

ISSN
2786-863X

СТУДЕНТСЬКИЙ НАУКОВИЙ ЖУРНАЛ

UNI VER SUM

№ 14 / 2024
ЛИСТОПАД

ISSN 2786-863X

UNI VER SUM

№ 14 / листопад 2024

DOI 10.36074/universum.14.2024

Вінниця, Україна
«UKRLOGOS Group»
2024

**УДК 082:001
U 55**

**Ідентифікатор медіа R30-02718
на підставі рішення Національної Ради
№ 424 від 22.02.2024**

Редакція журналу: ГО «Молодіжна наукова ліга»

Верстка: Зрада С.І.

Дизайн: Бондаренко І.В.

Головний редактор: Коренюк І.О.

Журнал видається за підтримки Інституту науково-технічної інтеграції та співпраці.

Редакційна колегія:

Афанасьєва Наталя Євгенівна – доктор психологічних наук, професор
Харківський національний економічний університет ім. С. Кузнеця

Бацуровська Ілона Вікторівна – доктор педагогічних наук, доцент
Миколаївський національний аграрний університет

Ємельянов Олександр Юрійович – доктор економічних наук, професор
Національний університет «Львівська політехніка»

Костюченко Валентина Миколаївна – доктор економічних наук, професор
Державний торговельно-економічний університет

Онікієнко Сергій Володимирович – доктор економічних наук, професор
Київський національний економічний університет імені Вадима Гетьмана

Ащепкова Наталія Сергіївна – кандидат технічних наук, доцент
Дніпровський національний університет ім. Олеся Гончара

Ковальова Світлана Сергіївна – кандидат юридичних наук, доцент
Національний університет біоресурсів і природокористування України

Кулик Алла Василівна – кандидат економічних наук, доцент
Державний торговельно-економічний університет

Мартинюк Віталій Олексійович – кандидат географічних наук, доцент
Рівненський державний гуманітарний університет

Мудра Світлана В'ячеславівна – кандидат педагогічних наук, доцент
Київський інститут Національної гвардії України

Павшук Катерина Олександрівна – кандидат юридичних наук, доцент
Національний юридичний університет імені Ярослава Мудрого

Ротова Наталія Володимирівна – кандидат філологічних наук, доцент
Українська інженерно-педагогічна академія

Христин Ніна Сергіївна – кандидат педагогічних наук, доцент
Університет Григорія Сковороди в Переяславі

Шевченко Оксана Борисівна – кандидат ветеринарних наук, доцент
Державний біотехнологічний університет

Єгоренков Анатолій Іванович – Радник Президента НАМН України з питань біоетики, доцент
Національний медичний університет ім. О.О. Богомольця

Фішер Володимир Михайлович – заслужений діяч мистецтв України, доцент
Київський національний університет культури і мистецтв

Оленюк Дмитро Олександрович – старший викладач
Поліський національний університет

Дурова Наталія Вікторівна – асистент
Поліський національний університет

Мокрякова Марина Іванівна – асистент
Харківський національний медичний університет

**Журнал «UNIVERSUM» індексує вміст в міжнародній
наукометричній базі наукових публікації Google Scholar.**

**Матеріали випуску є загальнодоступними на умовах міжнародної ліцензії
Creative Commons Attribution-ShareAlike 4.0 (CC BY-SA 4.0).**

© Автори статей, 2024
© ГО «Молодіжна наукова ліга», 2024
© ТОВ «УКРЛОГОС Груп», 2024

ЗМІСТ**РОЗДІЛ 1.
ЕКОНОМІЧНА ТЕОРІЯ, МАКРО- ТА
РЕГІОНАЛЬНА ЕКОНОМІКА**

РОЛЬ ЗЕЛЕНОЇ ЕКОНОМІКИ У СТРАТЕГІЯХ СТАЛОГО РОЗВИТКУ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКИЙ КОНТЕКСТ Шавикін С.О., Середа А.В., Науковий керівник: Шпак О.В.	10
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ АСОРТИМЕНТНОЇ ПОЛІТИКИ ПІДПРИЄМСТВА В УМОВАХ ТУРБУЛЕНТНОСТІ Іщенко О.М., Науковий керівник: Гуляницький В.В.	19

