DOI https://doi.org/10.32782/2521-6643-2022.1-63.4
УДК 004

Ульяновська Ю. В., кандидат технічних наук, доцент,
завідувач кафедри комп'ютерних наук
та інженерії програмного забезпечення
Університету митної справи та фінансів
ORCID: 0000-0001-5945-5251

Яковенко В. О., доктор технічних наук, доцент,
професор кафедри комп'ютерних наук
та інженерії програмного забезпечення
Університету митної справи та фінансів
ORCID: 0000-0001-7762-5410

Яковенко Т. Ю., кандидат економічних наук, доцент,
доцент кафедри комп'ютерних наук
та інженерії програмного забезпечення
Університету митної справи та фінансів
ORCID: 0000-0003-1900-8283

Рябоволенко В. А., викладач кафедри комп'ютерних наук
та інженерії програмного забезпечення
Університету митної справи та фінансів
ORCID: 0000-0002-3049-2718

РОЗРОБКА ПЛАГІНУ ДЛЯ ЗАХИСТУ ВІД ВІРУСНОЇ ІНФОРМАЦІЇ

З розвитком інформаційно-комунікаційних технологій та імплементації Інтернету майже в усіх сферах життєдіяльності суспільства виникає проблема поширення в мережі та проникнення до користувачів небажаного контенту, який може нанести користувачам як моральну, так і матеріальну шкоду. Одним зі шляхів вирішення цієї проблеми є фільтрація контенту, що надходить до користувача. Це призводить до формулювання науково-прикладного завдання щодо формування системи фільтрації контенту в Інтернеті, а також прикладного програмного забезпечення реалізації цього завдання, що зумовлює актуальність цього дослідження. Робота пов'язана з розробкою програмного забезпечення, що перевіряє текстовий Web-контент з метою виявлення шкідливих ресурсів і захисту користувачів від шкідливої інформації.

Ключові слова: *плагін, Web-контент, захист від шкідливої інформації.*

Ulianovska Yu. V., Yakovenko V. O., Yakovenko T. Yu., Riabovolenko V. A. Developing a plugin to protect against virus information

With the development of information and communication technologies and the implementation of the Internet in the almost all spheres of social life, the problem of dissemination and penetration of inappropriate content, which could cause both moral and material harm to users, arises. One of the ways to solve this problem is to filter the content coming to the user. This leads to the scientific and practical issue of developing a content filtering system on the Internet, as well as the applied software to implement this task. The significance of this issue determines the relevance of this research. The paper is related to the development of a software that checks the text content of the Web in order to identify potentially dangerous resources and protect users from unwanted information.

Key words: *plugin, Web-content, protection against unwanted information.*

Постановка проблеми. Однією з основних ознак розвитку сучасного суспільства є стрімкий розвиток інформаційних технологій, зокрема Інтернет-технологій.

Інформатизація нашого суспільства спричиняє як позитивні, так і негативні наслідки. З одного боку, користувач має доступ до великих масивів даних, можливість досить швидкого пошуку необхідної інформації, а з іншого боку, неконтрольовані вебресурси впливають на психіку, фізичне здоров'я, соціальну поведінку людей. Особливо цьому впливу піддаються молодь та підлітки.

Популярність інтернет-ресурсів, крім позитивних моментів швидкого доступу до необхідної інформації, призвела до зростання кількості порушень прав та поширення недостовірної й конфіденційної інформації. На жаль, більшість користувачів не володіють інформацією про небезпеку Інтернету й не мають сформованої онлайн-культури. Тому часто вони не розуміють, як можуть захиститися [1].

Все більше уваги громадськості та науковців привертають актуальні і болючі для українського суспільства проблеми, зокрема посилення негативного впливу засобів масової інформації, в тому числі Інтернету.

На думку багатьох дослідників комунікацій, найхарактернішою ознакою сучасного етапу розвитку Інтернету є запровадження засобів персоналізації. Момент, коли гіганти IT, такі як Google чи Facebook, почали широко використовувати ці технології, називають початком «ери персоналізації» в Інтернеті. Однак негативний вплив цих явищ на суспільство, політику, права людей здебільшого залишається недооціненим та малодослідженим [2].

