1. NetworkX. Документація NetworkX. URL: https://networkx.org/documentation/stable/
2. Matplotlib. Документація Matplotlib. URL: https://matplotlib.org/stable/
3. Floyd R.W. Алгоритм 97: Найкоротший шлях. Communications of the ACM, 1962, 5(6), 345.
4. Prim R.C. Найкоротші мережі зв'язку та деякі узагальнення. Bell System Technical Journal, 1957, 36(6), 1389–1401.

Anotation: *The use of graph algorithms for optimizing harvest transportation logistics has been studied. Algorithms for shortest path search and minimum spanning tree have been considered, along with their implementation in Python using the NetworkX library. The efficiency of these methods for the agricultural sector has been determined, as well as the prospects for their integration with modern optimization technologies..*
Key words: *logistics optimization, crop transportation, graph algorithms, Python, NetworkX, shortest path, transportation network, agricultural sector*.

Науковий керівник:
Пархоменко О. Ю.,
к. ф.-м. н., доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет

УДК 004.056

Основні аспекти забезпечення інформаційної безпеки

Дмитро Кулєшов,
здобувач вищої освіти спеціальність 204 Технологія ВППТ
Миколаївський національний аграрний університет
м. Миколаїв, Україна

Анотація: *у роботі розглядаються основні аспекти забезпечення інформаційної безпеки. Проаналізовано методи захисту інформації в інформаційних системах.*
Ключові слова: *інформаційна безпека, конфіденційність, цілісність, доступність, аутентифікація, авторизація.*

Забезпечення інформаційної безпеки – це процес захисту інформації від несанкціонованого доступу, пошкодження, змін або знищення, а також забезпечення її доступності та цілісності.

Конфіденційність є одним із основних аспектів інформаційної безпеки. Вона передбачає захист інформації від несанкціонованого доступу, зміни чи розголошення, тобто, забезпечення того, щоб інформація була доступна тільки тим особам або системам, яким це дозволено. Важливість конфіденційності полягає в захисті чутливої інформації, що може бути предметом комерційної

таємниці, особистих даних, фінансової інформації або інших важливих відомостей. До основних принципів конфіденційності відноситься контроль доступу,

шифрування, політика мінімальних прав, аудит та моніторинг, відповідність нормативним вимогам. Загрозу конфіденційності несе несанкціонований доступ, фішинг та соціальна інженерія, витоки даних, шкідливе програмне забезпечення.

Забезпечити конфіденційність можна такими технічними засобами: шифруванням для захисту даних, механізмом двофакторної аутентифікації (2FA) для захисту доступу до облікових записів, VPN (віртуальна приватна мережа) для захищеного доступу до мережі, особливо при віддаленій роботі, системи управління доступом (наприклад, Active Directory, LDAP) для централізованого контролю доступу до ресурсів. Конфіденційність є критично важливою для збереження довіри до організацій та захисту чутливої інформації.

Ще один важливий аспект інформаційної безпеки – цілісність, що передбачає забезпечення того, щоб інформація не була змінена, пошкоджена або знищена без відповідного дозволу, як під час зберігання, так і під час передачі. Головною метою цілісності є гарантування того, що дані зберігають свою точність та достовірність і не піддаються змінам в результаті помилок або зловмисних дій. Забезпечують цілісність такі методи: хешування, цифровий підпис, контрольні суми, резервне копіювання та відновлення даних. Для забезпечення цілісності використовують такі технічні засоби як криптографія, інтеграційні контролі, надійні протоколи для передачі даних.

Доступність – це третій важливий аспект інформаційної безпеки, який гарантує, що інформація та ресурси доступні для авторизованих користувачів або систем у потрібний час. Це означає, що дані повинні бути доступні для використання, обробки та передачі без затримок і без перешкод, які можуть виникнути через відмови в роботі системи, збоїв, або атаки.

Основна мета доступності – забезпечити безперервний доступ до інформації та ресурсів, що критично важливо для нормальної роботи організацій та бізнесу, а також для своєчасного прийняття рішень. Доступність досягається за допомогою резервного копіювання та відновлення після аварії, використання балансування навантаження, мережевого і апаратного дублювання, моніторингу і управління інцидентами, захисту від атак типу "відмова в обслуговуванні", використання хмарних технологій.

Доступність є критичним компонентом інформаційної безпеки. Вона забезпечує, щоб інформація та ресурси були доступні для користувачів або систем у будь-який час, коли це необхідно. Забезпечення високої доступності є важливим аспектом для підтримки безперебійної роботи організацій та надійного обміну інформацією.

Ключові аспекти забезпечення інформаційної безпеки – це аутентифікація та авторизація, які відповідають за контроль доступу до інформаційних ресурсів. Вони допомагають визначити, хто має доступ до системи та що з цими системами можна робити. Аутентифікація та авторизація тісно взаємопов'язані.