**РОЗДІЛ 2.
ПІДПРИЄМНИЦТВО, ТОРГІВЛЯ ТА
СФЕРА ОБСЛУГОВУВАННЯ**

СУТНІСТЬ ТА ПРИНЦИПИ ПРОЦЕСУ ОРГАНІЗАЦІЙНОЇ ПІДТРИМКИ МІЖНАРОДНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА Ткаченко І., Науковий керівник: Гончаренко О.В.	28
--	----

**РОЗДІЛ 3.
ФІНАНСИ ТА БАНКІВСЬКА СПРАВА;
ОПОДАТКУВАННЯ, ОБЛІК І АУДИТ**

ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ПОДАТКОВОГО ЗАКОНОДАВСТВА УКРАЇНИ Гринік А.В., Науковий керівник: Фокша Л.В.	34
КОНВЕРГЕНЦІЯ ОБЛІКУ ВИТРАТ ТРАНСНАЦІОНАЛЬНИХ КОРПОРАЦІЙ У КОНТЕКСТІ СТАЛОГО РОЗВИТКУ Черевань А.А., Науковий керівник: Костюченко В.М.	40
СПЕЦИФІЧНІ ПІДХОДИ ДО РЕАЛІЗАЦІЇ СТРАХОВИХ ПОСЛУГ В СУЧАСНИХ УМОВАХ РОЗВИТКУ УКРАЇНИ Бондаренко Я.А., Науковий керівник: Загорська Д.М.	51

**РОЗДІЛ 4.
МАРКЕТИНГОВА ТА ЛОГІСТИЧНА ДІЯЛЬНІСТЬ**

АНАЛІЗ НА ОСНОВІ ІНТУЇЦІЇ: ЧИ МОЖЕ ШТУЧНИЙ ІНТЕЛЕКТ ПЕРЕДБАЧАТИ ПОТРЕБИ КЛІЄНТІВ? Папуша А.А., Статіва О.Б., Науковий керівник: Мангушев Д.В.	57
ВИКОРИСТАННЯ ПСИХОЛОГІЧНИХ АСПЕКТІВ У СТВОРЕННІ ЕФЕКТИВНОГО РЕКЛАМНОГО КОНТЕНТУ Гладких А.В., Науковий керівник: Третяк В.П.	68

РОЗДІЛ 5.

МЕНЕДЖМЕНТ, ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

УПРАВЛІННЯ ОРГАНІЗАЦІЙНОЮ КУЛЬТУРОЮ ПІДПРИЄМСТВА В НАПРЯМІ ПІДВИЩЕННЯ МОТИВАЦІЇ ПЕРСОНАЛУ Русавська І.В., Науковий керівник: Ключковський О.В.	74
ФОРМУВАННЯ УСПІШНОЇ БІЗНЕС-МОДЕЛІ ПІДПРИЄМСТВА Клягін Ю.В., Науковий керівник: Березянка Т.В.	80

РОЗДІЛ 6.

СОЦІАЛЬНА РОБОТА ТА СОЦІАЛЬНЕ ЗАБЕЗПЕЧЕННЯ

ПЕРСПЕКТИВИ ТА ШЛЯХИ ВПРОВАДЖЕННЯ ЄВРОПЕЙСЬКИХ ПІДХОДІВ ДО СОЦІАЛЬНОЇ ПОЛІТИКИ В УКРАЇНІ Батура Є.А., Науковий керівник: Татарінова С.О.	89
--	----

РОЗДІЛ 7.

