.
5. Візуалізація складних концепцій: мультимедійний формат дозволяє візуалізувати складні кібербезпекові концепції, діаграми та графіки, що полегшує розуміння матеріалу і покращує сприйняття інформації.

6. Інтерактивність: мультимедійні курси можуть включати інтерактивні вправи, вікторини та завдання, що допомагають здобувачам вищої освіти активно залучатися до навчання та встановлювати практичні навички.

7. Можливість дистанційного навчання: мультимедійний курс може бути доступним онлайн, що дозволяє здобувачам вищої освіти навчатися з будь-якого місця і в будь-який час, зменшуючи географічні та часові обмеження.

8. Персоналізоване навчання: мультимедійні курси можуть враховувати індивідуальні потреби здобувачів вищої освіти, надаючи можливість обирати шляхи навчання та фокусуватися на конкретних аспектах кібербезпеки.

9. Відстеження прогресу: платформа мультимедійного курсу може надавати звіти про прогрес здобувачаів вищої освіти, що допомагає науково-педагогічним працівникам, тренерам та інструкторам в оцінці успішності та адаптації курсу.

10. Ефективне поширення інформації: мультимедійний курс може бути легко поширюваним та доступним для широкої аудиторії, що сприяє розповсюдженню знань та навичок в області кібербезпеки.

Отже, розробка та впровадження мультимедійного курсу з кібербезпеки на вебсайті є необхідним етапом для зміцнення знань та навичок у цій надважливій галузі, щоб забезпечити надійний захист від кіберзагроз і зберегти цифрову безпеку в нашому сучасному глобалізованому світі.

Список літератури

1. Джерело: Verizon. (2022). 2022 Data Breach Investigations Report. [Посилання на джерело: https://enterprise.verizon.com/resources/reports/dbir/] (дата звернення: 10.11.2023)

2. https://blog.desdelinux.net/uk/segun-el-informe-de-2022-de-verizon-el-ransomware-aumento-un-13-en-comparacion-con-el-ano-pasado/ (дата звернення: 10.11.2023)

3. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України, https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit (дата звернення: 10.11.2023)

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

ДОСЛІДЖЕННЯ ПРИНЦИПІВ РОБОТИ МЕТАМОРФНИХ ВІРУСІВ

Гнусов Ю. В., Павленко О. В.
Харківський національний університет внутрішніх справ, Харків, Україна

Розвиток нових інформаційних технологій і загальна комп'ютеризація призвели до того, що інформаційна безпека не тільки стає обов'язковою, вона ще й одна з характеристик інформаційних систем. Існує досить великий клас систем обробки інформації, при розробці яких фактор безпеки відіграє першорядну роль [1].

З кожним днем віруси стають все більш витонченими, що призводить до істотної зміни профілю загроз. Але і ринок антивірусного програмного забезпечення не стоїть на місці, пропонуючи безліч продуктів. Їх користувачі, представляючи проблему лише в загальних рисах, нерідко втрачають важливі нюанси і в підсумку отримують ілюзію захисту замість самого захисту [1].

Незважаючи на прийняті в багатьох країнах закони про боротьбу з комп'ютерними злочинами і розробку спеціальних програмних засобів захисту від вірусів, кількість нових програмних вірусів постійно росте. Це вимагає від користувача персонального комп'ютера знань про природу вірусів, способи зараження вірусами і захисту від них [2].

Метою доповіді є побудова аналізу антивірусних програм, які спроможні знайти метаморфний вірус.

В доповіді наводяться результати аналізу антивірусних пакетів. В процесі проведення аналізу були успішно вирішені завдання, поставлені на початку роботи. Так були вивчені поняття ІБ, комп'ютерних вірусів та антивірусних засобів, визначені види загрози безпеки інформації, методи захисту, розглянуто класифікацію КВ и антивірусних програм и проведено аналіз антивірусних пакетів на предмет знаходження метаморфних вірусів, написана програма, яка виробляє поиск заражених файлів. Результати, отримані в процесі роботи можуть буть застосовані при виборі антивірусного засобу.

Варто відзначити, що універсальної антивірусної програми не існує. Жодна з них не може гарантувати нам 100% захисту від вірусів, та багато в чому вибір антивірусної програми залежить від самого користувача.

Список літератури

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

2. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері. Підручник/ [Цуранов М.В., Струков В.М., Пєвнєв В.Я.] Харків: ХНУВС, 2015. 256 с.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ МОНІТОРИНГУ ПІДОЗРІЛОЇ АКТИВНОСТІ В КОРПОРАТИВНИХ МЕРЕЖАХ

Цуранов М. В., Попов О. О.
Харківський національний університет внутрішніх справ, Харків, Україна

Сучасний світ неможливо уявити без засобів комунікацій та обчислювальної техніки. Інформаційні технології розвиваються дуже швидко, охоплюючи все більше областей людської діяльності. Тому безпека інформаційних технологій є одним з найважливіших аспектів забезпечення їх функціонування. Україна як і весь світ намагається не відставати від сучасних тенденцій у сфері інформаційних технологій. Але на місці не стоять і зловмисники. В Україні кількість виявлених злочинів у сфері кібербезпеки збільшується в середньому на 2,5 тисячі щорічно. За останні 5 років відбулось декілька великих кібератак на території України [1]: 2015 рік: Через вірус BlackEnergy 220 тис. споживачів залишилось без електроенергії; 2016 рік: Вірус WannaCry заблокував не менше 200 тис. комп'ютерів в 150 країнах світу; Вірус Petya вразив 60-80% українських підприємств, втрати становлять близько 10 млрд. грн.

Щоб вберегтись від сучасних мережевих загроз недостатньо використовувати лише традиційні засоби захисту як, наприклад, антивірусні програми чи брандмауери. Для вирішення проблеми використовуються системи виявлення вторгнень (IDS) або системи запобігання вторгнень (IPS). IDS/IPS часто виступає як наступний рівень безпеки після обминання зловмисником брандмауеру[1].

Метою доповіді є є реалізація автоматизованого встановлення та налаштування системи для моніторингу підозрілої активності в корпоративних мережах – системи виявлення та запобігання вторгненням.

В роботі був проведений огляд та дослідження найпоширеніших системи типу IDS/IPS. Для більшості даних систем відсутній власний графічний інтерфейс, велика кількість розглянутих систем позиціонує себе як лише вузлова чи лише мережева IDS/IPS-система, багато з систем працюють за замовчуванням лише в режимі виявлення вторгнень, а режим запобігання вторгненням є додатковим і вмикається за потреби, також системи даного типу складні в налаштуванні.

Список літератури

1.Литвиненко Б. В., Цуранов М.В. Моніторинг комп’ютерних мереж як засіб виявлення кіберзлочинців [Текст] / Б. В. Литвиненко, М.В. Цуранов // Всеукраїнська науково-технічна конференція “Актуальні питання протидії кіберзлочинності та торгівлі людьми”: Збірник матеріалів конференції. – 23 листоп. 2018р., м. Харків: МВС України, Харківський національний університет внутрішніх справ; Координатор проектів ОБСЄ в Україні – Харків: ХНУВС, 2018 – С. 293.

ДЕЯКІ ОСОБЛИВОСТІ ВИКОНАННЯ ТЕРМІНАЛЬНИХ КОМАНД НА СІМЕЙСТВІ СИСТЕМ WINDOWS

Барабаш В. О., Пересічанський В. М., Тулупов В. В.
Харківський національний університет внутрішніх справ, Харків, Україна

Розглядаючи систему розподілення доступу та привілеїв в сучасних системах таких як Windows 11, розуміють що під користувацькими обліковими записами є розподіл на адміністраторів та звичайних користувачів з обмеженими правами, а також у більш специфічному випадку можна згадати й групу доменних користувачів які особливо нічим не відрізняються від згаданої раніше локальної групи. З цими двома робочими групами стикається й прямо взаємодіє кожна людина, але є також майже не очевидна група користувачів, які працюють досить рідко й побічно через посередників, які виконують сервісну роль в нашій операційній системі – системна група (LocalSystem) [1].

До самої системної групи належить головний користувач NT AUTHORITY, він надається основному й найбільш важливому для роботи всієї операційної системи процесу ntoskrnl.exe [2] (NT Kernel & System). Ntoskrnl займається управлінням системними ресурсами, створенням та контролем процесів, тобто надає абстракцію між фізичним обладнанням та надає їх віртуальні образи для забезпечення безпеки та зручності виконання системних запитів від користувацького програмного забезпечення та драйверів пристроїв які виконуються на рівнях вже програмної системної абстракції.

Метою доповіді є розуміння які важливі функції та які повноваження має цей користувач та було б досить доречно володіти такими правами у випадках де необхідно бути вище за повноваженнями ніж адміністратор локальної групи.

Потрібно також розуміти, що ntoskrnl це ядро та є умовним містком між операційною системою та фізичним обладнанням, тому для його створення потрібен примусовий запуск умовного “нульового процесу” UEFI за допомогою Windows Boot Manager [2] під час завантаження вже з EFI завантажувача Windows.

Серед цих процесів, запущених як прямі нащадки ядра, є один на який через посередника може вплинути користувач - Планувальник завдань. Використовуючи schtasks [3] можна створити завдання на виконання при наступному завантаженні системи якоїсь дії.

В цю дію можна вкласти виконання термінальної команди від потрібного нам системного користувача, використовуючи вже механізм наслідування й надання змоги запуску програм від імені головного облікового запису процесу, принцип якого закладений в ядро.

Дуже скоро буде очевидно, що працювати виконуючи команди лише одного разу і лише при завантаженні системи є непрактичним, досить

затратним за часом процесом і деколи навіть неможливим при роботі з параметрами середовищ локальних груп.

У вирішенні цієї проблеми можна скористуватися власноруч написаною програмою, яка буде працювати від імені системи, виконуючи потрібні дії як повноцінний термінал у реальному часі в системному програмному просторі, який унеможливлює графічну і будь-яку взаємодію користувача з програмою.

Для спрощення взаємодії і реалізації на практиці та демонстрації принципу роботи коду цього процесу, можна створити демонстраційний комплекс програм, який складається з виконавчої частини на стороні системного програмного простору у обличчі системної служби Windows, створеною за допомогою експлуатації особливості наслідування користувачів, та клієнта на стороні вже графічного користувацького програмного простору за наступним посиланням на репозиторій з архівом, який має назву AbsoluteSolver.zip, [4] та який набув реалізації на мові програмування C#, що потребує SDK Visual Studio.NET але повністю виконує поставлену функцію – виконання термінальних команд користувачем від імені системи в реальному часі.

Роблячи підсумки можна впевнено сказати, що отримати користувачеві або зловмиснику системний рівень прав, знаючи поверхнево послідовність процесу завантаження системи та алгоритм наслідування параметрів у процесах наслідниках, є не такою вже і не можливою задачею, а навіть напроти до занепокоєння легкою та деструктивною.

При доброчесному використанні це рішення може бути задіяне при обслуговуванні системи або при відновленні завданої шкоди програмним забезпеченням зловмисника, захисний механізм якого є позбавлення користувача адміністратора прав на взаємодію з процесами або власними виконуючими файлами на рівні файлової системи.

Список літератури

1. LocalSystem URL:https://learn.microsoft.com/en-us/windows/win32/services/localsystem-account (дата звернення: 15.10.2023).

2. Ntoskrnl.exe URL: https://en.wikipedia.org/wiki/Ntoskrnl.exe (дата звернення: 15.10.2023).

3. schtasks.exe:URL: https://learn.microsoft.com/en-us/windows/win32/taskschd/schtasks (дата звернення: 17.10.2023).