Спочатку система перевіряє ідентичність користувача (аутентифікація), а після цього визначає, які ресурси і дії доступні цьому користувачеві (авторизація). Без правильно налаштованих аутентифікації та авторизації система може бути вразливою до атак, зловживань і витоків даних.

Аутентифікація – це процес підтвердження ідентичності користувача чи системи, що здійснюється через різні методи (паролі, біометрія, токени). Авторизація – це процес визначення прав доступу, що дозволяє користувачеві виконувати певні дії або отримувати доступ до конкретних ресурсів, після того як його ідентичність підтверджена. Використання цих двох процесів разом дозволяє забезпечити належний контроль доступу до інформаційних ресурсів та мінімізувати ризики безпеки.

В епоху цифрових технологій обсяги конфіденційних даних, таких як особисті дані, фінансова інформація та комерційні таємниці, постійно зростають. Забезпечення їхньої безпеки є критично важливим для захисту приватності та запобігання фінансовим втратам.

Інформаційні системи є основою для багатьох бізнес-процесів. Кібератаки та інші загрози можуть призвести до простоїв, втрати даних і фінансових збитків. Забезпечення інформаційної безпеки допомагає мінімізувати ці ризики та забезпечити безперервність роботи. Інформаційні системи є критично важливими для функціонування уряду, військових та інших ключових інфраструктур. Захист цих систем від кібератак є питанням національної безпеки.

Кіберзлочинність стає все більш витонченою та поширеною. Забезпечення інформаційної безпеки допомагає захистити від таких загроз, як фішинг, шкідливе програмне забезпечення та викрадення даних.

Багато країн та галузей мають закони та нормативні акти, що вимагають від організацій забезпечувати інформаційну безпеку. Дотримання цих вимог є обов'язковим для уникнення штрафів та інших юридичних наслідків. Витоки даних та інші інциденти інформаційної безпеки можуть завдати серйозної шкоди репутації організації. Забезпечення інформаційної безпеки допомагає запобігти таким інцидентам та зберегти довіру клієнтів.

Отже, забезпечення інформаційної безпеки є не просто технічним завданням, а критично важливим аспектом для всіх організацій та окремих осіб у сучасному цифровому світі.

Список використання джерел:

1. Internet Engineering Task Force (IETF). (2012*)*. The OAuth 2.0 Authorization Framework. RFC 6749. URL: https://tools.ietf.org/html/rfc6749

2. International Organization for Standardization (ISO). (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO/IEC 27001:2022. URL: https://www.iso.org/isoiec-27001-information-security.html

3. Інформаційна безпека: навчальний посібник / О.В. Корнілова, О.В. Філіпенко. – Харків: ХНУРЕ, 2020. – 204 с.

Abstract: *The article considers the main aspects of ensuring information security.*

Methods of protecting information in information systems are analyzed.
Keywords: *information security, confidentiality, integrity, availability, authentication, authorization.*

Науковий керівник:
Борян Л.О.,
старший викладач кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій,
Миколаївський національний аграрний університет

УДК 338.43:631.15:004.852

Застосування бібліотеки XGBOOST у Python для прогнозування цін на агропродукцію

Альона Куліковська,
здобувачка вищої освіти спеціальності 122 Комп'ютерні науки
Миколаївський національний аграрний університет
м. Миколаїв, Україна

Анотація: *коливання цін на агропродукцію є важливою проблемою, що вимагає застосування сучасних аналітичних методів. У роботі розглядається використання бібліотеки XGBoost для прогнозування цін на агропродукцію. Розглянуто переваги XGBoost, зокрема високу швидкість обробки, регуляризацію та гнучкість налаштувань.*
Ключові слова: *прогнозування цін, XGBoost, машинне навчання, агропродукція, обробка даних.*

У сучасних умовах коливання цін на агропродукцію є важливою проблемою для фермерів, трейдерів і аналітиків. Непередбачуваність ринкових умов вимагає використання потужних аналітичних методів для прогнозування цін. Машинне навчання пропонує ефективні інструменти, серед яких XGBoost є одним із найкращих. Бібліотека XGBoost забезпечує високу продуктивність та точність прогнозів завдяки використанню градієнтного бустингу. У роботі досліджуються особливості застосування XGBoost для прогнозування цін на агропродукцію.

XGBoost (Extreme Gradient Boosting) є потужним інструментом для побудови моделей машинного навчання, що ґрунтується на алгоритмі градієнтного бустингу дерев рішень. Однією з його видатних особливостей є висока швидкість обробки, яка досягається завдяки паралельним обчисленням та оптимізованій обробці даних. Ця ефективність дозволяє швидко обробляти великі набори даних, що робить його особливо корисним у різних аналітичних завданнях.