ПРАВО ТА МІЖНАРОДНЕ ПРАВО

ДЕЛІКТНІ ЗОБОВ'ЯЗАННЯ У МІЖНАРОДНОМУ ПРИВАТНОМУ ПРАВІ Бондарчук С.С.	94
Стаття вилучена з відкритого доступу за запитом автора.....	104
ДО ПИТАННЯ ПРО ПОВОРІТ ВИКОНАННЯ СУДОВИХ РІШЕНЬ У ЦИВІЛЬНОМУ СУДОЧИНСТВІ Сіренко С.М., Науковий керівник: Котвяковський Ю.О.	111
ЕТИКА У ВІДНОСИНАХ ПРОКУРОРА ІЗ СУДОМ ТА З ІНШИМИ УЧАСНИКАМИ СУДОЧИНСТВА Кислиця А.В., Науковий керівник: Лапкін А.В.	119
МОЖЛИВІСТЬ ЗАСТОСУВАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ЦИВІЛЬНОМУ СУДОЧИНСТВІ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ Малоок А.І., Науковий керівник: Шаповалова К.Г.	127
НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ФІНАНСУВАННЯ ВІДНОВЛЕННЯ УКРАЇНИ Вербицька А.І., Науковий керівник: Фокша Л.В.	134
ОРГАНІЗАЦІЯ ТРУДОВИХ ВІДНОСИН В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ Тимченко Н.В., Науковий керівник: Гресь Н.М.	139
ПІДСТАВИ ПРИПИНЕННЯ ТРУДОВОГО ДОГОВОРУ ПРИ ВІДМОВІ ПРАЦІВНИКА ВІД ПЕРЕВЕДЕННЯ, ПЕРЕМІЩЕННЯ ТА ЗМІНУ ІСТОТНИХ УМОВ ПРАЦІ Поліщук Є.Д., Науковий керівник: Золотухіна Л.О.	146

ЗМІСТ

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАЙНЯТОСТІ ТА ПРАЦЕВЛАШТУВАННЯ Чуракова Д.О., Науковий керівник: Золотухіна Л.О.	152
ПРАВОВЕ РЕГУЛЮВАННЯ ЗОВНІШНЬОЇ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ В УКРАЇНІ Шаргородська М.Ю.	159
РОЛЬ РИМСЬКОГО СТАТУТУ НА МІЖНАРОДНІЙ АРЕНІ ТА РАТИФІКАЦІЯ РИМСЬКОГО СТАТУТУ УКРАЇНОЮ Сухоставець В.Р.	167
РОЛЬ УКРАЇНИ В МІЖНАРОДНОМУ ВАЛЮТНОМУ ФОНДІ (МВФ): ЕКОНОМІЧНІ РЕФОРМИ ТА ПРАВОВІ АСПЕКТИ ФІНАНСОВИХ УГОД Черська Д.М.	173
ТРИРІВНЕВА ТИПОЛОГІЯ ЗОБОВ'ЯЗАНЬ ДЕРЖАВИ: ПОВАЖАТИ, ЗАХИЩАТИ ТА ЗАБЕЗПЕЧУВАТИ ЗДІЙСНЕННЯ ПРАВ ЛЮДИНИ Кислиця А.В., Науковий керівник: Ковтун В.І.	184
УЧАСТЬ УКРАЇНИ У ПРОГРАМАХ З МІЖНАРОДНОГО КОСМІЧНОГО ПРАВА Бондарчук С.С.	190
ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ БЮДЖЕТНОГО ЗАКОНОДАВСТВА Старина А.С., Науковий керівник: Фокша Л.В.	201

РОЗДІЛ 8.

ІНСТИТУТ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ, СУДОВА СИСТЕМА ТА НОТАРІАТ

