

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

**ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ:
НАУКОВО-ПРАКТИЧНИЙ ВИМІР
В УМОВАХ ВОЄННИХ ВИКЛИКІВ**

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 26 квітня 2024 року

Одеса
«Фенікс»
2024

*Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 15.05.2024 р.)*

За загальною редакцією **С. В. Ківалова**

Відповідальний за випуск **М. Р. Аракелян**

Є 24 **Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів** : матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2024. – 1000 с.
ISBN 978-617-8430-05-4

У збірнику відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології в умовах повномасштабного військового вторгнення. Висвітлено питання загроз національній безпеці в їх конституційному вимірі у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики. Відображено наукові напрацювання у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових і науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)»364»»20»(062.552)

Матеріали видано в авторській редакції

<i>Лобода Юлія Геннадіївна</i> ГЕНЕРАЦІЯ НАБОРУ ДАНИХ ДЛЯ МАШИННОГО НАВЧАННЯ.	860
<i>Манаков Сергій Юрійович</i> ВІРТУАЛЬНІ ПОТОКИ JAVA ТА КОРУТИНИ KOTLIN	862
<i>Чанишев Рашид Ібрагімович</i> ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРАВО: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РЕГУЛЮВАННЯ.....	864
<i>Чикунів Павло Олександрович</i> ВІДСТЕЖЕННЯ ПОШИРЕННЯ ПО ПРОГРАМІ НЕПЕРЕВІРЕНИХ ЗОВНІШНІХ ДАНИХ.....	866
<i>Щербина Юрій Володимирович</i> <i>Казакова Надія Феліксівна</i> ДОСЛІДЖЕННЯ ПОТОЧНОГО ШИФРУ, ПОБУДОВАНОГО НА ОСНОВІ XORSHIFT-ГЕНЕРАТОРА	870
<i>Грезіна Олена Миколаївна</i> ЦИФРОВА МАЙСТЕРНІСТЬ ТА ІННОВАЦІЇ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ – БЕЗПЕКОВІ ВИКЛИКИ ДЛЯ СФЕРИ ОСВІТИ	872
<i>Соловйов Артем Сергійович</i> ПРОБЛЕМАТИКА ФАЛЬСИФІКАЦІЇ СИСТЕМНИХ ЖУРНАЛІВ У ОПЕРАЦІЙНІЙ СИСТЕМІ LINUX	874
<i>Дика Анастасія Іванівна, Трофименко Олена Григорівна</i> АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ЗАСОБАМИ SNATGPT ДЛЯ ТЕСТУВАННЯ БЕЗПЕКИ ВЕБЗАСТОСУНКІВ.....	876
<i>Проданюк Назар Богданович</i> ДЕЯКІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ЮРИДИЧНИХ ПОСЛУГ У ЦИФРОВУ ЕПОХУ	878
<i>Світлічний Ігор Валерійович</i> <i>Світлічна Дар'я Ігорівна</i> ЧИ МАЮТЬ МИМОБІЖНІ ПРЯМІ ПРАВО НА ПЕРЕТИН? ДЕЯКІ АСПЕКТИ ЗНАХОДЖЕННЯ ВІДСТАНІ МІЖ МИМОБІЖНИМИ ПРЯМИМИ	880