Саме тому захист користувача від шкідливих ресурсів, виявлення та фільтрування небажаного («шкідливого») контенту в Інтернеті є надзвичайно актуальним питанням сьогодення.

Аналіз останніх досліджень і публікацій. У звіті спеціальної комісії Internet Safety Technical Task Force зазначається, що поганий вплив, який має Інтернет, перебільшений. Звіт став завершенням річної роботи представників трьох десятків компаній та організацій під керівництвом гарвардського BerkmanCenterfor Internet & Society. Вивчивши питання безпеки користувачів у мережі, члени комісії дійшли висновку, що Інтернет не є у цьому сенсі чимось принципово особливим. Небезпеки, яким користувачі піддаються в Інтернеті, складні і багатогранні, і здебільшого мало відрізняються від небезпек, які загрожують їм у реальному світі.

Водночас за даними агентства стратегічних досліджень Інтернет-залежність – це явище, яке останніми роками набуло справді вражаючого розмаху.

Інтернет-залежність, яка проявляється відхиленням у поведінці, за якого в людини порушується відчуття реальності, втрачається відчуття часу і критичне мислення, обмежується управління своїми вчинками, вона стає менш активною, порушується цикл сну і неспання. Настає психічна та фізична залежність.

Вплив негативних контентів має різноманітний характер. Крім вище вказаних негативних наслідків, які приводять до збиткової ваги, існує й більш небезпечна проблема – самогубство, кримінальні правопорушення тощо.

У роботі [3] запропоновано метод застосування моделей глибокого навчання до задачі аналізу тональності текстових даних, який відрізняється від наявних своєю структурою, що дозволяє підвищити точність виявлення інформаційно-психологічних впливів у контенті соціальних мереж.

У роботі [4] розглянуто підходи до опрацювання контенту у системах фільтрації вебресурсу, надано оцінку методам її реалізації з точки зору безпеки, конфіденційності та інших аспектів, які роблять цей процес більш ефективним. У роботі [5] наведено аналіз показників результативності, яка виникає на різних рівнях – для населення, підприємств і держави загалом. Одержала подальший розвиток наявна система індикаторів оцінки технологічної результативності впровадження комплексної системи фільтрації контенту шляхом додавання показників вартості та рівня адаптивності. Показано векторну спрямованість наявних і пропонованих індикаторів.

По-перше, від якісних і ефективних методів аналізу і фільтрування.

По-друге, від якісного складу самої системи фільтрації, а саме від рівня протоколів передачі даних, портів та інших пристроїв, що задіяні в такому процесі.

Виходячи з вищесказаного, у цій роботі запропонована практична реалізація систем фільтрації контенту.

Мета статті. Метою цієї статті є розробка плагіну для опрацювання текстового контенту на Web-контентах для автоматизації виявлення шкідливих ресурсів та захисту користувачів від вірусної інформації.

Виклад основного матеріалу. Контент-аналіз являє собою систематичну числову обробку, оцінку та інтерпретацію форми і змісту інформаційного джерела. При цьому увага зосереджується на елементах контекстуального вживання, оцінці інформації, аналізі способу презентації інформації, адекватній оцінці значимості інформації. Виділяють кількісний і якісний контент-аналіз. Кількісний контент-аналіз орієнтований на дослідження частоти появи в тексті зазначених вище характеристик змісту. Він легше піддасться реалізації в комп'ютерних програмах. Якісний контент-аналіз передбачає формування думки або певного питання навіть на основі єдиної присутності або відсутності певної характеристики змісту [6].

Обов'язковим елементом системи опрацювання Web-ресурсів є контентно-пошукова підсистема. До складу контентно-пошукової підсистеми системи опрацювання Web-ресурсів входять чотири основні модулі [7]:

1. Модуль реєстрації користувача і введення запиту.
2. Модуль опрацювання контенту.
3. Модуль пошуку контенту.
4. Модуль збереження та подання контенту

Виділяють такі стадії аналізу вебконтенту [3]:

1. Підготовка програми аналізу документів. На цьому етапі, як правило, формується так звана емпірична теорія дослідження. Тобто вхід і підготовки до проведення аналізу систематизуються гіпотези, які існують у контексті цієї проблематики, та відкидаються ті з них, які не піддаються верифікації на даних інформаційного масиву.