ДОКАЗИ ТА ДОКАЗУВАННЯ В ЦИВІЛЬНОМУ ПРОЦЕСІ В УМОВАХ ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ Кичата Л.О., Науковий керівник: Шаповалова К.Г.	207
ОКРЕМІ ПИТАННЯ ПРОЯВУ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ В УМОВАХ ВОЄННОГО СТАНУ Бондаренко А.В., Науковий керівник: Копилов Е.В.	212
ОСОБЛИВОСТІ ПРАВОВОГО СТАТУСУ ІНШИХ УЧАСНИКІВ СУДОВОГО ПРОЦЕСУ В ЦИВІЛЬНОМУ СУДОЧИНСТВІ Тернавська В.В., Науковий керівник: Шаповалова К.Г.	218
ОСОБЛИВОСТІ ТА ТАКТИКА ВИКОРИСТАННЯ БПЛА ПРАЦІВНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ПІД ЧАС ВИКОНАННЯ СЛУЖБОВО- БОЙОВИХ ЗАВДАНЬ Сорокіна Д., Поповська В., Науковий керівник: Король К.	224
РОЗВИТОК ФІЗИЧНИХ ЯКОСТЕЙ ПОЛІЦЕЙСЬКИХ МЕТОДАМИ СПЕЦІАЛЬНОЇ ФІЗИЧНОЇ ПІДГОТОВКИ Комарницький О.А., Журавльов О.О., Науковий керівник: Пожидаєв М.Ю.	232
РОЛЬ СПЕЦІАЛЬНОЇ ФІЗИЧНОЇ ПІДГОТОВКИ У ПІДВИЩЕННІ ПРОФЕСІЙНОЇ ГОТОВНОСТІ ПОЛІЦЕЙСЬКИХ ДО ЕКСТРЕМАЛЬНИХ СИТУАЦІЙ Шаблевська К.Д., Євдокимов І.І., Науковий керівник: Порохнявий А.В.	239

СИСТЕМА НОТАРІАЛЬНИХ ОРГАНІВ І ПОСАДОВИХ ОСІБ, НА ЯКИХ ПОКЛАДЕНО ОБОВ'ЯЗОК ВЧИНЯТИ НОТАРІАЛЬНІ ДІЇ В УКРАЇНІ. ЇХ КОМПЕТЕНЦІЯ Поліщук Є.Д., Науковий керівник: Золотухіна Л.О.....	246
СПЕЦИФІКА УКЛАДАННЯ НОВИХ ДОГОВОРІВ ПРО НАДАННЯ ПОСЛУГ В УМОВАХ ВОЄННОГО СТАНУ Кандаур К.А., Кравченко А.С., Науковий керівник: Фролов М.М.	252
ТЕХНОЛОГІЇ БЕЗПЕКИ: ЯК СУЧАСНЕ ОБЛАДНАННЯ ЗАХИЩАЄ ВИБУХОТЕХНІКІВ Кошевич М.В., Патока Д.С., Науковий керівник: Король К.С.....	258

РОЗДІЛ 9. КОМП'ЮТЕРНА ТА ПРОГРАМНА ІНЖЕНЕРІЯ

АНАЛІЗ ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ ПРОФЕСІЙНО-ОРІЄНТОВАНИХ ЗАВДАНЬ У НАВЧАЛЬНИЙ ПРОЦЕС Петро О.В., Науковий керівник: Тютюнникова Г.С.....	265
---	-----

РОЗДІЛ 10. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

АНАЛІЗ ТА ВИБІР ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ АВТОМАТИЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ ВИЗНАЧЕННЯ ПОТРЕБ СИРОВИНИ НА ПІДПРИЄМСТВАХ Ганжила Н.Б., Науковий керівник: Панфьорова І.Ю.....	273
ІНСТРУМЕНТИ РОЗРОБНИКА РЕЛЯЦІЙНОЇ БАЗИ ДАНИХ Міщенко А.А., Науковий керівник: Михайлова І.Ю.....	284
КІБЕРЗЛОЧИН В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ Помінчук Я.В., Науковий керівник: Любавіна В.П.....	289

РОЗДІЛ 11. ФІЗИКО-МАТЕМАТИЧНІ НАУКИ

ПАТРІОТИЧНЕ ВИХОВАННЯ НА УРОКАХ МАТЕМАТИКИ У СТАРШІЙ ШКОЛІ Компанець Ю.В.	298
---	-----

РОЗДІЛ 12. ФІЛОЛОГІЯ ТА ЖУРНАЛІСТИКА

АБРЕВІАЦІЇ В АНГЛІЙСЬКІЙ ТА УКРАЇНСЬКІЙ МОВАХ: ЗІСТАВНИЙ АНАЛІЗ НА МАТЕРІАЛІ ПУБЛІКАЦІЙ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ Хитрень О.І., Науковий керівник: Карамішева І.Д.	305
--	-----