4. https://github.com/vetkover/AbsoluteSolver/releases/tag/demo

РОЗРОБКА ІМІТАЦІЙНОЇ МОДЕЛІ ВИЗНАЧЕННЯ ВТОРГНЕНЬ У КОМП'ЮТЕРНИХ СИСТЕМАХ

Гнусов Ю. В., Зарудняк Д. С.
Харківський національний університет внутрішніх справ, Харків, Україна

Для проведення експериментальних досліджень статистичних властивостей мережного трафіку та обґрунтування практичних рекомендацій щодо побудови мережевих систем виявлення та запобігання вторгненням розроблено відповідну імітаційну модель.

Метою доповіді є опис розробленої імітаційної моделі яка містить:

– блок генерації мережного трафіку, призначений для імітації потоку даних у комп'ютерній системі (КС) як на підготовчому, так і на основному етапі функціонування;

– імітатори захоплення та фільтрації мережного трафіку – імітують відповідні процедури мережевого аналізатора, тобто, виробляють первинну обробку згенерованих блоком генерації даних;

– блок статистичної обробки призначений для аналізу відфільтрованих даних та формування на його основі статистичних портретів;

– блок зберігання даних зберігає статистичні портрети шаблонних даних;

– блок перевірки статистичних гіпотез призначений для обробки статистичних портретів шаблонних даних та потоків даних окремих служб та сервісів КС;

– блок прийняття рішення на підставі результатів перевірки статистичних гіпотез узагальнює та приймає рішення про наявність чи відсутність шкідливого мережевого трафіку та відповідного вторгнення;

– блок управління здійснює узгодження роботи інших блоків імітаційної моделі та управління основними обчислювальними операціями.

На підставі прийнятого рішення (у блоці прийняття рішення) у блоці формуванні повідомлення та впливів здійснюється формування керуючих впливів (у разі виявлення вторгнення) та формується повідомлення для системного адміністратора (фахівця з інформаційної безпеки) про поточний стан системи.

У доповіді визначено, що розроблена імітаційна модель може адаптивно реагувати на поточну ситуацію та за необхідності блокувати підозрілий трафік та розсилати попередження сусіднім вузлам мережі, робочу станцію мережного адміністратора, сервер протоколювання атак тощо.

РОЛЬ ТА МІСЦЕ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ВНЗ

Горелов Ю. П., Пересічанський В. М.
Харківський національний університет внутрішніх справ, Харків, Україна
Кобзев І. В.
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна

В епоху дедалі більшої цифрової присутності методи та засоби штучного інтелекту (ШІ) відіграють ключову роль у підвищенні кібербезпеки ВНЗ. Враховуючи підвищений обсяг цифрових даних, перехід на дистаційні технології навчання. важливість забезпечення безпеки університетських мереж стає незаперечною. Для ефективного захисту конфіденційних даних та інфраструктури ВНЗ необхідно інтегрувати різні технології кібербезпеки із передовими методами штучного інтелекту. Використання штучного інтелекту у сфері кібербезпеки у забезпечує низку значних переваг. Одним із ключових аспектів є здатність ШІ виявляти аномалії в мережі та запобігати атакам до їх виникнення. Для виконання цього завдання ШІ може використовувати наступні способи.

1. Моніторинг поведінки: ШІ може аналізувати нормальну поведінку користувачів, пристроїв та систем у мережі, ідентифікувати звичайні патерни активності та отримувати статистичні дані звичайного функціонування мережі. Коли в мережі відбувається щось незвичайне або відхиляється від звичайних патернів, ШІ може сигналізувати про це як потенційну аномалію.

2. Виявлення вторгнень: Використовуючи технології виявлення вторгнень, ШІ може аналізувати трафік у режимі реального часу та ідентифікувати аномальні спроби вторгнення, несанкціоновані спроби доступу та інші підозрілі активності. Це дозволяє ШІ завчасно виявляти потенційні загрози та вживати заходів для запобігання атакам.

3. Аналіз великих даних: ШІ може обробляти величезні обсяги даних, що збираються з різних джерел у мережі, включаючи журнали подій, відомості про трафік та багато інших параметрів. Аналіз цих даних дозволяє ШІ виявляти незвичайні чи непередбачені шаблони, які можуть свідчити про потенційні загрози безпеці.

4. Прогнозування загроз: Використовуючи алгоритми прогнозування та передбачення, ШІ може оцінювати ймовірність виникнення певних типів атак, ґрунтуючись на аналізі історичних даних та трендів. Це дозволяє вживати проактивних заходів для запобігання атакам до їх виникнення.

Крім виявлення загроз, ШІ також сприяє розробці більш складних та інтелектуальних методів шифрування, які б зробили мережі ВНЗ менш уразливими для злому.

1. Аналіз шифрування: ШІ здатний аналізувати існуючі методи шифрування та ідентифікувати їх слабкі місця. З використанням алгоритмів

машинного навчання, ШІ може запропонувати покращені методи шифрування, які краще захищають дані від злому та несанкціонованого доступу.

2. Створення нових алгоритмів: ШІ здатний генерувати нові алгоритми шифрування, використовуючи складні математичні моделі та статистичні методи. Ці алгоритми можуть бути більш складними та ефективними, що робить їх менш уразливими до атак зловмисників.

3. Адаптація до змін: ШІ може швидко адаптуватися до нових загроз і методів злому, що дозволяє йому модифікувати та вдосконалити алгоритми шифрування в реальному часі. Це допомагає мережам університету залишатися захищеними навіть в умовах кіберзагрози, що постійно змінюється.

4. Розподілені системи шифрування: ШІ здатний розробляти складніші та розподілені системи шифрування, які використовують безліч різних ключів та протоколів для захисту даних. Це робить злом мережі значно складнішим для зловмисників, оскільки вони повинні впоратися із кількома шарами захисту..

Однак, крім усіх переваг, існують і виклики, пов'язані з використанням штучного інтелекту в галузі кібербезпеки. Наприклад, необхідність навчання алгоритмів ШІ досить великих обсягів даних, що може створити нові ризики конфіденційності. Крім того, розробка та підтримка складних систем ШІ потребує спеціалізованих знань та фінансових витрат, що може стати викликом для багатьох університетів.

Для ефективного використання ІІ в галузі кібербезпеки ВНЗ необхідно встановити чіткі правила та стандарти безпеки, проводити регулярне навчання персоналу та підтримувати постійну моніторингову систему для виявлення нових загроз. Тільки за дотримання цих умов ВНЗ зможуть забезпечити надійний захист своїх цифрових ресурсів та даних, зберігаючи при цьому відкрите та інноваційне середовище для навчання та досліджень.

З огляду на зростаючу складність кіберзагроз і методи атак, що постійно змінюються, ВНЗ повинні також інвестувати в розробку та навчання власних систем ШІ, спеціально налаштованих для виявлення та аналізу нових загроз безпеці. Це дозволить покращити реакцію на нові загрози, у тому числі на такі, які можуть оминати стандартні системи безпеки. Важливо, щоб ці системи були гнучкими та могли адаптуватися до нових викликів та вимог кібербезпеки.

Виходячи з усього вищевикладеного, можна зробити висновок, що використання штучного інтелекту в галузі кібербезпеки ВНЗ є невід'ємною частиною сучасної цифрової інфраструктури. Правильне використання та розвиток систем ШІ, адаптованих до специфіки університетського середовища, зможе ефективно захистити дані та забезпечити стабільне та безпечне середовище для навчання та досліджень уВНЗ.

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ

Ткаченко О. С., Хавіна І. П.
Харківський національний університет внутрішніх справ, Харків, Україна

В сучасному світі організації, установи та підприємства все частіше потребують системи захисту інформації для збереження даних.

З кожним днем загрози стають більш ширшими та універсальними, що дає змогу зловмиснику з меншим прикладанням зусиль заволодіти інформацією.

Для запобігання від витоків, тримачі інформації потребують надійну автоматизовану систему, яка забезпечить конфіденційність та цілісність даних.

Тому потрібно обрати найефективнішу систему для захисту інформації в автоматизованій системі громадської організації.

Захист інформації в автоматизованій системі (АС) – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [1].

Метою доповіді є розробка рекомендацій, які дозволять побудувати комплексну систему захисту (КСЗІ) інформації для обробки інформації з різними ступенями захисту, для забезпечення цілісності та конфіденційність в автоматизованій системі громадської організації.

В доповіді наводяться рекомендації щодо створення комплексної системи захисту інформації.

Наведена інформація розкриває етапи створення КСЗІ, які розкривають подальшу послідовність дій, для забезпечення безпеки від витоку інформації технічними каналами. Порядок створення КСЗІ в автоматизованій системі громадської організації є єдиним незалежно від того, створюється КСЗІ в АС, яка проектується, чи в діючій АС, якщо виникла необхідність. Послідовність виконання та типовий зміст робіт кожного з етапів створення КСЗІ повинні узгоджуватися з відповідними стадіями і етапами робіт зі створення АС, визначеними НД ТЗІ 3.7-003-05 [2]. Також перед обранням КСЗІ, слід звернути увагу на комплекс засобів захисту (КЗЗ). Більш універсальним та доступним КЗЗ, є створення КСЗІ на базі операційної системи Windows 10 Pro. Переваги даного КЗЗ, є бюджетним варіантом та більш легким у налаштуванні та користуванні, як звичайному користувачу так і системному адміністратору. Також використання такого засобу в АС громадської організації є доступним для будь-якого тримача інформації. Але може не задовольнити в надійності захисту інформації з більш високим грифом обмеження доступу.

У разі необхідності КЗЗ для інформації з грифами вище ніж «Для службового користування», рекомендується обрати засоби з підвищеною безпекою, наприклад: Лоза-1 з рівнем підвищеною безпекою[3].

Список літератури

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

2. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf

3. Система захисту інформації Лоза™-1, ВЕРСІЯ 4 [Електронний ресурс]. – Режим доступу: http://avtoprom.kiev.ua/avtoprom/ru/content/Система-защиты-информации-ЛОЗА™-1-версия-4

АНАЛІЗ МЕТОДІВ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ КІБЕРБЕЗПЕЦІ

Онищенко Ю. М., Доманов Б. Г.
Харківський національний університет внутрішніх справ, Харків, Україна

Стрімкий розвиток інформаційних технологій та обчислювальних процесів зумовлюють необхідність чіткого розуміння та обґрунтування сучасних напрямків науки та техніки. Потужним інструментом прийняття рішень, які відіграють значення для прогресивного науково-технічного розвитку, є штучний інтелект. Вирішення надскладних завдань, пов'язаних із застосуванням технологічних процесів та наукових рішень напряму залежить від ефективного використання алгоритмів та систем штучного інтелекту. Проблематика застосування методів та систем штучного інтелекту є новим напрямком прикладної науки, який повинен мати ґрунтовну теоретичну деталізацію. Зважаючи на потребу у розвитку інтелектуальних технічних систем, спрямованих на розв'язання найскладніших виробничих завдань, дослідження методів та систем є штучного інтелекту є актуальним напрямом наукових узагальнень та пошуків [1]. У той же час активний розвиток технологій штучного інтелекту та аналізу великих даних відкриває для держави та бізнесу нові можливості оптимізації операційної та управлінської діяльності за рахунок цифровізації окремих процесів та цілих галузей. Тому актуальним та своєчасним є розгляд можливостей застосування технологій штучного інтелекту до такої галузі як оцінка ризиків [3].

Метою доповіді є визначення методів оцінки ризиків безпеки підприємства із застосуванням штучного інтелекту та надання практичних рекомендації щодо попередження ризиків інформаційних систем з використанням системи штучного інтелекту.

В доповіді розглянуто правові основи застосування технологій штучного інтелекту, проаналізовано методи оцінки стану інформаційної безпеки та надано практичні рекомендації щодо застосування технологій штучного інтелекту для нівелювання ризиків інформаційної безпеки підприємства. Подальші дослідження повинні бути спрямовані на з'ясуванні можливості розподілу методів за напрямками використання та за критерієм ефективності

відповідно до пріоритетів, закріплених Концепцією розвитку штучного інтелекту в Україні [4].