2. Відбір джерел аналізу. Необхідно визначити коло джерел, які містять матеріали та інформацію.

3. Визначення емпіричних моделей аналізу, формування вибірки (підбір комунікаційних органів, вибір матеріалів за різні періоди часу, визначення видів повідомлень, типу вибірки).

4. Розроблення методики конкретного аналізу.

5. Пілотажне дослідження, перевірка надійності методики.

6. Збір первинної емпіричної інформації.
7. Кількісне опрацювання зібраних даних.
8. Інтерпретація здобутих результатів, висновки дослідження.

Для вирішення поставленого завдання розробки автоматизованої системи аналізу вебконтентів та медіаресурсів необхідно провести їх класифікацію для віднесення ресурсів до негативних або позитивних. Здебільшого контенти класифікують за допомогою інформаційно-пошукових мов (ІПМ). Частковим випадком ІПМ є рубрикатор.

Наявні також спеціальні процедури підрахунку результату контент-аналізу, наприклад, формула розрахунку коефіцієнта Яніса, призначеного для обчислення співвідношення позитивних і негативних (щодо вибраної позиції) оцінок, думок, аргументів [9]. Коефіцієнт Яніса можна застосовувати, наприклад, для розрахунку співвідношення позитивних і негативних думок, висвітлених у коментарях користувачів щодо продукції, яка реалізується через систему електронної комерції. У разі, якщо кількість позитивних оцінок перевищує кількість негативних, коефіцієнт Яніса вираховується за формулою:

$$c = \frac{f^2 - fn}{rt} \quad (1),$$

де f – кількість позитивних оцінок;
n – кількість негативних оцінок;
r – об'єм змісту тексту, що має пряме відношення до проблеми, яка досліджується;
e – загальний об'єм аналізованого тексту.

У разі, коли кількість позитивних оцінок менша за негативну, коефіцієнт Яніса знаходиться за формулою:

$$c = \frac{fn - n^2}{rt} \quad (2).$$

У роботі [7] зазначається, що метод інформаційного пошуку, заснований на подібності ПРК із ПОК, не може повністю забезпечити пошук усієї множини контенту, що відповідає інформаційному запиту. Це призводить до того, що частина контенту, яка відповідає запиту, тобто релевантних йому, залишається невиданою користувачеві. Водночас у множині виданого контенту є такий, який не відповідає запиту, тобто не є релевантним. Фактично у будь-якій реальній контентно-пошуковій підсистемі є два основні типи помилок:

– помилки 1-го роду (або пропуск мети): невидання користувачеві фактично релевантного його запиту контенту;

– помилки 2-го роду (або помилкова тривога, інакше шум): видавання користувачеві нерелевантного контенту, який не відповідає поставленому запиту.

Наявність помилок 1-го і 2-го роду в реальній системі зумовлює розподіл усього масиву контенту системи щодо запиту на чотири підмасиви (табл. 1).

Таблиця 1

Розподіл масиву контенту

Масиви	Видане	Невидане
Релевантні	A – виданого релевантного контенту	C – невиданого релевантного контенту
Нерелевантні	B – виданого нерелевантного контенту	D – невиданого нерелевантного контенту

Наявні такі показники ефективності контентно-пошукової підсистеми, де a – кількість виданих релевантних документів; b – кількість виданих нерелевантних документів, c – кількість незнайдених релевантних документів; d – кількість незнайдених нерелевантних документів.

Таблиця 2

Показники ефективності контентно-пошукової підсистеми

№	Коефіцієнт	Характеризує частину	Формула
1	Повноти *p*	Виданого релевантного контенту у всьому масиві релевантного контенту	$p = \frac{a}{a + c}$
2	Точності *n*	Виданого релевантного контенту у всьому масиві виданого контенту	$n = \frac{a}{a + b}$
3	Шуму *e*	Виданого нерелевантного контенту у всьому масиві виданого контенту	$e = \frac{b}{a + b} = 1 - n$
4	Осаду *q*	Виданого нерелевантного у всьому масиві нерелевантного контенту	$q = \frac{b}{d + b}$
5	Специфічності *k*	Не знайденого нерелевантного контенту у всьому масиві не релевантного контенту	$k = \frac{d}{d + b}$

Алгоритм виявлення негативного інтернет-контенту. Проаналізувавши вхідні та вихідні дані, було реалізовано алгоритм роботи системи виявлення та фільтрування Web-контенту:

1. У background.js фонової сторінки вебплагіну підписуємося на подію зміни поточної вкладки браузера, а також на подію початку будь-якого вебзапиту з відкритої сторінки.