ЗМІСТ

АСТРАЛЬНІ ОБРАЗИ В ПОЕЗІЇ БОЛЕСЛАВА ЛЕСЬМЯНА Безлюдько К.М., Науковий керівник: Ткачук Т.О.	312
КОНЦЕПТУАЛІЗАЦІЯ ЕКЗИСТЕНЦІЙНИХ АСПЕКТІВ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ У СУЧАСНОМУ УКРАЇНСЬКОМУ ХУДОЖНЬОМУ ДИСКУРСІ В КОРПУСІ Груба О.О., Науковий керівник: Романишин Н.І.	317
НАВЧАННЯ МАЙБУТНІХ ВИКЛАДАЧІВ АНАЛІЗУ ЗАСОБІВ СТВОРЕННЯ ОБРАЗІВ - ПЕРСОНАЖІВ (НА МАТЕРІАЛІ РОМАНУ JANE AUSTEN "PERSUASION") Саницька В.Л., Науковий керівник: Жаборук І.А.	322
ОКАЗИОНАЛЬНІ НОВОТВОРИ В СУЧАСНІЙ ВОЄННІЙ ПОЕЗІЇ Зейда І.М., Науковий керівник: Максимчук В.В.	330
СТВОРЕННЯ КОРПУСУ НЕОЛОГІЗМІВ ТА ОПИС ПРОЦЕСУ ЇХ СЕМАНТИЧНОГО АНОТУВАННЯ Корпан Л.Б., Науковий керівник: Романишин Н.І.	337

**РОЗДІЛ 13.
ФІЛОСОФІЯ ТА ПОЛІТОЛОГІЯ**

СВІТОГЛЯДНА ПРИРОДА ФІЛОСОФСЬКОГО ЗНАННЯ Козак Д.Т.	347
---	-----

**РОЗДІЛ 14.
ПЕДАГОГІКА ТА ОСВІТА**

ІНТЕГРАЦІЯ КОМП'ЮТЕРНИХ ІГОР У МЕТОДИКУ ФОРМУВАННЯ АНГЛОМОВНОЇ ФОНЕТИЧНОЇ КОМПЕТЕНТНОСТІ МОЛОДШОГО ШКОЛЯРА Новосад С.Р., Науковий керівник: Дячук Н.М.	354
МАНДРІВКА У ЗМІСТ ВИХОВАННЯ. ІЄРАРХІЯ СИСТЕМИ ЦІННОСТЕЙ Козак Д.Т.	361
ОСОБЛИВОСТІ ЕКОНОМІЧНОГО ВИХОВАННЯ ДІТЕЙ СТАРШОГО ДОШКІЛЬНОГО ВІКУ Дрогуль Г.В., Науковий керівник: Войналович О.О.	366
ОСОБЛИВОСТІ ФОРМУВАННЯ АНГЛОМОВНОЇ ПИСЕМНОЇ КОМПЕТЕНЦІЇ УЧНІВ СТАРШОЇ ШКОЛИ ЗАСОБАМИ ОНЛАЙН ПЛАТФОРМ Шиманська Г.А., Науковий керівник: Зелена І.О.	371
РОЗВИТОК СПРИЙНЯТТЯ ОБМЕЖЕНОГО МОВЛЕННЯ У МОЛОДШИХ ШКОЛЯРІВ ІЗ ПОРУШЕННЯМ ІНТЕЛЕКТУ В УМОВАХ ІНКЛЮЗИВНОГО НАВЧАННЯ Лозовська І.В., Науковий керівник: Мога М.Д.	379