Список літератури

1.Батареєв В.В. Методи та системи штучного інтелекту. Вісник Хмельницького національного університету. 2021. №1 (293). С. 17-21.

2.Ковтуненко Ю.В. Застосування штучного інтелекту у системі управління підприємством: проблеми та переваги. Economic journal Odessa polytechnic university. 2019. №2 (8). С. 93-99.

3.Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.

4.Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Сучасний захист інформації. 2020. № 4 (44). С. 6-11.

РОЛЬ КРИПТОГРАФІЇ В ЗАБЕЗПЕЧЕННІ КОНФІДЕНЦІЙНОСТІ ДАНИХ В АНТИВІРУСНИХ СИСТЕМАХ

Хівренко Д. В., Медведєв С. О.
Харківський національний університет внутрішніх справ, Харків, Україна

Кожне антивірусне ПО крім своєї основної функції виявлення та запобігання дії зловмисних файлів має забезпечувати належну конфіденційність даних своїх користувачів. Адже лише за виконанням цієї умови особисті дані як звичайних користувачів, так і великих корпорацій можуть бути у безпеці. [1]. Метою доповіді є аналіз можливостей криптографії в антивірусних системах.

В доповіді визначенні методи захисту даних в специфікаціях і базах даних, захисту телекомунікацій та підписи і цифрового сертифікату [2]. Значна увага приділяється можливостям використання апарату криптографії у цих найважливіших сферах забезпечення конфіденційності.

Таким чином, криптографія важлива для забезпечення конфіденційності даних в антивірусних системах, оскільки вона допомагає захистити інформацію від несанкціонованого доступу та забезпечує безпеку важливих даних і комунікацій. Використання криптографії сприяє підвищенню ефективності та надійності антивірусних систем.

Список літератури

1. Про електронний цифровий підпис : Закон України від 22.05.03 р. № 852-IV. – URL: https://zakon.rada.gov.ua/laws/show/852-15 (дата звернення 13.10.2023)

2. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І. Горбенко ; Харк. нац. ун-т радіоелектрон., ЗАТ “Ін-т інформ. технологій”. – Х. : Форт, 2012. – 868 с.

БЕЗПЕЧНЕ КОРИСТУВАННЯ ГРОМАДСЬКОЮ ТА ДОМАШНЬОЮ МЕРЕЖЕЮ WI-FI

Божкевич А. Є., Онищенко Ю.М.
Харківський університет внутрішніх справ, Харків, Україна

Сьогодні мережа Wi-Fi широко поширена по всій земній кулі і неможливо уявити і дня без користування нею. Бездротова мережа сучасності дозволяє нам незалежно від місця знаходження завжди бути онлайн: обмінюватися даними, відправляти і приймати пошту, знаходити потрібну інформацію в мережі Інтернет. Бездротові мережі зручні і добре захищені, що дає можливість використання мережевих технологій цього типу і в домашніх умовах [1]. Користування Wi-Fi вдома передбачає наявність роутера, що, власне, «роздає» Wi-Fi. Саме налаштування цього пристрою є необхідною умовою безпеки. Якщо не приділити увагу цьому важливого питанню, зловмисники можуть отримати контроль над каналами передачі даних, вкрасти конфіденційну інформацію, гроші, обмежити та/або позбавити користувача доступу до мережі Інтернет. Безпека домашньої мережі – це набагато більше, ніж встановлення пароля для домашнього Wi-Fi. Члени вашої родини дивляться свої улюблені шоу на Smart TV, купують різні товари в інтернеті, грають в мережеві ігри або працюють вдома. При цьому всі види важливих даних – особиста інформація, паролі, адреси, приватні фотографії тощо – постійно підключені до інтернету через домашню мережу.

Більшість користувачів мережі Інтернет знає про такі поняття, як "фішинг" та "шкідливе програмне забезпечення", які хакери використовують, щоб замаскувати себе та отримати доступ до домашньої мережі для крадіжки або знищення персональних даних. Але чи справді усі користувачі обізнані з тим, що це насправді і як з цим боротися? Безпека домашньої мережі – це фундаментальна основа для захисту себе та родини від загроз з боку зловмисників. Існують певні правила, дотримуючись яких, можна з легкістю захистити власну інформацію від витоку у мережі. Перш за все, налаштовуючи роутер, треба зважати на такі аспекти, що є складовими високого рівня кібербезпеки «домашньої» мережі, адже визначають те, як і коли роутер буде дозволяти пристроям користуватися Wi-Fi:

1. Спершу змініть стандартні налаштування логіна і пароля, що встановленні виробником із заводу.

2. Змініть тип шифрування на WPA2 / WPA, що зробить передачу даних мережею більш захищеною.

3. Керуйте списком пристроїв що користуються Вашою Wi-Fi мережею через визначення MAC-адрес пристроїв що можуть до неї під'єднуватися.

4. Вимкніть функцію WPS (QSS) – ця функція спрощує підключення нових пристроїв до мережі. Якщо Wi-Fi користуються з одних і тих самих гаджетів, краще відключити цю функцію, оскільки вона має серйозні уразливості.

5. Приховайте свою мережу від пристроїв які сканують простір в пошуках мереж. Ідея полягає у тому, що якщо Wi-Fi мережу не бачать, то вірогідність того що її захочуть «зламати» суттєво знижується [2].

Слід зауважити, що сучасні технології дають нам можливість користуватись мережею Wi-Fi не лише вдома, а й в громадських місцях. Сьогодні підключитися до безкоштовних мереж Wi-Fi можна у багатьох закладах харчування, в парках, громадському транспорті, торговельних центрах і навіть в укриттях. Для багатьох українців це зручний та вигідний спосіб отримати доступ до мережі Інтернет та бути постійно на зв'язку [1].

Однак, варто пам'ятати, що переважна більшість Wi-Fi мереж у громадських місцях мають дуже низький рівень захисту від злому. Отже, отримавши доступ до керування ними, шахраї можуть отримати доступ до конфіденційної інформації користувачів у тому числі до логінів та паролів від облікових записів, якими кожен з нас активно користується.

Для того, щоб не потрапити на гачок шахраїв, необхідно дотримуватися простих правил безпеки при роботі з громадськими Wi-Fi мережами. Ці правила стосуються всіх видів пристроїв – ПК, планшетів, смартфонів: встановіть антивірус; використовуйте VPN-сервіси; краще підключатися до мереж Wi-Fi вручну; обмежте можливість автоматичного підключення пристрою. Це можна зробити в налаштуваннях ноутбука або смартфону; якщо є можливість, уточніть назву мережі, до якої маєте намір під'єднатися; пам'ятайте – кібершахраї можуть створювати фейкові мережі для заволодінням інформацією; вимкніть функцію надання спільного доступу до файлів через локальну мережу на всіх пристроях; при підключенні до громадського Wi-Fi вони можуть стати доступними зловмисникам; уникайте здійснення грошових операцій: перекази, покупки, регулярні платежі. Не використовуйте загальнодоступні мережі Wi-Fi для обміну чутливою конфіденційною інформацією і вирішення важливих справ; краще скористатися перевіреною стаціонарною мережею або мобільним інтернетом; відвідуйте сайти, що використовують безпечний протокол з'єднання HTTPS; вимкніть загальний доступ до файлів і папок на пристрої що буде приєднуватися до відкритої Wi-Fi мережі.

Отже, можна зробити висновок, що сьогодні більшість користувачів перебувають онлайн майже цілодобово. Значною мірою на це вплинула наявність загальнодоступних Wi-Fi у громадських місцях та активним користуванням мережею в домашніх умовах [2]. Враховуючи той факт, що протягом наступних кількох років Wi-Fi обіцяють зробити безпечнішим, наразі досі залишається актуальним питання щодо збереження своєї цифрової безпеки в кіберпросторі.

Список літератури

1. Бездротові мережі (Wi-Fi). URL: https://i-help.us/adjustment/wifi/
2. Wi-Fi безпека: вдома та в громадських місцях. URL: https://zillya.ua/index.php?q=wi-fi-bezpeka-vdoma-ta-v-gromadskikh-mistsyakh

ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ КІБЕРБЕЗПЕКИ НА ОСНОВІ ПОКАЗНИКІВ

Гнусов Ю. В., Штих С. О.
Харківський національний університет внутрішніх справ, Харків, Україна

Через те, що бізнес-процеси стають орієнтованими на IT, потреби в інформаційних системах в галузі безпеки зростають і стають все важливішими з кожним днем. В даний час Інтернет не є єдиним джерелом інформації, але це також середовище, в якому люди займаються бізнесом. Проте таке з'єднання також створює і нові загрози: шкідливі хакери, злочинці, промислові шпигуни. Ці загрози не тільки викрадають організаційні ресурси, але також спричиняють дефіцит сервісів або системні помилки, що шкодить репутації компанії та лякає клієнтів. Зростання складності Інтернету та його додатків та некерована електронна трансформація організацій для залучення нових бізнес-можливостей посилили незахищеність цифрового світу. Результати опитування IDC вказують на те, що безпека IT є зростаючим пріоритетом для організацій, і більше 80% організацій очікують збільшення своїх інвестицій в безпеку IT [1]. Незважаючи на те, що організації постійно інвестують на продукти безпеки IT, загрози та інциденти в галузі безпеки зростають з кожним днем. Брюс Шнайєр пояснює цей факт наступним чином: "Безпека на основі продуктів є нестійкою. Нове відкриття атак, розповсюдження інструментів нападу та недоліки в самих продуктах призводять до того, що мережа стає (і все частіше) вразливою з випадковими інтервалами" [2].

Метою доповіді є дослідження методів оцінки інформаційної безпеки на основі систем показників безпеки та розробка автоматизованого засобу оцінки інформаційної безпеки на основі показників безпеки стандарту NIST SP 800-55.

Аналіз існуючих систем дозволяє виділити такі системи. 1) системи виключно з кількісними показниками безпеки (таксономія CISWG); 2) системи, які передбачають виключно якісну оцінку (таксономія OCTAVE); 3) змішані системи показників (таксономія NIST, Erkan Kahrmana). Загальним і істотним недоліком всіх таксномій є те, що жодною з них не запропоновані будь-які підходи (рекомендації) щодо отримання комплексних (узагальнених) оцінок ні в рамках окремої групи показників, ні врамках напрямку або всієї діяльності щодо захисту інформації в цілому.

Список літератури

1. Using Data-Driven Operations to Overcome Digital Disruption [URL]: https://info.idc.com/data-driven-operations-ebook.html.

2. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері. Підручник/ [Цуранов М.В., Струков В.М., Пєвнєв В.Я.] Харків: ХНУВС, 2015. 256 с.

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В НАВЧАЛЬНИХ ЗАКЛАДАХ: ЯК ЗАБЕЗПЕЧИТИ БЕЗПЕКУ ДАНИХ.

Кондрацький Г. О., Дригач К. В., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Кібербезпека - це стан захищеності інформації та систем від несанкціонованого доступу, використання, розкриття, модифікації або знищення. У сучасному світі навчальні заклади стають особливо вразливими перед кіберзагрозами через обробку великих обсягів чутливих даних, таких як особисті дані студентів, викладачів і співробітників, а також цінні навчальні матеріали.

Кіберзлочинці часто використовують методи соціальної інженерії, представляючись надійними джерелами або авторитетними організаціями, для того, щоб проникнути в системи освітніх установ. Ці так звані фішингові атаки можуть призвести до несанкціонованого доступу до важливих даних. З іншого боку, віруси та інші шкідливі програми, як-от трояни, становлять загрозу для комп'ютерних мереж, пошкоджуючи системи та викрадаючи цінну інформацію [1].

Метою доповіді є ознайомлення з ключовими аспектами кібербезпеки у навчальних закладах. Кібергігієна висвітлює основні види загроз і вразливостей, а також пропонує дієві методики забезпечення захисту даних.