2. Тоді як користувач відкрив сторінку і з неї почав завантажуватися будь-який контент, спрацьовують події, на які ми підписалися в 1 пункті. З кожного об'єкта, який передається в оброблювачі подій, отримуємо URL запитуваного ресурсу.

3. Базуючись на масиві URL запитуваних ресурсів, формуємо масив, який складається виключно з доменів (він буде меншим, ніж початковий, тому що деякі ресурси можуть запитуватися з одного і того ж вебсайту).

4. Ініціюємо запит до сервера, куди передається масив доменів. На стороні сервера перевіряємо у базі даних те, чи є домени «шкідливими» та встановлюємо прапор blacklisted у true/false. Отриманий результат із серверу кеширується на стороні клієнта на деякий час, щоб у подальшому зменшити кількість запитів до сервера.

5. Аналізуємо результат перевірки доменів з пункту 4 та підраховуємо коефіцієнт Яніса за формулою 1 чи 2, залежно від кількості позитивних оцінок. Якщо коефіцієнт Яніса має велике значення, то показуємо overlay – блок з чорним фоном і попередженням, що на сторінці може бути присутнім шкідливий контент. Overlay додається, використовуючи код, який знаходиться у contentscript.js, тому що він має доступ до DOM-моделі документа.

6. Коли відкривається будь-яка вебсторінка, за допомогою коду зі background.js зберігаємо в БД інформацію про неї. Надалі через сторінку адміністратора можна проаналізувати те, скільки «шкідливого» контенту було виявлено на певній сторінці, і як багато часу користувач переглядав її.

7. За допомогою contentscript.js відображаємо в лівому куті екрана інформацію для адміністратора (якщо той пройшов аутентифікацію), про кількість шкідливого контенту на сторінці, а також кнопку «обмежити доступ», якщо він вважатиме за потрібне зробити це, щоб користувач не мав до нього доступ.

У відповідності до результатів дослідження предметної області, поставленого завдання та описаного алгоритму роботи системи можуть бути виділені категорії концептуальних класів, що наведені в таблиці 3.

Таблиця 3

Категорії концептуальних класів

Категорія	Приклади
Фізичні та матеріальні об'єкти	– користувачі; – звіти.
Ролі людей	– суперадміністратор; – адміністратор; – звичайний користувач.
Події	– створення та адміністрування користувача; – опрацювання даних, що надійшли з вебплагіну; – формування журналів статистики роботи вебплагіну та помилок, що були виявлені під час їх роботи.
Процеси	– авторизація; – робота з користувачами; – робота зі вебконтентами; – робота з журналами.

Користуючись списком категорій та підходом архітектурного патерну MVC, розроблено список класів для предметної області:

1. Користувачі.

Опис розробленого застосунку. Для розробки програмного забезпечення використано такі технології та мови програмування:

AJAX (англ. Asynchronous JavaScript and XML – Асинхронний JavaScript та XML) – це технологія звертання до серверу без перезавантаження сторінки за допомогою JavaScript. Головна особливість полягає в тому, що за рахунок цього зменшується час відгуку вебдодатка.

JavaScript – динамічна, об'єктно-орієнтована прототипна мова програмування. Реалізація стандарту ECMAScript. Найчастіше використовується для створення сценаріїв вебсторінок, що дає можливість на боці клієнта (пристрої кінцевого користувача) взаємодіяти з користувачем, керувати браузером, асинхронно обмінюватися даними із сервером, змінювати структуру та зовнішній вигляд вебсторінки.

JSON (англ. JavaScript Object Notation) – це текстовий формат обміну даними, що не залежить від мови програмування. Це формат легкий як для сприйняття людиною, так і для обробки пристроями.

Apache – це надійний та гнучкий до налаштування HTTP-сервер, що оброблює HTTP-запити. Він використовується для передачі через HTTP протокол статичних та динамічних вебсторінок [8].

MySQL – це система керування реляційними базами даних. Реляційна база даних являє собою структурований за певними правилами набор даних.

