ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

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

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

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

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

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

ISBN 978-617-8430-61-0

СЕКЦІЯ 24. КОГНІТИВНО-ПРАГМАТИЧНІ ДОСЛІДЖЕННЯ ДИСКУРСУ, ТЕОРІЯ ТА ПРАКТИКА ПЕРЕКЛАДУ В АСПЕКТІ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ

Кухаренко Сергій Вікторович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук, доцент

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ МЕДІА В УКРАЇНІ

Актуальні проблеми захисту інформації у сфері медіа в Україні сьогодні значно посилюються через контекст війни, обмеженість ресурсів і структурні труднощі в запровадженні нових технологій. Система захисту інформації у сфері медіа в Україні – це комплекс правових, технічних, організаційних і програмних заходів, спрямованих на забезпечення інформаційної безпеки, збереження конфіденційності, достовірності та доступності інформації, що поширюється через засоби масової інформації. Організація системи захисту інформації в медіа є ключовим аспектом забезпечення безпеки в сучасному інформаційному просторі, де кіберзагрози та витоки конфіденційної інформації можуть мати серйозні наслідки для суспільства і для свободи слова. Із зростанням цифрових комунікацій у медіа зростає і потреба в надійних заходах захисту даних, що охоплюють як технічні, так і організаційні стратегії. Матеріал доповіді присвячений розгляду основних складових системи захисту інформації, яка використовуються для запобігання несанкціонованому доступу до конфіденційної інформації, захисту персональних даних користувачів та підтримки безпеки журналістських джерел.

На даний час, можливо виділити декілька аспектів захисту інформації в медіа, серед яких технічні можливості, організаційні заходи і так званий моральний аспект в роботі з журналістськими джерелами. Розглянемо деякі складові, які відносяться до системи захисту:

1. *Технічна інфраструктура*. Практична організація захисту даних в медіа починається з впровадження надійної технічної інфраструктури для захисту інформаційних систем і даних користувачів. Основні складові цієї інфраструктури включають:

- Шифрування даних. Використання шифрування для захисту даних під час зберігання та передачі, є обов'язковою практикою. Медіа платформи, особливо ті, що працюють з OTT-сервісами (Over-the-Top), застосовують протоколи шифрування (наприклад, TLS або SSL) для захисту від несанкціонованого доступу до конфіденційної інформації, як-то персональні дані користувачів чи інформація, що передається під час журналістських розслідувань.
- Мережеві брандмауери та системи виявлення вторгнень. Для захисту від несанкціонованого доступу до внутрішніх серверів і баз даних медіа компанії використовують системи брандмауерів та системи виявлення вторгнень (IDS/IPS). Ці технології дозволяють виявляти і зупиняти потенційні кібератаки, зокрема, DDoS-атаки, які можуть бути спрямовані на медіа ресурси.
- Системи резервного копіювання та відновлення даних. Критично важливим для безперебійної роботи медіа компаній є використання систем

резервного копіювання, що дозволяють швидко відновити роботу після технічних збоїв чи атак. Зокрема, для OTT-платформ, де користувачі очікують постійного доступу до контенту, резервні копії баз даних і контенту є обов'язковим елементом захисту.

2. *Організаційні заходи.* Медіа компанії повинні забезпечити організаційну підтримку захисту інформації через впровадження відповідних політик і процедур, а саме:

- Регулярні аудити кібербезпеки. Медіа компанії проводять регулярні аудити своїх систем для перевірки на відповідність чинним вимогам та стандартам з кібербезпеки. Це допомагає ідентифікувати потенційні вразливості в системах, що могли б бути використані для несанкціонованого доступу до інформації.
- Навчання співробітників. Однією з головних загроз є людський фактор. Тому медіа компанії необхідно проводити регулярні тренінги для журналістів та технічних фахівців щодо захисту персональних даних та роботи з конфіденційною інформацією. Це особливо актуально для журналістів, які працюють з джерелами, де можливий виток інформації.
- Політики доступу до інформації. Впровадження чітких політик контролю доступу до інформації є важливою складовою захисту даних. Наприклад, журналісти повинні мати обмежений доступ лише до тієї інформації, яка необхідна для їхньої роботи, а чутливі дані мають бути захищені двофакторною автентифікацією.

3. *Захист журналістських джерел*. Журналістам важливо зберігати конфіденційність своїх джерел, особливо під час розслідувань. Для цього повинні використовуватися як правові механізми, так і технічні засоби, такі як шифрування комунікацій між журналістами та їхніми джерелами. Платформи для безпечної передачі інформації, наприклад, Signal або ProtonMail, що допомагають захистити ці дані.

Досліджуючи міжнародний досвід, можна взяти для порівняння захист даних в медіа сфері в США, де це регулюється кількома ключовими актами, такими як CLOUD Act (безпека у хмарі) та Stored Communications Act (закон про збережені комунікації). Американські медіа компанії широко застосовують комплексні системи кібербезпеки, зокрема автоматизовані системи аналізу загроз (SIEM) та штучний інтелект для виявлення підозрілої активності в реальному часі. Також важливу роль відіграють постійні інвестиції в розвиток і тестування резервних копій даних і впровадження систем багатофакторної автентифікації.

Отже, система захисту інформації у сфері медіа в Україні відіграє ключову роль у забезпеченні національної безпеки, демократичного розвитку суспільства та захисту прав громадян на достовірну інформацію. Особливо у контексті війни між Україною та Росією, кіберзагроз і масових інформаційних атак з боку ворога, медіа-простір стає не лише інструментом інформування, а й полем боротьби, оскільки медіаресурси відіграють важливу роль у формуванні громадської

думки. Напади на дані медіаорганізацій можуть включати витік конфіденційної інформації, персональних даних користувачів і журналістських джерел.

Важливість ефективної системи захисту полягає в протидії дезінформації та ворожій пропаганді, які можуть маніпулювати свідомістю населення; забезпеченні достовірності та об'єктивності інформації, що формується у ЗМІ; захисті персональних даних та конфіденційної інформації; підвищенні довіри громадськості до національних медіа та гарантуванні свободи слова, але в межах, що не шкодять інтересам держави та суспільства.

Список використаних джерел:

1. Закон України «Про інформацію». Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12

2. Закон України «Про медіа». Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2849-20

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

5. Кіберзахист медіа в Україні: стан і виклики. *Інститут масової інформації.* URL: https://imi.org.ua

6. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu

Ключові слова: кібербезпека, безпека даних, захист інформації, система захисту інформації, інформація.

Keywords: cybersecurity, data security, information protection, information protection system, information.

Чепурна Олена Євгенівна

Національний університет «Одеська юридична академія»,

доцент кафедри кібербезпеки, кандидат фізико-математичних наук, доцент

АНАЛІЗ ТЕОРЕТИКО-ІГРОВИХ МЕТОДІВ СУЧАСНОЇ КІБЕРБЕЗПЕКИ

В умовах глобалізації та стрімкого розвитку інформаційних технологій кібербезпека стає критично важливою складовою національної безпеки кожної держави. В особливості це стосується України в контексті військових дій, що тривають на її території, та прагнення до європейської інтеграції. Сучасні методи забезпечення кібербезпеки часто ґрунтуються на застосуванні теоретико-ігрових методів, які дозволяють аналізувати кіберінциденти та моделювати і