СУЧАСНІ МЕТОДИ НАВЧАННЯ МАТЕМАТИКИ В АСПЕКТІ ОСОБИСТІСНОГО САМОРОЗВИТКУ УЧНІВ Салій А.С.	384
--	-----

РОЗДІЛ 15. ПСИХОЛОГІЯ ТА ПСИХІАТРІЯ

ВЗАЄМОЗВ'ЯЗОК ОСОБИСТІСНОЇ ЗРІЛОСТІ З ФАКТОМ ВИНИКНЕННЯ ПСИХОЛОГІЧНОГО БЕЗПЛІДДЯ Кривошеєва М.А., Науковий керівник: Кучманіч І.М.	389
ГЕНДЕРНІ ОСОБЛИВОСТІ ЕМОЦІЙНОГО ВИГОРАННЯ СЕРЕД СТУДЕНТІВ, ЩО ПРАЦЮЮТЬ Чаплінська М.В., Науковий керівник: Лисенкова І.П.	396
ПСИХОЛОГІЧНА РЕАБІЛІТАЦІЯ ВЕТЕРАНІВ: ПОДОЛАННЯ ДЕФОРМАЦІЙ ОСОБИСТІСНОГО ТА ПРОФЕСІЙНОГО ХАРАКТЕРУ Кокошко Б.Р., Науковий керівник: Сафін О.Дж.	402
ПСИХОЛОГІЧНИЙ ВПЛИВ ВІЙСЬКОВОЇ СЛУЖБИ НА СІМЕЙНІ СТОСУНКИ: АДАПТАЦІЯ ВІЙСЬКОВИХ ТА ЇХ РОДИН Балачій Л.О.	409
ФАКТОРИ РИЗИКУ СУЇЦИДАЛЬНИХ НАСТРОЇВ СЕРЕД ВІЙСЬКОВОСЛУЖБОВЦІВ: ПОПЕРЕДЖЕННЯ ТА ПСИХОЛОГІЧНА ПІДТРИМКА Жданюк А.І.	417

РОЗДІЛ 16. МЕДИЧНІ НАУКИ ТА ГРОМАДСЬКЕ ЗДОРОВ'Я

НЕЙРОТРОПНА ТЕРАПІЯ ГІПОКСИЧНО-ІШЕМІЧНОЇ ЕНЦЕФАЛОПАТІЇ В НОВОНАРОДЖЕНИХ ДІТЕЙ: СУЧАСНИЙ СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВИРІШЕННЯ ПИТАННЯ Стромило А.В., Науковий керівник: Маліч Т.С.	425
--	-----

РОЗДІЛ 17. ФІЗИЧНА КУЛЬТУРА, СПОРТ ТА ФІЗИЧНА ТЕРАПІЯ

ВАЖЛИВІСТЬ СПЕЦІАЛЬНОЇ ФІЗИЧНОЇ ПІДГОТОВКИ ДЛЯ ПОЛІЦЕЙСЬКИХ Войхевич Д.С., Овчинников О.В., Науковий керівник: Порохнявий А.В.	435
ОСОБЛИВОСТІ ФІЗИЧНОГО ТА ПСИХІЧНОГО РОЗВИТКУ ДІТЕЙ З ОСОБЛИВИМИ ОСВІТНИМИ ПОТРЕБАМИ (ООП) Літвінов Р.О., Могиленко А.В., Науковий керівник: Пожидаєв М.Ю.	440
РОЛЬ ФІЗИЧНОЇ ПІДГОТОВКИ ПОЛІЦЕЙСЬКОГО У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ Білан О.Є., Кіщенко А.Ю., Науковий керівник: Порохнявий А.В.	447

ЗМІСТ

ФУНКЦІОНАЛЬНА ПІДГОТОВКА ЯК ОСНОВА СПЕЦІАЛЬНОЇ ФІЗИЧНОЇ ПІДГОТОВКИ ДЛЯ ПРАВООХОРОНЦІВ Будчик Д.А., Іщенко Д.С., Науковий керівник: Порохнявий А.В.....	454
---	-----