Для того щоб запобігти несанкціонованому доступу, вхід у систему здійснюється з перевіркою логіну та пароля користувача. Пароль шифрується за допомогою алгоритму хешування md5, що перетворює масив вхідних даних довільної довжини у бітову строку фіксованої довжини, яка є унікальною. Результат роботи хеш-функції зберігається у базу даних.

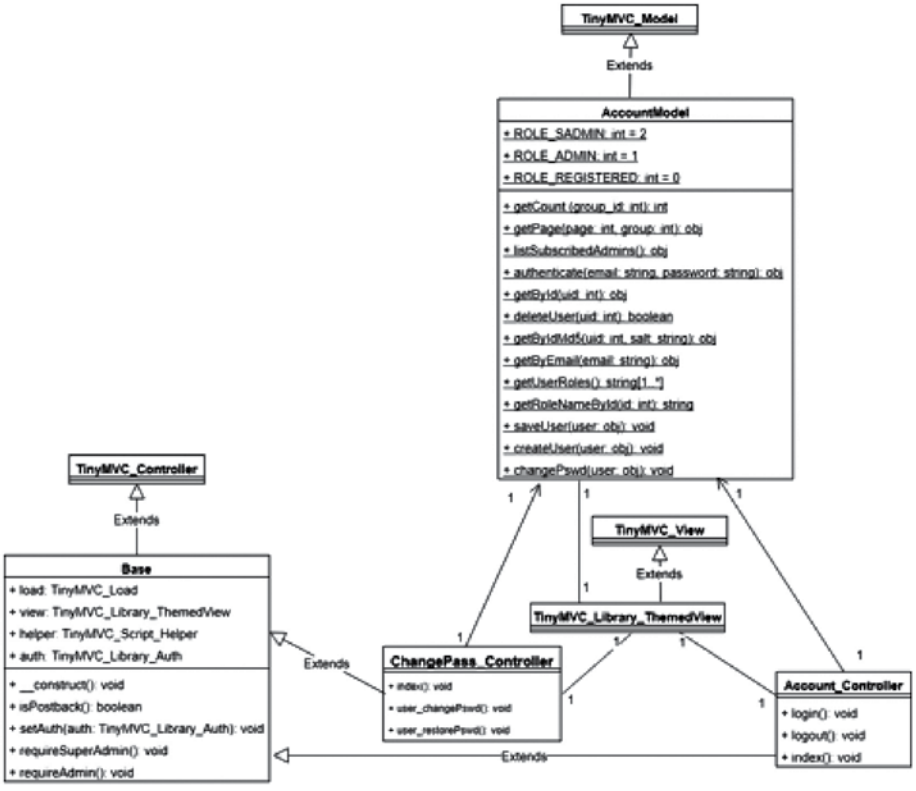

Рис. 1. Діаграма MVC класів для роботи з користувачами

2. Вебконтенти та їх логотипи.

Рис. 2. Діаграма MVC класів для роботи з вебконтентами та їх логотипами

Розглянемо основний функціонал розробленого програмного забезпечення. Користувач може налаштувати роботу плагіну під свої потреби. У налаштуваннях плагіну можливо вибрати сценарій роботи (рис. 3).

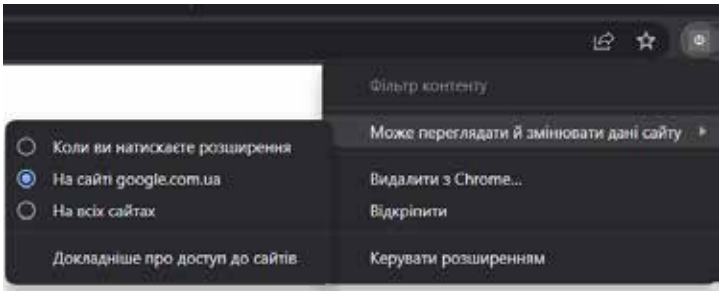

Рис. 3. Сценарії роботи плагіну

Передбачена можливість заблокувати небажаний контент на вебресурсі, на якому знаходимось (рис. 4).