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

<i>Горбаченко Станіслав Анатолійович, Дикий Олег Вікторович</i> ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕСІ МАРКЕТИНГОВОГО ЦІНОУТВОРЕННЯ	883
<i>Казакова Надія Феліксівна, Кулешова Євгенія Романівна</i> ВИБІР ТИПУ ХМАРНИХ ПОСЛУГ ТА РИЗИК ВИТОКУ ЧУТЛИВОЇ ІНФОРМАЦІЇ.....	885
<i>Ахметмет'єва Ганна Валеріївна</i> ПРОБЛЕМИ РОЗПОВСЮДЖЕННЯ ФЕЙКОВИХ МУЛЬТИМЕДІА В МЕРЕЖІ INTERNET	887
<i>Бойко Віктор Дмитрович</i> БІБЛІОТЕКА NUMPY – ОСНОВА ІНСТРУМЕНТАЛЬНОГО СТЕКУ НАУКОВИХ РОЗРАХУНКІВ SCIPY.....	888
<i>Кухаренко Сергій Вікторович</i> ПОЛІТИКИ ТА ПРОЦЕДУРИ РЕАГУВАННЯ НА ПОРУШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ.....	891
<i>Чепурна Олена Євгенівна</i> КІБЕРЗАГРОЗИ ДЛЯ БІЗНЕС-СЕРЕДОВИЩА ТА СУЧАСНІ ЗАХОДИ ПРОТИДІЇ	893
<i>Черевко Євген Володимирович</i> ШТУЧНИЙ ІНТЕЛЕКТ ТА ЙОГО ЗАСТОСУВАННЯ У ФУНДАМЕНТАЛЬНИХ ДОСЛІДЖЕННЯХ.....	895
<i>Овчинников Микола Юрійович</i> ОСОБЛИВОСТІ ВБУДОВУВАННЯ ПРИХОВАНОЇ ІНФОРМАЦІЇ У ФАЙЛИ ФОРМАТУ MP3	898
<i>Разінкін Нікіта Сергійович</i> КІБЕРЗАХИСТ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙНИ.....	902
<i>Саврацький Олександр Олександрович</i> ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ	905

СЕКЦІЯ 25. ПИТАННЯ МЕТОДИКИ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ, ТЕОРІЇ ТА ПРАКТИКИ ПЕРЕКЛАДУ ЯК ЗАСОБУ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ

<i>Томчаковська Юлія Олегівна</i> СТРАТЕГІЇ І ТАКТИКИ МЕДІЙНОГО ДИСКУРСУ	908
<i>Строченко Леся Василівна</i> ПЕРЕКЛАД У ВІЙСЬКОВІЙ ГАЛУЗІ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ	910
<i>Варешкіна Наталія Володимирівна</i> ДО ПРОБЛЕМИ ВИКЛАДАННЯ АНГЛІЙСЬКОЇ МОВИ ЗА ПРОФЕСІЙНИМ СПРЯМУВАННЯМ	911
<i>Дихта Наталя Миколаївна, Явдошук Анастасія Андріївна</i> НАВЧАННЯ ФОНЕТИЦІ АНГЛІЙСЬКОЇ МОВИ.....	913

Сучасний стан розвитку автоматизованих розподілених інформаційних систем вимагає пошуку нових інженерно технічних рішень в галузі криптографічного захисту інформації. Зазвичай, поточні шифри, що використовуються для шифрування даних в реальному часі, уявляють собою комбінацію декількох компонентів: програмних генераторів ПВЧ, засобів пост оброблення вихідного числового потоку та синхронізації. Основною ціллю досліджень в цьому напрямку є пошук ефективних, з точки зору криптографічної стійкості і простоти формування псевдовипадкових чисел, процедур програмної реалізації генераторів ПВЧ. Як показують результати виконаних досліджень, одним із можливих рішень цієї проблеми є використання запропонованого Джорджем Марсальєю економічного лінійного генератора Xorshift.

Список використаних джерел

1. Schneier B. Applied Cryptography : Protocols, Algorithms, and Source Code in C. 2nd ed. 1995. 662 p.
2. Ferguson N., Schneier B. Practical cryptography. 2003. 539 p.
3. Panneton F., L'Ecuier P. On the Xorshift Random Number Generators. *ACM Transactions on Modeling and Computer Simulation*. 2005. Vol. 15, Iss. 4. P. 346–361. DOI:10.1145/1113316.1113319. URL: <https://web.archive.org/web/20210126143346/http://www.iro.umontreal.ca/~lecuyer/myftp/papers/xorshift.pdf>
4. Rueppel R. A. Good stream ciphers are hard to design. *International Carnahan Conference on Security Technology: Proceedings, Zurich, Switzerland, 3–5 Oct. 1989*. DOI:10.1109/CCST.1989.751974. URL: https://www.researchgate.net/publication/3790837_Good_stream_ciphers_are_hard_to_design
5. Knuth D. E. The Art of Computer Programming. Vol. 2. Seminumerical Algorithms. 3rd ed. Boston, Mass, USA : Addison-Wesley, Longman Publishing, 1997. 762 p.