Доповідь акцентує увагу на важливості розробки комплексних політик безпеки, здійсненні постійного аудиту та оновлення захисних систем, і підкреслює значення навчання персоналу і студентів основам. Забезпечення кібербезпеки в освітніх установах вимагає інтегрованого підходу, включаючи використання передових технологій для захисту від онлайн-загроз. Це означає імплементацію надійного програмного та апаратного забезпечення, здатного виявляти та блокувати потенційні атаки. Також критично важливим є навчання співробітників та студентів основам кібербезпеки, щоб вони могли розпізнавати загрози і знали, як реагувати у випадку безпекових інцидентів. Крім того, розробка ефективної політики безпеки та впровадження чітких процедур є ключовими для захисту інформаційних ресурсів. Співпраця з професійними постачальниками кібербезпеки може додатково зміцнити безпеку даних, пропонуючи експертизу та підтримку в цій важливій сфері [2].

Список літератури

1. Пінчук О. П. СИНТЕТИЧНЕ НАВЧАЛЬНЕ СЕРЕДОВИЩЕ – КРОК ДО НОВОЇ ОСВІТИ [Електронний ресурс] / О. П. Пінчук, С. Г. Литвинова, О. Ю. Буров. – 2017. – Режим доступу до ресурсу: https://journal.iitta.gov.ua/index.php/itlt/article/view/1831?articlesBySameAuthorPage=2.

СЕКЦІЯ 4
КОМП'ЮТЕРНІ МЕТОДИ І ЗАСОБИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА УПРАВЛІННЯ

Керівники секції: д.т.н. проф. І. В. Рубан, ХНУРЕ, Харків
д.т.н. проф. А. А. Коваленко, ХНУРЕ, Харків
Секретар секції: к.т.н. доц. О. С. Ляшенко, ХНУРЕ, Харків

ВИЯВЛЕННЯ ВТОРГНЕНЬ У КОМП'ЮТЕРНІ МЕРЕЖІ ЗА ДОПОМОГОЮ БІБЛІОТЕКИ NETWORKX PYTHON

Гавриленко С. Ю.
Національній технічний університет «ХПІ», Харків, Україна
Кісь А. А.
Полтавський політехнічний фаховий коледж
Національного технічного університету «ХПІ», Полтава, Україна

Інтеграція різноманітних мережних інструментів є важливою проблемою, з якою мають справу сучасні комп'ютерні технології. Величезний набір даних, що надходять у різних форматах, потребує використання та розробки нових алгоритмів їх обробки.

Розробка інтерфейсу мережевих програм та обладнання є складним завданням, для вирішення якого необхідно використовувати потужні та прості інструменти програмування.

Зокрема, Python дає можливість вирішення цих завдань та включає бібліотеку NetworkX, яка використовується для дослідження й аналізу різних типів мереж і мережевих алгоритмів, вбудованих у граф алгоритмів та генераторів графів. Бібліотека NetworkX Python містить велику колекцію мережевих структурних даних, а саме: простий граф, спрямований граф, повний граф, повний дводольний граф, граф Петерсена та ін. В бібліотеці NetworkX є вбудована підтримка генераторів складних випадкових графів, таких як: Ердос-Реньї, Барбасі-Альберт, Small World та ін. [1].

Крім того, використання бібліотеки NetworkX має широкі можливості керування даними для представлення багатьох типів мереж або графів, зокрема: прості графи, спрямовані графи та графи із самоциклами та паралельними ребрами. Вузли в графах NetworkX можуть бути будь-якими, наприклад, хешованими об'єктами Python, а ребра можуть містити довільні дані [2]. Ця гнучкість робить NetworkX ідеальним для представлення різних типів мереж у багатьох науково-практичних сферах. Також, в основних структурах даних реалізовано багато графових алгоритмів для обчислення властивостей мережі і показників структури: розподіл за ступенями, найкоротші шляхи, централізованість, кластеризація та ін. [1]. Приклад графових алгоритмів, наведено на рис. 1.

NetworkX може зчитувати та зберігати різні формати графів для легкого обміну наявними даними, а також надає генератори для багатьох класичних графів і популярних моделей графів Small World, Ердоес-Реньї, Барабасі-Альберта. Гнучкість та простота використання мови програмування Python, разом із підключенням до інструментів Matplotlib та SciPy, роблять NetworkX потужним інструментом для проведення інженерно-технічних та наукових обчислень та надають можливість моделювання та аналізу складних мереж які поєднують інформацію із різних джерел даних [2].

1 – граф Ердос-Реньї; 2 – граф Small World; 3 – Граф Барбасі-Альберт.

Рис. 1. Приклад графових алгоритмів

Бібліотека містить вбудовані функції та алгоритми для виявлення та аналізу мережевих вторгнень, наприклад, кластерів скомпрометованих пристроїв. NetworkX пропонує численні варіанти візуалізації для представлення та аналізу даних, що додатково полегшує виявлення та аналіз вторгнень. Використовуючи NetworkX, можливо створювати надійні та ефективні моделі виявлення вторгнень для великих складних мереж [3].

Список літератури

1. Yedhu Sastri, Kuttyamma A.J. NetworkX and Matplotlib an Analysis. Disinformation International Journal of Scientific & Engineering Research. V. 4. № 8. 2013.

2. A Hagberg, D Schult, P Swart, Exploring Network Structure, Dynamics, and Function using NetworkX in Proceedings of the 7th Python in Science conference (SciPy 2008), pp. 11-15

3. Olga Papadopoulou,Themistoklis Makedas, Lazaros Apostolidis, Francesco Poldi, Symeon Papadopoulos, Ioannis Kompatsiaris. MeVer NetworkX: Network Analysis and Visualization for Tracing Disinformation. *Future Internet*, 2022, № 14, 26 p., URL: https://www.researchgate.net/publication/360506219_MeVer_NetworkX_Network_Analysis_and_Visualization_for_Tracing_Disinformation; doi; https://doi.org/10.3390/fi14050147.

A COMPARATIVE TEXT ANALYSIS USING COMPUTATIONAL AND DEEP LEARNING METHODS

Dun Bao, Kuchuk N. H., Antsyferova O. O.
National Technical University «KhPI», Kharkiv, Ukraine

Diaries of Samuel Pepys and John Evelyn provide valuable historical insights, offering first-hand observations of politics, religion, economy, landscape, lifestyle and entertainment in 17th century London and England. This paper utilizes computational and deep learning-based approaches to perform a comparative text analysis and mining on these diaries [1].

Word- and frequency-based features are distilled from the diaries to perform comparative analysis of the linguistic style of the texts.

This study then extracts themes from all entries with LDA model, performs clustering analysis to recognize influential social events. Bidirectional LSTM (BiLSTM) and Transformer models are trained and evaluated on various text mining tasks, including extracting historical insights, performing sentiment analysis, recognizing named entities, conducting social network analysis, and modeling topics [2].

The results of the study indicate that of while both of the diaries contribute to enhancing our understandings of the period, linguistic styles and topics covered by Samuel Pepys and John Evelyn are significantly different, which is consistent with previous literature.

In addition, deep-learning models reveal undiscovered connections between the diaries in social networks, common topics and sentiments.

Future work may aim to explore the scalability of the proposed methodology to other historical text data and evaluate the effectiveness of emerging deep learning models in historical text analysis.

This will pave the way for more extensive computational exploration in historical and sociocultural research [3].

References

1 Gomathi, B., Saravana Balaji, B., Krishna Kumar, V., ...Masud, M., Kuchuk, N. Multi-Objective Optimization of Energy Aware Virtual Machine Placement in Cloud Data Center. Intelligent Automation and Soft Computingthis link is disabled, 2022, 33(3), pp. 1771–1785.

2 Kuchuk N., Mozhaev O., Mozhaev M. Method for calculating of e-learning traffic peakedness. Problems of Infocomunications. Science and technology : IEEE 4-th International Scientific – Practical Conference (October 10-13, 2017., Kharkiv, Ukraine). Kharkiv, 2017. P. 359-362.

3 Kuchuk N., Bulba S., Semenova A., Hu Z. Transaction Planning Methods in Hyperconverged Architecture Systems. Conflict Management in Global Information Networks, CMiGIN 2019 : Proceedings of the International Workshop (November 29, 2019, Lviv, Ukraine). Lviv, 2019. P. 35-46.

ФОРМУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМ

Кучук Н. Г., Шиман А. П.
Національній технічний університет «ХПІ», Харків, Україна

В доповіді розглянуто основні принципи формування інтелектуальних транспортних систем комфортного міського середовища з урахуванням планувальних обмежень, що пов'язано з досконалим знанням організації транспортних процесів у містах.

Метою доповіді є дослідження умов для розвитку та впровадження технологій інтелектуальних транспортних систем.

Транспортна інфраструктура поступово наближається до створення в місті простої транспортної системи, яка дозволяє якісно та ефективно регулювати пасажиропотік та реагувати на будь-яку ситуацію на дорогах [2].

Міста, які бажають стати розумним містом, найчастіше починають із розбудови інтелектуальної транспортної інфраструктури у формі Інтелектуальної транспортної мережі (ITN).

ITN включає:

систему управління громадським транспортом,
інформаційну систему маршруту та електронний розклад руху,
систему безпеки та керування транспортним засобом,
єдиний тариф [1].

При формуванні інтелектуальних транспортних систем в дорожньому русі в по-перше необхідно організувати збір інформації про стан трафіку. Один із способів це зробити – забезпечити отримання даних безпосередньо від користувачів.

Практично у кожної людини є смартфон з GPS і іншими корисними датчиками, які дозволяють передавати актуальні відомості про транспортній системі. Для збору та подальшого аналізу інформації може бути розроблений застосунок, де користувач буде вказувати свій маршрут, допомагаючи системі зібрати дані про швидкість, затримки на певних ділянках, висоті над рівнем моря і багатьох інших факторах, які можуть бути використані для аналізу дорожньої обстановки [3].

Список літератури

1 Smart city mobility. URL: https://mobility.here.com/learn/smart-citymobility/smart-citymobility-7-major-cities-getting-it-right

2 Інтелектуальні транспортні системи: проблема термінології та формування системи класифікації[Electronic resource] – 2018. – Access mode: https://www.econa.org.ua/index.php/ econa/article/view/1679.

3 Socio-psychological factors that influence acceptability of intelligent transport systems: A model [Electronic resource] – 2018. – Access mode: https://www.taylorfrancis.com/books/e/ 9781315578132/ chapters/ 10.1201/9781315578132-4.

ТЕХНОЛОГІЯ РОЗПІЗНАВАННЯ ШРИФТУ БРАЙЛЯ НА БАЗІ НЕЙРОННОЇ МЕРЕЖІ

Бовчалюк С. Я., Врублевський В. О.
Харківський національний університет радіоелектроніки, Харків, Україна

Шрифт Брайля – це рельєфно-крапковий тактильний шрифт, який дає змогу людям з обмеженими можливостями зору читати і писати. Існує багато методів розпізнавання шрифту брайля, які об'єднані під терміном OBR (Optical Braille Recognition) [1]. У наш час бурхливого розвитку нейронних мереж і штучного інтелекту, з'являються дедалі новіші сфери їх застосування, однією з популярних сфер застосування є машинний зір. У машинному зорі таким методом є конвертація зображень до відтінків сірого, як і повна бінаризація пікселів [2].

Метою доповіді є визначення оптимальних методів бінаризації зображень для зменшення кількості інформації про зображення без помітної втрати якості даних, а також виділення ключових ознак, необхідних для подальшої роботи із зображенням.

Бінаризація – це процес перетворення зображення з градацій сірого на двоколірне (бінарне) зображення, пікселі якого можуть мати лише два значення: чорний або білий. У контексті обробки зображень, бінаризація має на увазі використання порогового значення, для диференціювання класів пікселів чорного (об'єкт) і білого (фон). Методи знаходження порогу бінаризації можна розділити на дві умовні категорії – глобальні та локальні. У глобальних методах обробляється все зображення, використовуючи заздалегідь підібраний поріг бінаризації, за допомогою якого відбувається диференціювання на чорний і білий колір. Методи бінаризації, за яких зображення ділиться на частини або береться якесь оточення пікселя називають локальними.