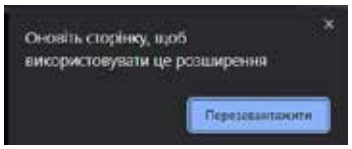

Рис. 4. Запит плагіну на перезавантаження сторінки

Плагін дозволяє додавати конкретний вебресурс до списку, що буде превірятися плагіном. Список ресурсів можна преглянути в налаштуваннях плагіну у браузері (рис. 5).

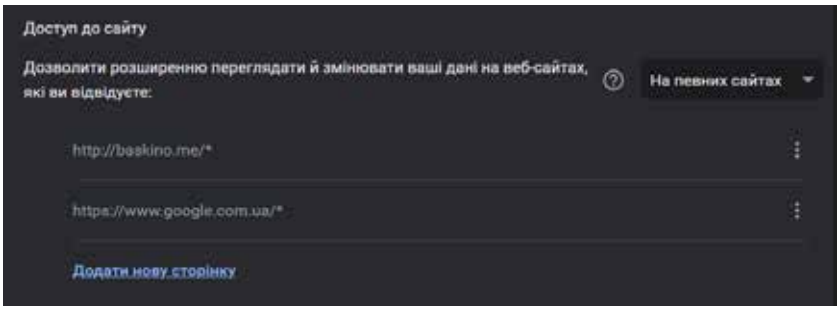

Рис. 5. Список ресурсів, де працює плагін

Сторінка (рис. 4) для звичайного та суперадміністратора має посилання на сторінку адміністрування користувачів «Users», їх груп «Groups», а також каналів даних (вебконтентів) «Channels».

Група, для якої виконується адміністрування, може бути вибрана за допомогою списку, що випадає під час натискання на назву групи. Звичайний користувач не може змінювати групу та бачити інформацію про її інших учасників.

Також суперадміністратор, на відміну від інших ролей, має можливість: генерувати тестові дані у форматі JSON, для імітації роботи вебплагіну – «Data Generator»; переглядати журнал даних вебплагіну у неопрацьованому вигляді – «Raw Log»; адмініструвати логотипи каналів – «All Channel Logos».

Усі типи користувачів мають доступ до формування звітів «Reports» щодо почасового перегляду вебконтентів «Watching Hours» та звіту, що відображає частку перегляду вебконтентів від загального часу «TimeAmount».

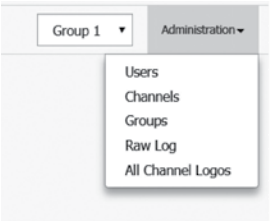

Рис. 6. Головна сторінка для суперадміністратора

За результатами фільтрації плагіну провайдери з небажаним контентом добавляються та зберігаються до файлу blackList.txt (рис. 7).

```
1  testad.com
2  another.domen.ru
3  reclama.org
4  googleads.g.doubleclick.net
5  googlesyndication.com
6  tpc.googlesyndication.com
7  facebook.com
```

Рис. 7. blackList.txt

У разі завантаження web-сторінки плагін перевіряє сторінку на наявність контенту, який завантажується зі вказаних у списку ресурсів. Після знаходження такий контент буде заблокований. На рис. 6 показана робота плагіну, де у разі виключеного плагіну відображається реклама посуду, а після ввімкнення зникає небажана реклама.

а)

б)

Рис. 8. Вигляд реклами: а) до блокування рекламного банера; б) після блокування рекламного банера

Висновки з цього дослідження і перспективи подальших розвідок у такому напрямі. На основі проведеного аналізу предметної області були визначені проблеми сучасних web-контентів. Наявність різнотипної шкідливої інформації вимагає впровадження додаткових засобів для фільтрації контенту користувача. Для вирішення цієї проблеми був розроблений застосунок для аналізу та фільтрації контенту web-сторінок.

Список використаних джерел:

1. Куценко С.І. Діти онлайн: як уберегти від кібербулінгу. *Укрінформ.* URL: https://www.ukrinform.ua/rubric-society/2702033-diti-onlajn-ak-uberegti-vid-kiberbulingu.html.

2. Сухорольський П.М. Персоналізація в Інтернеті та її вплив на забезпечення прав людини / П.М. Сухорольський, Г.П. Хлібойко. *Правова інформатика.* 2013. № 4. С. 3–9.

