ІНСТИТУТ ЦИФРОВІЗАЦІЇ ОСВІТИ
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ

ЗВІТНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ ІНСТИТУТУ ЦИФРОВІЗАЦІЇ ОСВІТИ НАПН УКРАЇНИ

ЗБІРНИК МАТЕРІАЛІВ

10 лютого 2022 року
м. Київ

УДК 001:004

Рекомендовано до друку:
Вченою радою Інституту цифровізації освіти
Національної академії педагогічних наук України.
Протокол № 4 від 28.02.2022 р.

З 41 **Звітна науково-практична конференція Інституту цифровізації освіти НАПН України** : збірник матеріалів, 10 лютого 2022 р., м. Київ / упоряд.: О.П. Пінчук, Н.В. Яськова. Київ : ІЦО НАПН України, 2022. 148 с.

Організаційний комітет:

Биков В.Ю. – д-р. т. наук, проф., дійсний член НАПН України, директор ІЦО НАПН України (голова).
Литвинова С.Г. – д-р. пед. наук, с.н.с., заступниця директора з наукової роботи ІЦО НАПН України (заступник голови).

Збірник містить матеріали Звітної науково-практичної конференції. У доповідях учасників конференції визначено сучасні напрями розвитку інформаційно-комунікаційних і цифрових технологій у відкритій освіті, описано теоретичні та практичні аспекти проектування і використання сучасних засобів навчання у комп'ютерно орієнтованому середовищі, зокрема, застосування хмарних технологій в освітньому процесі.
Збірник адресований науковим і науково-педагогічним працівникам, керівниками наукових установ НАПН України, аспірантам, студентам закладів вищої освіти та для всіх, хто цікавиться використанням інформаційно-цифрових технологій у науковій і науково-педагогічній діяльності.
Матеріали надруковані в авторській редакції. За достовірність фактів, посилань, стилістичне та орфографічне оформлення відповідальність несуть автори публікацій та їх наукові керівники.

ВСТУП

Звітну науково-практичну конференцію проведено 10 лютого 2022 року на базі Інституту цифровізації освіти Національної академії педагогічних наук України.

Збірник містить матеріали виступів учасників науково-практичної конференції і стане в пригоді науковим і науково-педагогічним працівникам, керівниками наукових установ НАПН України, аспірантам, студентам закладів вищої освіти та всім, хто цікавиться використанням інформаційно-цифрових технологій у науковій і науково-педагогічній діяльності.

Мета конференції: обмін досвідом і обговорення питань інформаційно-цифрових технологій в освіті, а саме: дослідження теоретико-методичних і психолого-педагогічних проблем інформатизації освіти і науки; обґрунтування методологічних засад відкритої освіти; дослідження інформаційно-освітніх інновацій і розроблення методик їх впровадження в освітньо-наукову практику; розроблення технологій створення відкритих навчальних середовищ у закладах освіти; розроблення та науково-методичний супровід впровадження відкритих освітньо-наукових інформаційних систем, Інтернет орієнтованих баз даних; дослідження ефективності та безпечності використання комп'ютерно орієнтованих засобів навчальної, наукової й управлінської діяльності.

На конференції працювало 2 секції:

СЕКЦІЯ 1. Відкриті науково-освітні системи та компаративістика інформаційно-освітніх інновацій.

СЕКЦІЯ 2. Хмаро орієнтовані системи та технології відкритого навчального середовища.

У рамках конференції були обговорені актуальні питання щодо особливостей технологій AR/VR при їх використанні в освітньому процесі; підходи пом'якшення впливу засобів віртуальної реальності на учнів; навчання з використанням імерсивних технологій; відповідальне використання технологій доповненої і віртуальної реальності освіті; цифрові технології для оцінювання результативності педагогічних досліджень; підходи до проєктування електронної енциклопедії; виклики дистанційного та змішаного навчання, цифрова компетентність всіх учасників освітнього процесу тощо.

Тематика представлених доповідей свідчить про актуальність розроблення науково-методичного забезпечення та пошуку шляхів упровадження ІКТ у систему освіти на всіх її рівнях та проведення наукових досліджень.

Координатор конференції
Олександра СОКОЛЮК

ЗМІСТ

Попп М.І., Кривонос О.М.
Житомирський державний університет імені Івана Франка

ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ ТЕКСТОВИХ ДАНИХ

Кожному відомо, що з розвитком новітніх технологій, які базуються на численній кількості даних, світом керує інформація. Всі дані лише в межах одного комп'ютера – це програмне забезпечення і особисті дані та інформація користувача. Оскільки програмне забезпечення створене для роботи та обробки певної інформації, дані – найцінніша складова будь-якої системи. Більшість мов програмування використовують текстовий формат для подання та зберігання вихідного коду тої чи іншої програми.

Текстові дані – це послідовність певних символів, відповідно якихось наборів символів буквам алфавіту і знаків пунктуації. Кожен використаний символ зазвичай кодується у вигляді одного байта, тобто одиниці зберігання і обробки цифрової інформації. У сучасних обчислюваних системах один байт дорівнює восьми бітам, також одній з найвідоміших одиниць виміру інформації.

Якщо брати до уваги інформацію не лише в межах одного комп'ютера звичайного користувача, а базу даних певної організації, то існують дані, які не повинні виходити за межі певної організації чи компанії та дані, які можуть та мають бути опубліковані для надання інформації користувачам та надаючи змогу конкурувати на ринку. Такі дані відповідно називають внутрішньо-спрямованими та зовнішньо-спрямованими [4].