Для того, щоб визначити найбільш ефективний алгоритм бінаризації, було обрано різні комбінації з пар: режим конвертації зображення в градації сірого та методу бінаризації. За результатами отриманих зображень можна зробити висновок, що найбільш оптимальним виявився алгоритм Бредлі, оскільки кінцевий результат містить найменшу кількість шуму, збережена ключова інформація з вихідного зображення, а обчислювальна складність поступається лише методам глобальної бінаризації.

Список літератури

1. Isayed, S. A review of optical Braille recognition / S. Isayed, R. Tahboub //2015 2nd World Symposium on Web Applications and Networking (WSWAN). – IEEE. 2015. – С. 1–6.

2. Romano He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep Residual Learning for Image Recognition. В 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (с. 770–778).

ТЕХНОЛОГІЯ ЗБОРУ ДАНИХ В ІНТЕЛЕКТУАЛЬНИХ ЕНЕРГЕТИЧНИХ МЕРЕЖАХ

Бовчалюк С. Я., Цірульніков Д. В.
Харківський національний університет радіоелектроніки, Харків, Україна

Останні декілька років характеризуються, як суттєвим зростанням енергоспоживання, так і певними змінами у джерелах генерування електричної енергії [1, 2]. Інтелектуальні енергетичні мережі – «Smart Grid», є передовою концепцією в області енергетики, яка включає в себе використання інформаційних технологій для оптимізації виробництва, розподілу та споживання електроенергії. Основна мета Smart Grid – забезпечення високоефективної, надійної, економічної та сталої системи постачання електроенергії.

Метою доповіді є аналіз підходів, технологій, технічних засобів збору і обробки даних для реалізації технології Smart Grid.

Основними складовими інтелектуальних енергетичних мереж є: «розумні» або «інтелектуальні» лічильники; постачальник енергії; суматор даних; центр управління розподілом.

Інтелектуальні лічильники – різновид лічильників, забезпечених (додатково) комунікаційними засобами для передачі накопиченої інформації за допомогою мережних технологій з метою моніторингу та здійснення розрахунків за комунальні послуги. Суматор відправляє агреговані дані в центр управління розподілом, керований комунальною компанією. Зокрема, головний сервер вдосконаленої вимірювальної інфраструктури (Advanced Metering Infrastructure, AMI), який зберігає дані лічильників і спільно використовує збережені дані за допомогою системи управління даними лічильників (Meter Data Management System, MDMS), яка управляє даними з іншими системами, такими як системи реагування на запити, історію та біллінгові системи. Зібрані дані доправляються до центру управління, де дані інтелектуальних лічильників зберігаються, олброблюються й аналізуються, і на основі цього постачальником енергії можуть бути прийняті певні рішення на основі отриманих даних.

Використання розглянутих технологій дозволить енергетичним мережам бути гнучкими, адаптивними та ефективними в управлінні енергоресурсами, а також реагувати на змінні потреби споживачів і динамічні умови ринку.

Список літератури

1. Бовчалюк С. Я. Перспективи побудови інтелектуальних мереж SMART GRID базі ПЛІС-технологій / С. Я. Бовчалюк, С. О. Тимчук, І. О. Фурман, О. М. Піскарьов // Вісник Вінницького політехнічного інституту. –2017. – №5 (134). – С. 80–85.

2. Stanislav Bovchaliuk. The Architecture of Fuzzy Logic Automat of Parallel Action for the Intelligent Smart Grid Networks / S. Bovchaliuk, S.Tymchuk, S. Shendryk, V. Shendryk // New Technologies, Development and Application III. NT 2020. Lecture Notes in Networks and Systems, vol. 128. Springer, – 2020. – P. 462–468.

ТЕХНОЛОГІЯ ТА СЕРВІС МОНІТОРИНГУ РОБОТИ АВТОМОБІЛЬНОГО ТРАНСПОРТУ

Бовчалюк С. Я., Підлужний В. С.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі, де автомобільний транспорт відіграє важливу роль у глобальних економічних та соціальних процесах, виникає необхідність вдосконалення та ефективного контролю за його функціонуванням. Отже технології моніторингу стають ключовим інструментом для забезпечення безпеки, оптимізації продуктивності та зменшення негативного впливу на навколишнє середовище [1].

Метою доповіді є дослідження та аналіз сучасних технологій та сервісів моніторингу, спрямованих на поліпшення функціонування автомобільного транспорту з метою визначення їхнього впливу на транспортну інфраструктуру, економіку та екологію.

Основні складові системи моніторингу автопарку включають в себе апаратні та програмні засоби, які спільно забезпечують ефективний контроль за рухом та станом транспортних засобів. До апаратних засобів можна віднести: трекер, датчики рівня палива, відкриття дверей, куту нахилу транспортного засобу, ультразвуковий датчик наближення, тощо. Всі перераховані апаратні засоби моніторингу транспорту відіграють важливу роль у забезпеченні ефективного управління автопарком, але одним із ключових елементів в ефективному управлінні комерційним транспортом є точне вимірювання споживання палива та контроль за його використанням. Впровадження сучасних датчиків палива дозволяє операторам транспортних парків моніторити рівень палива в реальному часі, виявляти витоки та несправності системи. Аналіз даних дозволяє здійснювати стратегічне планування щодо зниження витрат, підвищення рентабельності управління транспортними парками, впроваджувати екологічно чисті практики та зменшувати негативний вплив на довкілля.

Функції збору та обробки даних покладено на сервіс моніторингу транспорту, що забезпечує постійний контроль за рухом та станом транспортних засобів в реальному часі. Цей сервіс використовується для відстеження місцезнаходження, шляхів руху, а також робочих параметрів транспортних засобів, таких як швидкість, витрати палива, температура двигуна та інші важливі показники.

Дослідження у сфері технології та сервісів моніторингу транспорту дозволить розвиватися та вдосконалюватися сучасному бізнесу з метою забезпечення найефективніших та інноваційних інструментів.

Список літератури

1. Johnson, Emily. "Fuel Monitoring Systems in Modern Transportation." Journal of Logistics and Supply Chain Management, vol. 18, no. 3, 2022.

МЕТОД ПІДВИЩЕННЯ ЯКОСТІ РАСТРОВИХ ЗОБРАЖЕНЬ НА БАЗІ ТЕХНОЛОГІЙ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

Бовчалюк С. Я., Лук'яненко Є. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Існує думка, що у наш час текст та книги поступово втрачають свою ключову роль у постачанні інформації, а їхнє місце займають зображення та відео. Сучасні камери дозволяють створювати високоякісні фотографії та відео в великому розширенні, але такі можливості не завжди були доступні. Існують обставини, коли отримати якісне зображення високої роздільної здатності виявляється проблематичним, наприклад, при дослідженні глибоких водойм або внутрішніх структур організму людини. Крім того, розмір таких зображень має значення, і навіть при зростанні обсягу пам'яті складно зберігати великі файли високоякісного відео на портативних пристроях. Час від часу виникає потреба у покращенні якості деяких растрових зображень[1]. Загалом якість може оцінюватися кількістю пікселів на одиницю площі екрану, але це не завжди враховує всі аспекти сприйняття якості людським зором.

Метою доповіді є аналіз і удосконалення методу підвищення якості зображень на базі існуючих архітектур нейромереж. Пропонується дослідити існуючі нейромережеві методи, відібрати кращі відомі архітектури нейромереж, побудувати власні архітектури, та зробити порівняння всіх цих методів.

В доповіді наводяться результати аналізу базових методів підвищення якості растрових зображень в порівнянні з використанням технології глибокого навчання та штучних нейронних мереж для покращення деталізації візуального матеріалу.

Наведені дані показують, що нейронні мережі протягом останнього десятиліття зазнали значного прогресу, вражаючи своєю здатністю класифікації, апроксимації, передбачення та виокремлення об'єктів з надзвичайною точністю. У сфері машинного зору вони викликали значний революційний стрибок. У вдосконаленні якості та інформативності зображень, нейромережі також досягли значних успіхів. З появою згорткових нейромереж розпочалися експерименти у вивченні цієї проблематики, і виявилося, що прості архітектури згорткових нейромереж дають кращі результати, ніж інші відомі методи разом.

Список літератури

1. Mather, P. M. Computer Processing of Remotely Sensed Images / Paul M. Mather and Magaly Koch. – An Introduction. West Sussex. John Wiley & Sons Ltd. 2004. – С. 1-26

ПОБУДОВА ТА АДАПТАЦІЯ БАЗОВОЇ МІЖПРЕДМЕТНОЇ ОНТОЛОГІЇ ДЛЯ РОБОТИ З РІЗНОРІДНИМИ ДАНИМИ

Пилипенко А. Г.
Харківський національний університет радіоелектроніки, Харків, Україна

Виявлення кореляційних залежностей між сутностями та об'єктами відіграє вирішальну роль у використанні онтологічних систем і графів знань. Це дає можливість отримати глибше розуміння взаємозв'язків між різними об'єктами та їх взаємодії в різних контекстах. Використовуючи потужність розширюваної міжпредметної онтології та графа знань можливо виявлення прихованих зв'язків між об'єктами, допомагаючи ідентифікувати ланцюги, що призводять то певних змін в їнщих об'єктах, що напряму з вхідними даними не пов'язані.

Метою цієї доповіді є аналіз проблеми побудови нової та адаптації існуючих онтологій до включення різнорідних даних з окремих доменів та уможливлення подальшого динамічного розширення такої онтолгії в процесі її використання та безперевної адаптації до нових даних на основі підтверджених кореляційних залежностей.

Для глибокого пошуку кореляцій необхідна побудова нової, чи об'єднання кількох предметних онтологій в одну мідпредметну, що матиме здатність до розширення через аналіз вхідних даних та зворотній зв'язок в системі. В доповіді наводяться деякі підходи до побудови такої онтології через операції, що зберігають правильність, для систематичного введення типів і підтипових відношень у таксономічні структури [1]. Також аналізуються способи підтримання в актуальному стані, розширення зв'язків та адаптації онтології за допомогою класифікація сутностей домену в концепції верхнього рівня через комбінації термінів, що представляють сутності домену, та їх неформальних визначень [2] та інших.

Створення базової міжпредметної онтології відбувається на основі існуючих предметних онтологій, є ітеративним. В подальшому онтологія, так само як графу знань доповнюється та уточнюється постійно на основі аналізу нових вхідних даних за допомогою класичних експертів та сучасних інформаційних моделей та методів.

Список літератури

1. Jeferson O. Batista, João Paulo A. Almeida, Eduardo Zambon, Giancarlo Guizzardi. Ontologically correct taxonomies by construction. Data & Knowledge Engineering, 2022, T. 139, DOI: https://doi.org/10.1016/j.datak.2022.102012.
2. Alcides Lopes, Joel Carbonera, Daniela Schmidt, Luan Garcia, Fabricio Rodrigues, Mara Abel. Using terms and informal definitions to classify domain entities into top-level ontology concepts: An approach based on language models. Knowledge-Based Systems, 2023, T. 265, DOI: https://doi.org/10.1016/j.knosys.2023.110385.