3. Войтович О. Виявлення негативних впливів у соціальних інтернет-сервісах / О. Войтович, В. Островська, І. Закалов. *Цифрова платформа: інформаційні технології у соціокультурній сфері*. 2018. № 2. С. 93–105.

4. Saravana Balaji B. Adaptability of SOA in IoT Services – An Empirical Survey / Saravana Balaji B., Amin Salih Mohammed, Chiai Al-Atroshi. *International Journal of Computer Applications*. 2018. Vol. 182. P. 25–28.

5. Князєв О.А. Оцінка результативності впровадження комплексних систем фільтрації контенту. *Системи управління, навігації та зв'язку.* ПНТУ ім. Юрія Кондратюка. 2019. № 1. С. 147–152.

6. Квіта Г.М. Контент-аналіз вебсайтів як інструмент фахівця з економічної кібернетики. / Г.М. Квіта, К.О. Шіковець. *Економіка та управління підприємствами*. 2017. № 10. С. 19–23.

7. Чирун Л.Б. Особливості методів контент-аналізу текстових масивів даних web-ресурсів у межах регіону / Л.Б. Чирун, В.В. Кучковський, В.А. Висоцька. *Вісник Національного університету «Львівська політехніка». Серія «Інформаційні системи та мережі»* : збірник наукових праць. 2015. № 829. С. 296–320.

8. Скотт Хокинс. Администрирование веб-сервера Apache и руководство по электронной коммерции. Москва : Вильямс, 2001. 336 с. ISBN 0-13-089873-2.

9. Чирун Л.В. Застосування контент-аналізу текстової інформації в системах електронної комерції / Л.В. Чирун, В.А. Висоцька. *Вісник Національного університету «Львівська політехніка». Серія «Інформаційні системи та мережі»*. 2010. № 689. С. 332–347.

References:

1. Kutsenko, S.I. Dity onlain: yak uberehty vid kiberbulinhu. Ukrinform. Retrieved from: https://www.ukrinform.ua/rubric-society/2702033-diti-onlajn-ak-uberegti-vid-kiberbulingu.html.

2. Sukhorolskyi, P.M. (2013). Personalizatsiia v Interneti ta yii vplyv na zabezpechennia prav liudyny / P.M. Sukhorolskyi, H.P. Khliboiko. Pravova informatyka. № 4. S. 3–9.

3. Voitovych, O. (2018). Vyiavlennia nehatyvnykh vplyviv u sotsialnykh internet-servisakh / O. Voitovych, V. Ostrovska, I. Zakalov. Tsyfrova platforma: informatsiini tekhnolohii v sotsiokulturnii sferi. № 2. Pp. 93–105.

4. Saravana Balaji B. (2018). Adaptability of SOA in IoT Services – An Empirical Survey / Saravana Balaji B., Amin Salih Mohammed, Chiai Al-Atroshi. International Journal of Computer Applications. Vol. 182. P. 25–28.

5. Kniaziev, O.A. (2019). Otsinka rezultatyvnosti vprovadzhennia kompleksnykh system filtratsii kontentu. Systemy upravlinnia, navihatsii ta zviazku. PNTU im. Yuriia Kondratiuka. 2019. № 1. S. 147–152.

6. Kvita, H.M. (2017). Kontent-analiz veb-saitiv yak instrument fakhivtsia z ekonomichnoi kibernetyky. / H.M. Kvita, K.O. Shikovets. Ekonomika ta upravlinnia pidpryiemstvamy. № 10. S. 19–23.

7. Chyrun, L.B. (2015). Osoblyvosti metodiv kontent-analizu tekstovykh masyviv danykh web-resursiv u mezhakh rehionu / L.B. Chyrun, V.V. Kuchkovskyi, V.A. Vysotska. Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: Informatsiini systemy ta merezhi: zbirnyk naukovykh prats. № 829. S. 296–320.

8. Skott Khokyns. (2001). Admynystryrovanye veb-servera Apache y rukovodstvo po elektronnoi kommertsyy. Moskva: Vyliams, 2001. 336 s. ISBN 0-13-089873-2.

9. Chyrun, L.V. (2010). Zastosuvannia kontent-analizu tekstovoi informatsii v systemakh elektronnoi komertsii / L.V. Chyrun, V.A. Vysotska. Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: Informatsiini systemy ta merezhi. № 689. S. 332–347.