Ключові слова: Поточные шифры, Блочные шифры, Критерий Пирсона, фоновый трафик, Равномерное распределение вероятностей.

Keywords: Stream ciphers, Block ciphers, Pearson criterion, background traffic, Uniform probability distribution.

Грезіна Олена Миколаївна

Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій, доктор філософії у галузі права

ЦИФРОВА МАЙСТЕРНІСТЬ ТА ІННОВАЦІЇ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ – БЕЗПЕКОВІ ВИКЛИКИ ДЛЯ СФЕРИ ОСВІТИ

У сучасну цифрову епоху інформаційні технології є невід’ємною складовою сфери освіти, відкриваючи безліч можливостей для покращення освітнього процесу та підвищення якості освіти. Цифрова майстерність, що означає вміння ефективно використовувати інформаційні технології, стає ключовим компетентним елементом сучасної освіти. Проте разом з цими перевагами постають і значні безпекові виклики, які можуть стати перешкодою для успішної інтеграції технологій в освітній процес України.

Актуальність даної теми полягає в тому, що сучасна освіта стикається з різноманітними безпековими загрозами в контексті використання інформаційних технологій. Зростання кількості кібератак, витоків конфіденційної інформації, а також інші форми кіберзлочинності ставлять під загрозу якість освіти та приватність учасників освітнього процесу. Освіта є важливим фактором розвитку суспільства, розуміння і вирішення безпекових проблем, пов’язаних з інформаційними технологіями в освіті має бути невідкладним завданням для освітян, дослідників та практиків.

У Концепції розвитку цифрових компетентностей вказано що: «...із збільшенням темпів розвитку цифрових технологій, впровадженням інноваційних рішень у всіх сферах суспільного життя виникає необхідність у підвищенні якості підготовки працівників для створення можливості модернізації економіки країни відповідно до сучасних вимог» [1].

У науковій статті Безлепкіна В. Є. зазначається що: «...процес цифровізації освіти поступово виходить за межі ролі допоміжного чи альтернативного сегмента освітньої сфери і стає важливим фундаментальним елементом цієї суспільної галузі. Внаслідок соціокультурних змін у останні роки цифровий потенціал використовується не просто як інноваційний формат, але як єдиний можливий спосіб організації освітнього процесу на всіх рівнях» [2].

Зазначена думка підкреслює, що цифрові технології є не просто інноваційним форматом, а вважаються єдиним можливим способом організації освітнього процесу на всіх рівнях.

Постає питання необхідності розвитку цифрової майстерності серед всіх учасників освітнього процесу. Оскільки цифрові технології є основою для організації освітнього процесу на всіх рівнях, навички у сфері цифрової грамотності стають критичними для успішного функціонування в сучасному світі.

Крім того, зростання значення цифрової майстерності у сучасному світі ставить під сумнів важливість захисту приватності та безпеки даних. Інноваційні методи навчання, які базуються на використанні інформаційних технологій, несуть у собі ризик незаконного доступу до особистих даних учасників освітнього процесу. Таким чином, дослідження безпекових аспектів цифрової майстерності в контексті освіти має важливе значення для забезпечення захисту прав та інтересів учасників освітнього процесу.

Проте разом з перевагами цифрової майстерності та інновації інформаційних технологій постають і значні безпекові виклики, які можуть стати перешкодою для успішної інтеграції технологій в освітній процес України.

Серед таких викликів можна визначити кіберзагрози та кібератаки, які, з оновленням технологій отримують нові можливості для атак на освітні мережі та системи. Багато закладів освіти можуть стати вразливими перед потенційними кіберпроникненнями через недостатню кіберзахищеність. Збільшення обсягів освітньої інформації в електронному форматі створює проблеми з приватністю та захистом персональних даних учасників освітнього процесу. Недостатня кібербезпекова грамотність серед учасників освітнього процесу може ускладнювати ефективний захист освітніх систем. Крім того, використання цифрових технологій в освітніх цілях може породжувати соціальні та етичні питання, зокрема пов'язані з контролем за даними та моніторингом здобувачів освіти. Зміни в законодавстві також мають бути покликані вимагати від закладів освіти додаткових заходів у забезпеченні відповідності стандартам кібербезпеки та захисту даних.