РОЗДІЛ 18.**КУЛЬТУРА ТА МИСТЕЦТВО**

ВПЛИВ СВІТОВИХ ТЕНДЕНЦІЙ ВУЛИЧНОЇ МОДИ НА ФОРМУВАННЯ МОЛОДІЖНОГО СТИЛЮ В СУЧАСНОМУ ОДЯЗІ Заїкіна М.С., Науковий керівник: Колосніченко О.В.	461
---	-----

РОЗДІЛ 10.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

Помінчук Яна Віталіївна

здобувачка вищої освіти факультету фінансів та цифрових технологій
Державний податковий університет, Україна

Науковий керівник: Любавіна Вікторія Петрівна

канд. юрид. наук, доцент кафедри кримінального права та процесу
Державний податковий університет, Україна

КІБЕРЗЛОЧИН В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ

АНОТАЦІЯ. У статті досліджено природу та еволюцію кіберзлочинності в Україні, проаналізовано основні тенденції розвитку кіберзлочинності, а також вивчені фактори, що сприяють її поширенню. Розглянуто основні положення законодавства України щодо боротьби з кіберзлочинами, включаючи аналіз актуальних норм та ініціатив, що регулюють цю сферу. Виявлено недоліки в правовій системі України, такі як застарілість норм, недостатня координація між правоохоронними органами, відсутність ефективних механізмів міжнародного співробітництва, а також проблеми в розслідуванні кіберзлочинів. Запропоновано шляхи вдосконалення законодавства України у сфері кібербезпеки, зокрема: інтеграція міжнародних норм та стандартів, підвищення рівня освіти і підготовки кадрів у сфері кібербезпеки, удосконалення механізмів співпраці з міжнародними організаціями, а також посилення відповідальності за кіберзлочини. Встановлено, що впровадження цих заходів може суттєво покращити ефективність боротьби з кіберзлочинністю в Україні, зробити цю боротьбу більш системною та цілеспрямованою, а також сприяти підвищенню рівня безпеки в інформаційній сфері.

КЛЮЧОВІ СЛОВА: кіберзлочинність, кібербезпека, законодавство, міжнародні стандарти, боротьба з кіберзлочинами, Україна.

Кіберзлочинність є комплексом злочинної діяльності, що відбувається у цифровому просторі та включає в себе широкий спектр дій — від фішингових атак і шкідливого програмного забезпечення до кібертероризму та крадіжки персональних даних. Здебільшого кіберзлочинність асоціюється з поняттям "несанкціонованого доступу" або "хакерства", однак у цифровій сфері існує чимало інших форм незаконної діяльності, що можуть завдати значної шкоди як окремим особам, так і бізнесу чи суспільству загалом.

З розвитком інформаційних технологій світ дедалі глибше інтегрується в цифрове середовище, що водночас відкриває нові можливості для злочинців, які використовують передові технології для реалізації своїх протиправних намірів. Поширення інтернету, мобільних пристроїв та цифрових платформ надає злочинцям широкий спектр інструментів, завдяки яким кіберзлочинність сьогодні вже є однією з найприбутковіших форм злочинної діяльності у світі. За оцінками експертів, у 2021 році глобальні збитки від кіберзлочинності сягнули 6 трильйонів доларів США, що, у разі її уявного представлення як окремої економіки, вивело б кіберзлочинність на третє місце за масштабом економічної потужності після США та Китаю [13].

Актуальність теми кіберзлочинності стає особливо значущою на тлі швидкого розвитку технологій, які безпосередньо впливають на безпеку в інформаційному середовищі. Впровадження нових технологічних рішень, зокрема криптовалют та блокчейну, спричинило появу нових форм фінансових шахрайств, що значно ускладнюють процеси виявлення злочинців та проведення розслідувань. Окрім того, кіберзлочинці постійно вдосконалюють свої методи, активно застосовуючи техніки соціальної інженерії для маніпулювання жертвами з метою отримання конфіденційної інформації. Це посилює потребу в розробці ефективних заходів безпеки та актуалізує дослідження кіберзлочинності як явища, що становить загрозу на глобальному рівні.