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА АВТОМАТИЗАЦІЮ УПРАВЛІНСЬКИХ ПРОЦЕСІВ

Калугіна В. М., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Штучний інтелект став невід'ємною частиною нашого життя, трансформуючи різні галузі та революціонізуючи спосіб взаємодії з технологіями. Ця галузь науки розвиває методи та технології, які дозволяють комп'ютерам розуміти, аналізувати та вирішувати завдання, імітуючи людський інтелект. Вплив штучного інтелекту на управлінські процеси є суттєвим, оскільки відкриває нові можливості для сучасного управління багатьма сферами життєдіяльності суспільства, тому дослідження управлінських аспектів використання штучного інтелекту не викликає сумнівів. Із завданням впровадження штучного інтелекту для автоматизації завдань та оптимізації прийняття рішень пов'язаний динамізм зовнішнього середовища. Завдяки здатності штучного інтелекту аналізувати великі обсяги інформації, створювати стратегії і прогнози, приймати більш обґрунтовані рішення та надавати рекомендації або альтернативні варіанти для прийняття рішень, можна досягти підвищення продуктивності та ефективності різноманітних процесів.

Метою доповіді є розгляд застосування штучного інтелекту для автоматизації вирішення рутинних завдань та оптимізації прийняття рішень.

В доповіді наводяться результати теоретичного аналізу переваг і викликів використання інтелектуальних машин для вирішення певних рутинних людських завдань. Наведені дані показують, що масштабний успіх у використанні цієї технології здається ймовірним і покращить життя багатьох людей. Штучний інтелект дозволяє автоматизувати такі рутинні завдання як обробка даних, сортування та архівація документів, перевірка і контроль якості, планування певних подій, пошук інформації, збір та аналіз відомостей, розраховує успіх і ризики, пропонує самостійно прийняті оптимальні варіанти важливих управлінських рішень, які раніше могли бути здійсненні лише людиною або вимагали її постійного втручання. Використання технологій штучного інтелекту надає змогу людині досягти більшого успіху, зекономити час та зусилля, направити свої сили для більш важливих і творчих завдань, але варто враховувати, що не варто зловживати його використанням, оскільки, незважаючи на значні переваги, існують й виклики такі як порушення етичних питань, відсутність критичного мислення, вплив на ринок праці, загроза безпеці даних і вартість обслуговування. Проте однозначно можна вважати, що за умови правильного і контрольованого користування можливостями штучного інтелекту, він принесе користь людству.

Список літератури

1. Stuart R. Artificial Intelligence: A Modern Approach / R. Stuart, N. Peter., 2006. – 1132 с. https://people.engr.tamu.edu/guni/csce421/files/AI_Russell_Norvig.pdf

2. Вплив штучного інтелекту на розв'язання проблем HCI: виклики та можливості [Електр. ресурс]. – 2020. – URL: https://ts2.space/uk
3. Використання технологій штучного інтелекту в управлінні: переваги і загрози [Електр. ресурс]. – 2016. – URL: http://www.spilnota.net.ua/ua/article/id-1671/.

ІНТЕГРАЦІЯ 5G ТЕХНОЛОГІЙ У ПІДПРИЄМНИЦЬКУ СФЕРУ

Лященко В. О., Показій К. О., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Швидкісні можливості, які надає технологія 5G, відкривають нові горизонти для підприємницької діяльності. Зокрема, вони дозволяють реалізувати високоякісний відеострімінг, додатки віртуальної реальності, автономні транспортні засоби та інші інноваційні рішення. Це може призвести до підвищення продуктивності роботи підприємств та збільшення їх конкурентоспроможності на ринку [1].

Паралельно з розвитком технології 5G, зростають кіберзагрози, які можуть впливати на стабільність та безпеку мереж. Швидкість передачі даних, яку надає 5G, може бути використана зловмисниками для швидкого розповсюдження шкідливого ПЗ або проведення DDoS-атак. Важливо, щоб підприємства розуміли ці ризики та активно інвестували в заходи забезпечення безпеки, такі як сучасні системи захисту, шифрування даних та регулярне тестування на проникнення. Тільки комплексний підхід до безпеки може гарантувати, що переваги, які надає 5G, не будуть затьмарені потенційними загрозами [2].

Метою доповіді є аналіз можливостей, які надає технологія 5G для підприємницької діяльності, а також розгляд потенційних загроз безпеці, пов'язаних із її впровадженням.

В доповіді розглядаються основні напрямки використання 5G в бізнесі, а також потенційні ризики для безпеки корпоративних мереж. Особлива увага приділяється питанням захисту від кібератак та забезпечення конфіденційності корпоративної інформації. З розвитком 5G та збільшенням кількості підключених пристроїв, зокрема в рамках IoT, "площа атаки" для потенційних зловмисників розширюється, що збільшує кіберзагрози та вимагає від компаній більш ретельного підходу до кібербезпеки.

Список літератури

1. Петренко О. О., Ляшко О. Т. Аналіз можливостей використання технології 5G в підприємницькій діяльності. Науковий журнал «Телекомунікації». 2022. Т. 5, № 2. С. 45–50.
2. Шевченко Ю. І. Виклики та загрози безпеки при впровадженні технології 5G. Журнал «Безпека інформації». 2023. Т. 7, № 1. С. 10–15.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ УПРАВЛІННЯ ДЛЯ ПРИЙНЯТТЯ РІШЕНЬ

Кондрацький Г. О., Дригач К. В., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Штучний інтелект (ШІ) - це галузь комп'ютерних наук, що вивчає та розробляє системи та технології, які дозволяють комп'ютерам та програмам виявляти імітувати інтелектуальні функції, які зазвичай пов'язані з розумними діями людей.

Штучний інтелект може бути надзвичайно корисним для прийняття рішень у реальному часі в різних галузях та сферах діяльності. Ця здатність відкриває перед нами безліч можливостей і переваг, та може бути надзвичайно корисним для прийняття рішень на основі великих обсягів даних, які неможливо обробити людині[1].

Також він може бути вельми корисним для прийняття рішень у складних ситуаціях, де людські рішення можуть бути недостатньо точними або об'єктивними.

Метою доповіді є аналіз ролі та можливостей використання штучного інтелекту в системах управління для прийняття рішень. Також проаналізовано, як штучний інтелект може використовуватися для підвищення ефективності та продуктивності, а також для прийняття більш обґрунтованих рішень у складних ситуаціях.

В доповіді досліджені основні види систем управління, в яких може бути використаний штучний інтелект.

Системи управління - це складні комплекси обладнання, програмного забезпечення та алгоритмів, які використовують технології штучного інтелекту для керування певними процесами, системами або об'єктами. Окремо можна зазначити що, штучний інтелект має потенціал для революціонізації систем управління для прийняття рішень.

Однак, перш ніж його можна буде широко використовувати в системах управління, необхідно вирішити ряд проблем, таких як вартість, необхідність даних і необхідність розуміння ШІ [2].

Список літератури

1. Нопонен Н. Використання штучного інтелекту в менеджменті [Електронний ресурс] / Ніл Нопонен. – 2019. – Режим доступу до ресурсу: https://www.researchgate.net/publication/338554514_Impact_of_Artificial_Intelligence_on_Management.

2. Кумар А. Прикладний штучний інтелект в менеджменті майбутнього [Електронний ресурс] / Арул Кумар. – 2018. – Режим доступу до ресурсу: https://www.academia.edu/38498657/Applicalion_of_Artifcial_lntelligenl%20in%20the%20%D1%82%20anagem%20entintheJuturepdf.

ОПТИМІЗАЦІЯ БІЗНЕС-ПРОЦЕСІВ ЗА ДОПОМОГОЮ АНАЛІЗУ ДАНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кондрацький Г. О., Дригач К. В., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Підприємство є загальною системою, у якій протікають багато пов'язаних процесів, які впливають на стан всієї організаційної системи в цілому. Але певні дії, які виконуються під час процесу, визначають стан, у якому перебуває система.

У свою чергу різні стани викликають різні подальші дії, які проходять через логічно послідовний процес. Ресурси, які використовуються в процесі, змінюються.

Обробка даних є важливою частиною сучасного бізнесу. Для підприємств у конкурентному світі оптимізація бізнес-процесів за допомогою аналізу даних і інформаційних технологій є стратегічно важливою. Ця доповідь присвячена аналізу впливу інформаційних технологій та аналізу даних на оптимізацію бізнес-процесів, виявлення проблем, які можуть виникнути під час цього процесу, і розгляду потенційних рішень [1].

Метою доповіді є оптимізація бізнес-процесів за допомогою аналізу даних та інформаційних технологій.

Сучасні компанії генерують величезний обсяг даних щодня. Аналіз цих даних виявляє тенденції, проблеми та можливості оптимізації. Аналіз даних включає статистичні методи, машинне навчання та інші аналітичні інструменти.

Ефективне управління масивами даних вимагає вжиття заходів, які гарантуватимуть їх конфіденційність і захист від небажаного доступу, адже будь-яке порушення може призвести до значних проблем. Складність інтеграції різноманітних інформаційних систем і платформ є критичною для поліпшення бізнес-процесів.

Втім, цей процес може бути складним, і невдачі в інтеграції можуть негативно вплинути на ефективність бізнесу. Застосування новітніх методів і технологій залежить від компетентності та професійного розвитку співробітників, і без адекватної підготовки можливості для удосконалення бізнес-операцій можуть бути обмежені [2].

Список літератури

1. Антоненко В.М. Сучасні інформаційні системи і технології: управління знаннями : навч. посібник / В.М. Антоненко, С.Д. Мамченко, Ю.В. Рогушина. – Ірпінь : Нац. університет ДПС України, 2016. – 212 с

2. Василевська А.О. Роль інформаційних технологій в управлінні проектами / А.О. Василевська // Науковий вісник Полтавського університету економіки і торгівлі. – № 2 (47). – 2011. – С. 139–142.

АДАПТИВНІ АЛГОРИТМИ ДЛЯ ШВИДКОЇ ТА ДОСТОВІРНОЇ ОБРОБКИ ДАНИХ У РЕАЛЬНОМУ ЧАСІ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Кондрацький Г. О., Дригач К. В., Гук А. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Обробка даних в режимі реального часу є однією з ключових функцій сучасних комп'ютерних систем та мереж, що виконується з високою швидкістю та значенням.

Завдання полягає у швидкому аналізі, обробці та реакції на поступові дані, де навіть мілісекунди мають важливе значення, тому системи мають бути оптимізовані для надійної роботи в цих умовах [1].

Сучасні алгоритми, що працюють в реальному часі, є незамінними у світі, де пріоритетами є швидкість та точність. Вони надають можливість для більш продуктивної обробки даних, порівняно з класичними методами, та здатні адаптуватися до змін у вхідних даних та умовах, що гарантує високу точність обробки даних у складних ситуаціях [2].

Мета доповіді полягає в тому, щоб розкрити основні поняття, принципи роботи та застосування адаптивних алгоритмів для швидкої та достовірної обробки даних у реальному часі, демонструючи при цьому інноваційний потенціал цих алгоритмів у вирішенні сучасних завдань обробки інформації.

У доповіді висвітлені ключові концепції та практичне застосування цих алгоритмів для швидкої та точної обробки даних. Важливість цих алгоритмів у сучасному технологічному контексті не можна недооцінювати, оскільки вони розширюють можливості в таких сферах, як управління процесами, штучний інтелект, віртуальна реальність та багато інших. Ці методи перевищують традиційні підходи, надаючи змогу ефективно вирішувати завдання обробки даних в реальному часі, відповідаючи на зміни у вхідних даних та середовищі.

Список літератури

1. Дерев'янко І. В. АДАПТИВНІ АЛГОРИТМИ ДЛЯ ШВИДКОЇ ТА ДОСТОВІРНОЇ ОБРОБКИ ДАНИХ У РЕАЛЬНОМУ ЧАСІ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ / Ігор Валерійович Дерев\'янко. – Дніпро: Видавничий центр «Академія», 2003. – 324 с. – (науково-технічний журнал «Наука та будівництво»). – (5; кн. 3).Haykin S. Adaptive Filter Theory / Simon Haykin., 1986. – 177 с.

2. Волошин М. І. Адаптивні алгоритми та їх види / Максим Іванович Волошин. – Київ: «Знання», 2009. – 204 с. – (Вісник Національного технічного університету України «Київський політехнічний інститут»). – (3; кн. 1).