Відповідно до цього пропонується наступний перелік перспективних напрямів вирішення безпекових викликів для сфери освіти, серед них:

- розробка та впровадження системи кібербезпеки для захисту від атак на освітні мережі та інформаційні ресурси, що включає підготовку розробки і впровадження комплексної системи захисту, яка включатиме стратегії, техніки та методи, щоб забезпечити стійкість закладів освіти до кібератак;
- аналіз впливу культури кібербезпеки на поведінку користувачів у закладах освіти – це напрямок, який зосереджений на вивченні ролі освітніх програм та свідомості користувачів у формуванні безпечних практик в інтернеті;
- розробка та впровадження комплексної системи моніторингу та реагування на кіберзагрози в закладах освіти, що передбачатиме інтеграцію технологічних та організаційних заходів безпеки для ефективного виявлення та запобігання кіберзагрозам;
- розробка та валідація методів інформаційної грамотності та кібербезпеки для підвищення ступеня захищеності учасників освітнього процесу. За цим напрямом передба-

чається навчання учасників освітнього процесу навичкам безпечного користування цифровими технологіями;

- аналіз законодавчої бази щодо захисту освітніх даних в умовах цифрової трансформації. Визначення недоліків та шляхів вдосконалення правового середовища для захисту освітніх даних;
- дослідження впливу соціальних мереж та онлайн-платформ на приватність та безпеку закладів освіти. Ідентифікація потенційних ризиків та шляхи їх запобігання в контексті використання соціальних мереж та онлайн-платформ у навчальних закладах.

Відповідно до цього, слід зробити висновок, що у сучасну цифрову епоху інформаційні технології є невід'ємною складовою сфери освіти, відкриваючи широкі можливості для покращення освітнього процесу. Зростання цифрової майстерності є важливим елементом сучасної освіти. Проте із цими перевагами постають значні безпекові виклики, що загрожують якості освіти та приватності учасників освітнього процесу. Розуміння та вирішення цих проблем вимагає комплексних заходів з підвищення кібербезпеки та розвитку цифрової грамотності серед учасників освітнього процесу.

Список використаних джерел

1. Концепція розвитку цифрових компетентностей : схвалено розпорядженням КМУ від 03.03.2021 р. № 167-р. URL: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text> .
2. Безлепкін Г. Є. Економічні засади імплементації цифрових інноваційних технологій в сфері освіти. *Економіка та суспільство*. 2023. № 57. URL: <https://doi.org/10.32782/2524-0072/2023-57-83>.

Ключові слова: інформаційні технології, освіта, цифрова майстерність, безпекові виклики, кіберзлочинність, цифрові компетентності, кібербезпека, кібератаки, захист даних. Начало формы

Keywords: information technology, education, digital mastery, security challenges, cybercrime, digital competences, cyber security, cyber attacks, data protection.

Соловйов Артем Сергійович

*Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій*

ПРОБЛЕМАТИКА ФАЛЬСИФІКАЦІЇ СИСТЕМНИХ ЖУРНАЛІВ У ОПЕРАЦІЙНІЙ СИСТЕМІ LINUX

Системні журнали в операційній системі Linux відіграють важливу роль у забезпеченні безпеки та налагодженні системи. Лог-файли містять записи про події, що відбуваються в системі, такі як [1]:

- входи та виходи користувачів;
- запуски програм;
- зміни конфігурації;
- системні помилки;
- записи сторонніх програм.

Фальсифікація таких журналів може мати серйозні наслідки для безпеки та цілісності системи. Існує декілька методів фальсифікувати журнали:

- Пряме редагування: Зловмисник може мати отримати доступ до журналів та внести зміни до них.
- Використання спеціальних програм: Існує програмне забезпечення яке дозволяє фальсифікувати журнали