Для того, щоб захистити інформацію від зовнішнього втручання та попередити її спотворення або знищення потрібно вміти її шифрувати та дешифрувати. Для цього використовують різні алгоритми, які поєднують у собі такі науки як математика та комп'ютерні технології.

Відносно зашифрованих текстових даних та їх початкового вигляду, існують такі поняття як відкритий (вихідний) або ж чистий текст та шифротекст (шифрований або закритий текст). Відкритий текст – це дані, які передаються без використання криптографії, в той час як шифротекстом називають дані, отримані після застосування певної криптосистеми з використанням параметру шифру, такого як ключ [5].

Тож, давайте розберемося, що ж таке шифрування. Шифрування даних – це процес перетворення певної інформації для того, щоб приховати її вміст від небажаних очей. Для шифрування використовують один з двох видів алгоритмів: симетричні або асиметричні. Алгоритм криптографічного перетворення визначає собою сукупність перетворень будь-яких даних на їх зашифровану форму.

Шифрування тексту відбувається за допомогою криптографії, науці про методи забезпечення конфіденційності і автентичності інформації. Криптоаналіз, в свою чергу, наука про математичні методи порушення цієї конфіденційності та цілісності інформації, тобто вивчає способи та методи несанкціонованого дешифрування даних [5, с. 9-10]. Тож, дешифрування – це процес вилучення чистого тексту без знання криптографічного ключа для розшифровки інформації. На противагу цьому поняттю, існує термін розшифрування, що являє собою нормальне санкціоноване застосування криптографічних алгоритмів перетворення зашифрованих текстових даних у вихідний текст, знаючи ключ для здійснення даного процесу.

Методи кодування даних здійснюються за допомогою ключів. Ключ є послідовністю цифрових, буквених або ж змішаних (буквених та цифрових) символів, тобто являє собою

параметр вибору конкретного перетворення. В симетричному алгоритмі шифрування для кодування та декодування використовується пов’язані або ідентичні ключі. При асиметричному кодуванні для процесу шифрування та дешифрування використовують різні ключі, з яких один є загальнодоступним, а інший – приватний.

В симетричних криптосистемах алгоритми бувають блоковими та потоковими. В блокових алгоритмах інформація кодується поділеними на фіксований розмір даних у певній послідовності блоками. Інформація може бути зашифрована за допомогою підстановки або перестановки даних, тобто символи вихідного тексту замінюються іншими або ж міняються місцями, відповідно. В потоковому шифрі символи відкритого тексту шифруються по черзі з різними перетвореннями незалежно від інших символів

В асиметричних криптосистемах відправник, тобто сторона, яка зашифровує дані, використовує відкритий загальнодоступний ключ, тим часом як одержувач, тобто сторона, яка має на меті розшифрувати інформацію, користується приватним закритим (доступним тільки певній людині або людям) ключем.

Насправді, інформація може бути зашифрована за допомогою відкритого або ж закритого ключа, оскільки немає значення, який ключ буде використаний для кодування, а який для декодування даних, але для правильної роботи алгоритму перетворення даних в обидві сторони, потрібна наявність обох вище зазначених ключів.

Якщо говорити про те, який з вище вказаних способів є надійнішим, то з усією впевненістю можна сказати, що це асиметричний спосіб шифрування інформації, оскільки при симетричному шифруванні, якщо єдиний ключ для кодування та декодування даних буде викрадено, будь-хто зможе розшифрувати важливу інформацію, чого не можна зробити, маючи публічний ключ асиметричного шифрування.

Кожен побудований алгоритм перетворення даних має повертати однакову інформацію на одному комп’ютері, але, залежно від вимог реалізації шифрування, він може повертати інші дані на різних комп’ютерах.

Кожна з даних систем може бути зламана методом перебору існуючих ключів, але при використанні асиметричного алгоритму шифрування, це зробити набагато важче. Якщо певна система здатна протистояти втручанню інших небажаних сторін у розшифрування текстових даних, тобто зламуванню, це називається крипостійкістю алгоритму шифрування.

З розвитком технологій, багато алгоритмів стають уразливими до викриття та знаходження потрібного ключа для декодування. Для того, щоб алгоритм було складніше зламати, потрібно використовувати різні підходи до генерації та перетворень ключа, так як чим більше операцій покладено в основу алгоритму перетворення інформації, тим надійнішим вважається даний алгоритм, але на його виконання може бути витрачено більше часу, ніж на більш простий шифр.

Список використаних джерел

1. Fouché Gaines, Helen Cryptanalysis: A Study of Ciphers and Their Solution. New York: Dover Publications Inc., 1956. 259 p. Retrieved from: https://archive.org/details/cryptanalysis00hele/page/n5/mode/2up
2. Simon Lehna Singh The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Doubleday and Knopf Doubleday Publishing Group, 1999. 416 p.
3. Stephens Rod Essential Algorithms: A Practical Approach to Computer Algorithms/ R. Stephens. Indianapolis, Indiana, 2013. 624 p. Retrieved from: https://cutt.ly/YSE0slw.
4. Нильс Фергюсон, Брюс Шнайер Практическая криптография. Вильямс, 2005, 424 с.
5. Саломаа А. Криптография с открытым ключом. Пер. с англ. М.: Мир, 1995. 318 с.