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ МОДЕЛІ «TRANSFORMER» ДЛЯ ВИЯВЛЕННЯ ВТРУЧАННЯ В КОМП'ЮТЕРНІ МРЕЖІ

Гавриленко С. Ю., Полторацький В. О.
Національний технічний університет "ХПІ", Харків, Україна

Системи виявлення вторгнень в комп'ютерні мережі базуються на використанні методів машинного навчання (МН). Одним із найбільш популярним напрямком МН є методи глибокого навчання.

Моделі глибокого навчання володіють властивістю автоматичного вивчення внутрішньої репрезентації ознак з наданих даних, надаючи їм значущий підхід для розв'язання завдань, які вимагають складних аналізів. В сфері глибокого навчання найсучаснішою архітектурою є Трансформер (Transformer). Трансформер – модель нейронної мережі яка спеціалізується на процесі глибокого навчання з використанням механізму «уваги» до кожного елементу в отриманому наборі вхідних даних. Ця архітектура стала революційним кроком у сфері обробки природної мови (Natural Language Processing, NLP) і застосовується у різних завданнях, таких як машинний переклад, аналіз тональності тексту, генерація тексту та багато інших.

У рамках проведених досліджень були побудовані моделі виявлення вторгнень в комп'ютерні мережі які базуються на методах Vision Transformer (ViT) та Vision Transformer For Small-size Datasets (ViTSD). Запропоновано процедуру перетворення табличних вихідних даних у спеціальний формат зображень, необхідний для роботи моделей.

З метою порівняння ефективності, ті ж дані були також піддані класифікації за допомогою інших алгоритмів, зокрема: Support Vector Machines та K-nearest neighbors. Це дозволило оцінити та порівняти результати різних методів та підходів у задачі класифікації з використанням нейронних мереж та традиційних алгоритмів машинного навчання.

Дослідження показали, що завдяки застосуванню архітектури Трансформер суттєво зросла точність класифікації. Зокрема, показник точності (accuracy) для класифікатора SVM досяг 0,910, у KNN — 0,933, ViT – 0,973 тоді як ViTSD показав найвищу точність 0,987.

Список літератури

1. Ahmad, Zeeshan & Shahid Khan, Adnan & Shiang, Cheah & Ahmad, Farhan. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies. 32. 10.1002/ett.4150.

2. Vaswani, Ashish & Shazeer, Noam & Parmar, Niki & Uszkoreit, Jakob & Jones, Llion & Gomez, Aidan & Kaiser, Lukasz & Polosukhin, Illia, "Attention is all you need", 2017. NIPS'17: Proceedings of the 31st International Conference on Neural Information Processing Systems.

3. Lee, Seung & Lee, Seunghyun & Song, Byung. "Vision Transformer for Small-Size Datasets". arXiv:2112.13492v1 [cs.CV] 27 Dec 2021

МЕТОДИ ОБРОБКИ ДАНИХ НА ОСНОВІ РЕЗУЛЬТАТІВ МОНІТОРИНГУ

Гармаш В. С., Климова І. М.
Харківський національний університет радіоелектроніки, Харків, Україна

Моніторинг систем – це ключовий елемент у забезпеченні їх надійності та ефективності. Через моніторинг отримується велика кількість даних, які потребують детальної обробки для подальшого використання. Методи обробки даних включають в себе декілька етапів, які дозволяють перетворити сиру інформацію в ціннісні дані для прийняття рішень. Результати моніторингу є критичними для прийняття обґрунтованих рішень у різних галузях, від охорони здоров'я до екології, від інформаційних технологій до урядового планування. Щоб перетворити великі та часто непорівнянні набори даних, отримані завдяки моніторингу, на корисну інформацію, використовуються різноманітні методи обробки даних [1].

Метою доповіді є аналіз існуючих методів обробки даних, які отримані завдяки моніторингу. В доповіді наводяться результати досліджень. На першому етапі проводиться збір та інтеграція даних по результатах моніторингу. Це можуть бути сенсори, логи систем, бази даних, API та інші сервіси. Після збору даних необхідно їх інтегрувати у єдину систему для подальшої обробки. Передопрацювання включає в себе виправлення помилок, видалення шуму, нормалізацію та трансформацію даних. Ці кроки допомагають підготувати дані до аналізу, забезпечуючи їх чистоту та релевантність. На етапі аналізу даних використовуються статистичні методи та алгоритми машинного навчання для виявлення закономірностей та аномалій у даних. Методи аналізу можуть включати в себе класифікацію, кластеризацію, регресійний аналіз тощо. Ще одним важливим інструментом є візуалізація [2], яка дозволяє зрозуміти дані на інтуїтивному рівні. За допомогою графіків, діаграм, теплових карт та інших засобів візуалізації користувачі можуть легше виявляти тенденції та здійснювати порівняльний аналіз. На етапі інтерпретації результатів аналітики та експерти роблять висновки та рекомендації на основі оброблених даних. Ефективна обробка даних є критично важливою для розуміння та управління системами. Завдяки правильному використанню методів обробки даних можливо покращити якість прийняття рішень та оптимізувати процеси. Сучасні інструменти та технології надають широкі можливості для аналітиків у цій області.

Список літератури

1. Hey T., Tansley S., Tolle K. The fourth paradigm: Data-intensive scientific discovery // Microsoft Research. 284 p.

2. Few S. "Now You See It: Simple Visualization Techniques for Quantitative Analysis"// Analytics Press, 2021, 301 p.

РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНОГО ДОСЛІДЖЕННЯ НАБЛИЖЕНИХ АЛГОРИТМІВ РІШЕННЯ ЗАДАЧІ ЦІЛОЧИСЕЛЬНОГО ЛІНІЙНОГО ПРОГРАМУВАННЯ З БУЛЕВИМИ ЗМІННИМИ НА ОСНОВІ РАНГОВОГО ПІДХОДУ

Рибальченко А. О.
Національний технічний університет "ХПІ", Харків, Україна

Відомо, що для оптимізації розподілення фрагментів бази даних (БД) в хмарній мережі необхідно зменшувати середній об’єм передачі даних. Тому, запропоновано використовувати наближені алгоритми рангового підходу (РП) до рішення задачі цілочисельного лінійного програмування (ЦЛП) з булевими змінними (БЗ) [1-2].

Метою доповіді є експериментальне дослідження наближених алгоритмів рішення задачі ЦЛП з БЗ на основі РП.

Порівняльний аналіз розроблених алгоритмів з відомими за вибраними показниками ефективності показав, що їх часова складність істотним чином залежить від рангу оптимального рішення, який може належати одній з трьох умовно виділених зон. Тому, об’єктивне порівняння алгоритмів можливо лише для рішень, що належать одній і тій же зоні. З порівняння рішень за зонами можливо побачити, що найбільший виграш розроблені алгоритми дають у другій зоні, де число припустимих рішень експоненціально, що є важливою перевагою у порівнянні з відомими. Дослідження погрішності наближених алгоритмів показало, що із збільшенням розмірності вирішуваної тестової задачі, вона стабілізується і для різних стратегій відсікання лежить у межах від 1 до 10%. Результати імітаційного моделювання показали, що при рівні оперативності $P \geq 0{,}9$ у даний час забезпечення розрахунками етапу оптимального планування можливо тільки алгоритмами з тимчасовою складністю $O(n)$ та алгоритм, який забезпечує задану точність обчислень при припустимих часових і ресурсних витратах. Застосування точних алгоритмів можливо при невеликій розмірності задачі розподілу – до 250 вершин графу, алгоритмів з часовою складністю $O(n^2)$ до 400.

Список літератури

1. Використання методів рангового підходу в моделі транзакційної системи з реплікацією фрагментів бази даних для розгортання у хмарному середовищі / О. Коломійцев та ін. InterConf. 2023. № 38(175). С. 326-341.

3. Голубничий Д.Ю. Інформаційна технологія відсікання неперспективних варіантів в алгоритмах рішення задачі цілочисельного лінійного програмування з булевими змінними на основі рангового підходу: кол. монографія / Д.Ю. Голубничий, О.В. Коломійцев, В.Ф. Третяк, О.В. Сальник, С.М. Хабоша // Boston: International Science Groupe, 2023. – Pp. 177-189.

УДОСКОНАЛЕННЯ ВЕБ-ЗАСТОСУНКІВ ІЗ ЗАСТОСУВАННЯМ МЕТОДІВ БЕЗПЕРЕРВНОЇ ІНТЕГРАЦІЇ ТА ПОСТАЧАННЯ

Діденко С. С., Голубничий Д. Ю.
Харківський національний економічний університет
імені Семена Кузнеця, Харків, Україна
Коломійцев О. В., Бречко В. О., Коломійцев В. О.
Національний технічний університет
«Харківський політехнічний університет», Харків, Україна

Останнім часом, використання різних середовищ для виробництва коду, розробки та тестування, коли кілька змін коду надсилаються одночасно стало широко популярною практикою. Методологія Development and Operations (DevOps), яка активно сприяє взаємодії та інтеграції між програмістами, тестувальниками та системними адміністраторами, виникла з метою швидкого створення та оновлення програмних продуктів і сервісів. Такий підхід вимагає постійного моніторингу у режимі реального часу для успішної реалізації [1].

Методологія DevOps означає буквальне злиття двох раніше роз'єднаних процесів: розробки та експлуатації програмного продукту. Раніше ці дві групи працювали у окремих сферах з обмеженою взаємодією, обумовленою ідеологічними різницями та різними компетенціями. Даний розрив створював проблеми з тривалими циклами забезпечення якості та обмеженими можливостями виробничих розгортань. Методологія Agile та безперервна інтеграція і постачання (CI/CD) є важливою частиною DevOps [2].

Метою доповіді є використання методів безперервної інтеграції та постачання для удосконалення веб-застосунків.

В доповіді наводяться результати розробки веб-застосунків з використанням стеку MEAN. Проаналізовано два підходи до впровадження безперервної інтеграції та постачання: GitLab CI/CD + Heroku та GitHub Actions + AWS EC2. Отримані результати вказують на те, що автоматизований процес CI/CD може значно покращити процес розробки програмного забезпечення, надаючи командам швидкий зворотний зв'язок щодо їхньої останньої роботи і сприяючи покращенню якості коду та прискоренню доставки.

Список літератури

1. Ankita Patil, Mitesh Soni. Hands-on Pipeline as Code with Jenkins: CI/CD Implementation for Mobile, Web, and Hybrid Applications Using Declarative Pipeline in Jenkins. – BPB Publications, 2021. – 516 с.

2. What is CI/CD? Continuous integration and continuous delivery explained [Електронний ресурс] // Infoworld. – 2022. – Режим доступу: https://www.infoworld.com/article/3271126/.

ПРОПОЗИЦІЇ ЩОДО ЗАСТОСУВАННЯ ГЕОМЕТРИЧНО НЕОДНОРІДНОГО РАДІОІЗОТОПНОГО ПОКРИТТЯ ДЛЯ ПОГЛИНАННЯ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ

Катунін А. М.
Національний університет цивільного захисту України, Харків, Україна
Коломійцев О. В.
Національний технічний університет "ХПІ", Харків, Україна

Відома значна кількість методів щодо поглинання електромагнітних випромінювань [1]. Так, існує метод на основі використання перколяційного покриття, у якому фізичною реалізацією перколяційного покриття є неврегульовані суміші з високо- і низькопровідних частинок. Однак, більшість методів характеризується вузьким діапазоном довжин хвиль електромагнітних випромінювань, у якому здійснюється поглинання.

Метою роботи є розробка пропозицій щодо застосування геометрично неоднорідного радіоізотопного покриття для поглинання електромагнітних випромінювань.

В доповіді розкрито сутність запропонованих пропозицій щодо поглинання електромагнітних випромінювань у широкому діапазоні. Їх сутність полягає у додатковому нанесенні геометрично неоднорідної структури (дифракційної відбивної решітки) на шар радіоізотопного композитномого покриття хвиль. Завдяки чому формується в геометрично неоднорідне радіоізотопне композитне покриття. Отже, можливо збільшити поглинання електромагнітних випромінювань одночасно в радіо- і оптичному діапазонах довжин хвиль за рахунок одночасної дії декількох фізичних явищ та процесів, які мають максимальний ефект у різних ділянках діапазону довжин хвиль. Загасання випромінювань радіодіапазону забезпечується розсіюванням хвиль на неоднорідностях провідностей матеріалу покриття, α – радіоактивних вкрапленнях радіоізотопного композитного покриття; загасанням хвиль за рахунок іонізації прилеглого до радіоізотопного композитного покриття шару оточуючого середовища, на треках α – часток; перетворенням випромінювань на нелінійності радіоізотопного композитного покриття.

Таким чином, загасання електромагнітних випромінювань оптичного діапазону здійснюється шляхом перерозподілу енергії в просторі.

Список літератури

1. Катунін, А., Коломійцев, О., Пустоваров, В. і Олійник, Р. (2023) «Можливості щодо використання методів керування дифракцією оптичного випромінювання на відбивних покриттях озброєння та військової техніки для її захисту від боєприпасів із напівактивними лазерними системами наведення», *Збірник наукових праць
Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*, 15(1), С. 62-67. doi: 10.37701/dndivsovt.15.2023.08.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТІ

Кірвас В. А.
Харківський гуманітарний університет «Народна українська академія»,
Харків, Україна

Відомо що в освіті сучасні дослідження зосереджені на цифровій трансформації навчання, формування та розвиток цифрових компетенцій.

Термін «штучний інтелект» (ШІ) вперше був згаданий Джоном Маккарті ще у 1956 році. ШІ розглядають тепер як машинне навчання, глибоке навчання, експертні системи, машинний зір тощо. Передові університети вже використовують інструменти ШІ.

Одним з складових ШІ є генеративний ШІ, який може створювати тексти, зображення, відео, музику, і т. д. Сьогодні вже доступні багато генеративних ШІ. Наприклад, вдосконалена генеративна модель ШІ – ChatGPT, заснована на архітектурі генеративного попередньо навченого перетворювача (GPT), яка, після текстового запрошення створює відповіді, подібні до людських. Це досягається за рахунок обробки природної мови, і завдяки цьому процесу результат стає у більшості випадків контекстуально релевантним і майже не відрізняється від людського тексту. На сьогодні доступні дві версії: ChatGPT3,5 – безкоштовна, та коштовна версія GPT-4, яка працює набагато краще, ніж її попередник. Успішно розробляється і скоро вийде версія GPT-5. Багато дослідників стверджують, що з появою ChatGPT освіта, можливо, отримає одну з найзначніших трансформацій за всю історію.

ChatGPT може використовуватися в освіті як викладачами, так і студентами для досягнення цілей прискореного навчання. З допомогою ChatGPT можна: проводити дослідження та іспити з певної теми; складати та планувати програми навчальних дисциплін; швидко підготувати питання з кількома варіантами відповідей, отримати допомогу при оцінюванні академічних успіхів та заохочувати критичне мислення студентів; узагальнювати великі текстові розділи, пояснювати теми для конкретних потреб читачів тощо. ChatGPT є надзвичайно корисним інструментом, який має величезний потенціал у сфері освіти. Наприклад, він також допомагає забезпечити індивідуальний підхід до навчання; добре допомагає при написанні листа; корисний при освоєнні та перекладі мов; надає допомогу при програмуванні – створює та перекладає код.

Однак є і недоліки використання ChatGPT в освіті: великі побоювання з приводу плагіату; упередженість відповідей ШІ (систематичні та необґрунтовані припущення), через обмеження лише кількома джерелами; багато обговорень з приводу питань конфіденційності. Крім того, він також може видавати невірні твердження, генерує несподівані чи безглузді результати, які він вважає дійсними з високим ступенем достовірності. Ця характеристика відома як галюцинація ШІ. Тому необхідно обов'язково перевіряти конкретну інформацію, і тоді можна впоратися з цими проблемами.

Взагалі ChatGPT, як стверджують багато дослідників, приносить більше користі, ніж недоліків освіти. І традиційна оцінка успіхів навчання змінюватиметься, а допуск таких революційних інструментів до студентської аудиторії не за горами.

PROPOSALS FOR CONTROLLING THE FLIGHTS OF UNMANNED AERIAL VEHICLES IN URBAN AREAS USING INFORMATION TECHNOLOGY

Kolomiitsev O. V., Rudakov I. S.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
Tretiak V. F., Kuleshov O. V., Kalachova V. V.
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
Komarov V. O.
Kruty Heroes Military Institute
of Telecommunications and Information Technology, Kyiv, Ukraine
Pustovarov V. V.
State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine

Currently, one of the most effective techniques for providing monitoring services for various urban aspects is the use of cellular technology, which is formed by a small unmanned aerial vehicle (drone). The main advantages of drones include their ease of deployment, low acquisition and maintenance costs, a variety of payloads, high manoeuvrability and hovering capabilities. However, urban development poses a risk of collisions between drones and other aircraft, etc. Drone management must ensure flight safety and avoid conflicts in the air.

Thus, the use of methods and models of machine (deep) learning to control drones in the urban environment is an urgent scientific task.

The purpose of the report is to work out scientific and technical proposals for controlling the flights of unmanned aerial vehicles (drones) in urban areas using information technologies**.**

The report analyses well-known machine (deep) learning methods and models for controlling drones in the urban environment. Based on the analysis, a number of scientific and technical proposals have been developed to use machine and deep learning technology to detect obstacles, etc. and to analyse data from sensors and video cameras to ensure the safety of drone flights.

References

1. Голубничий Д. Ю. Інформаційна технологія відсікання неперспективних варіантів в алгоритмах рішення задачі цілочисельного лінійного програмування з булевими змінними на основі рангового підходу / Д. Ю. Голубничий, О. В. Коломійцев, В. Ф. Третяк та ін. // Theoretical foundations in research in Engineering : collective monograph. – Boston (USA), 2022. – С. 96–133.

ПРОПОЗИЦІЇ ЩОДО ЗНИЖЕННЯ ШУМУ ТУРБОРЕАКТИВНИХ ДВОКОНТУРНИХ ДВИГУНІВ З НАДВИСОКИМ СТУПЕНЕМ ДВОКОНТУРНОСТІ ШЛЯХОМ ЗАСТОСУВАННЯ ЗВУКОПОГЛИНАЮЧИХ ТА ЗВУКОРОЗСІЮВАЧИХ КОНСТРУКЦІЙ

Комаров В. О.
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут, Київ, Україна
Коломійцев О. В.
Національний технічний університет
«Харківський політехнічний університет», Харків, Україна
Дмітрієв О. М., Мажаров В. С., Падалка І. О.
Льотна академія Національного авіаційного університету,
Кропивницький, Україна

На даний час газотурбінні двигуни (ГТД) високотехнологічні та суттєво перевершують за своїми характеристиками традиційні двигуни внутрішнього згоряння. Основне своє поширення ГТД отримали в авіаційній промисловості, а у автомобільній – не одержали у зв'язку з проблемами зі споживанням палива, крім танкобудування. Існують два основних способи боротьби з шумом ГТД, що встановлені на літальні апарати (ЛА): зниження шуму у джерелі та зниження шуму на шляхах його поширення шляхом використання звукопоглинаючих конструкцій (ЗПК).

Метою доповіді є розробка науково-технічних пропозицій щодо зниження шуму турбореактивних двоконтурних двигунів з надвисоким ступенем двоконтурності.

В доповіді проведено аналіз основних методів, способів та ЗПК для зниження шуму в ГТД. На основі проведеного аналізу використання ЗПК встановлено, що розширюється діапазон звукопоглинання шуму, але суттєво збільшується вага мотогондолі, що облицьована ЗПК. Для зменшення ваги ЗПК, пропонується зменшити кількість багатошарових ЗПК за рахунок використання комбінованих методів облицювання внутрішньої поверхні мотогондолі двоконтурного турбореактивного двигуна з надвисоким ступенем двоконтурності, насамперед, за рахунок установки на двигун (у мотогондолу), у комплексі, звукопоглинаючих та звукорозсіювачих конструкцій.

Список літератури

1. Коломійцев О.В., Комаров В.О. Застосування звукопоглинаючих та звукорозсіювачих конструкцій для зниження шуму турбореактивних двоконтурних двигунів з надвисоким ступенем двоконтурності. *The 7th International scientific and practical conference "Global problems of improving scientific inventions"* (October 31 – November 03, 2023) Copenhagen, Denmark. International Science Group. 2023. P. 287-296. URL: https://isg-konf.com/global-problems-of-improving-scientific-inventions/

УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 3, 4, додаткові)

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Азербайджанський технічний університет, Баку, Азербайджан
Академія Державної прикордонної служби, Баку, Азербайджан
Академія міністерства надзвичайних ситуацій, Баку, Азербайджан
Військовий інститут імені Гейдара Алієва, Баку, Азербайджан
Громадська організація "Чисті серця Калуш", Калуш, Україна
Державний біотехнологічний університет, Харків, Україна
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
Державний університет інфраструктури та технологій, Київ, Україна
Інститут геології і геофізики Азербайджанської НАН, Баку, Азербайджан
Інститут проблем математичних машин та систем НАН України, Київ
Інститут систем управління Азербайджанської НАН, Баку, Азербайджан
Кіровоградська льотна академія, Кропивницький, Україна
Національна академія Національної гвардії України, Харків, Україна
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна
Національний авіаційний університет, Київ, Україна
Національний аерокосмічний університет імені М. Є. Жуковського "Харківський авіаційний інститут", Харків, Україна
Національний технічний університет "ХПІ", Харків, Україна
Національний університет оборони, Баку, Азербайджан
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
Національний університет цивільного захисту України, Харків, Україна
Національний університет "Чернігівська політехніка", Чернігів, Україна
Представництво «Оракл Іст Сентрал Юроп Сервісис Б.В.», Київ, Україна
Університет технології і гуманітарних наук, Бельсько-Бяла, Польща
Управління метрології та стандартизації, Київ, Україна
Харківський військовий інститут танкових військ, Харків, Україна
Харківський національний автомобільно-дорожній університет, Україна
Харківський національний економічний університет ім. С. Кузнеця, Україна
Харківський національний університет внутрішніх справ, Харків, Україна
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Харківський національний університет міського господарства імені О. М. Бекетова, Харків, Україна
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна
Харківський національний університет радіоелектроніки, Харків, Україна
Черкаський державний технологічний університет, Черкаси, Україна
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля, Україна
Черкаський національний університет імені Б. Хмельницького, Україна

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

ЗМІСТ

НАУКОВЕ ВИДАННЯ

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей
одинадцятої міжнародної науково-технічної конференції
(16 – 17 листопада 2023 року)
Том 4: секції 3, 4 (додаткові)

Відповідальна за випуск *Н. Г. Кучук*
Технічний редактор *І. А. Лєбедева*
Коректор *В. В. Богомаз*
Комп'ютерне складання та верстання *Н. Г. Кучук, І. Ю. Петровська*

Адреса оргкомітету: вул. Кирпичова, 2, Харків, 61002, Україна
Вечірній корпус, кімната 314
тел. +38 (057) 707 61 65

Підписано до друку 16.11.2023 Формат 60 × 84/16
Ум.-вид. арк. 3,25. Тираж 100 пр. Зам. 1116-23

Віддруковано з готових оригінал-макетів у цифровій друкарні Impress
61002, м. Харків, вул. Пушкінська, 56, тел. **+ 38 (057) 714-52-11**
e-mail: **irina@impress.biz.ua**