Зважаючи на масштаб і різноманітність кіберзлочинності, ця проблема набуває дедалі більшої ваги як на національному, так і на глобальному рівнях. Від фішингових атак і шкідливих програм до цілеспрямованих кібернападів на критичну інфраструктуру — сучасні кіберзлочинці активно використовують новітні технології, адаптуючи їх для досягнення своїх злочинних цілей. Ця діяльність охоплює всі аспекти цифрового середовища, а її наслідки можуть бути руйнівними не лише для окремих осіб, а й для цілих секторів економіки, а іноді й для цілих країн.

Така ситуація підкреслює необхідність поглибленого дослідження кіберзлочинності та розробки ефективних засобів для боротьби з нею. З огляду на це, питання безпеки стає одним із ключових пріоритетів для компаній, урядів і міжнародних організацій. Важливість обізнаності щодо кіберзагроз, розуміння новітніх злочинних тактик і розробка стратегій захисту є вирішальними елементами для забезпечення стабільності та безпеки у цифровому середовищі.

Аналіз останніх досліджень та публікацій. Питання кіберзлочинності залишається надзвичайно актуальним, однак наукова спільнота не приділяє йому достатньої уваги. Кількість публікацій, що глибоко досліджують проблеми кіберзлочинності, механізми її виникнення та протидії, залишається недостатньою. Це ускладнює формування ефективної стратегії боротьби з

РОЗДІЛ 10.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

кіберзлочинами, оскільки відсутність теоретичного підґрунтя не дозволяє отримати цілісне бачення проблеми.

Аналіз доступних матеріалів демонструє, що наявні дослідження здебільшого зосереджені на окремих аспектах кіберзлочинності, не утворюючи системного підходу до цієї теми. Зокрема, дослідження механізмів виникнення кіберзлочинів та їхньої еволюції, ролі сучасних технологій, таких як штучний інтелект і блокчейн, у захисті від кіберзагроз залишаються недостатньо розробленими. Це створює складнощі у формуванні ефективних державних і корпоративних стратегій безпеки.

Крім того, доступні матеріали вказують на необхідність глибшого аналізу ролі держави та суспільства у протидії кіберзлочинності. Оскільки кіберзагрози не обмежуються межами окремих країн, міжнародна співпраця та обмін інформацією стають ключовими елементами боротьби з цим видом злочинної діяльності. Отже, для ефективної протидії кіберзлочинності необхідне не лише покращення технічних рішень, а й ґрунтовне теоретичне підґрунтя, що дозволить забезпечити цілісне бачення проблеми та розробити ефективну стратегію протидії.

Метою даної статті є дослідження проблеми кіберзлочинності в інформаційних технологіях, аналіз її впливу на суспільство та економіку, а також виявлення ефективних методів боротьби з цим явищем. Стаття має на меті висвітлити основні види кіберзлочинності, їх наслідки та ризики, з якими стикаються як індивідуальні користувачі, так і великі корпорації та державні установи. Окрім цього, у статті будуть запропоновані рекомендації щодо підвищення рівня кібербезпеки та важливості міжнародної співпраці у боротьбі з кіберзлочинністю, щоб створити безпечніше цифрове середовище для всіх.

Кіберзлочинність охоплює широкий спектр незаконних дій, що здійснюються в цифровому середовищі. Серед основних видів кіберзлочинності можна виділити такі:

Фішинг: Фішинг є однією з найпоширеніших форм кіберзлочинності, яка передбачає використання підроблених електронних листів, веб-сайтів або повідомлень для обману користувачів з метою отримання конфіденційної інформації, такої як паролі, номери кредитних карток або особисті дані. Найчастіше зловмисники, які займаються фішингом видають себе за банки чи інші фінансові установи, щоб змусити жертву заповнити фальшиву форму та отримати дані облікових записів. У минулому для виманювання даних користувачів кіберзлочинці часто використовували неправильно написані або оманливі доменні імена. Сьогодні зловмисники використовують більш складні методи, завдяки чому фальшиві сторінки дуже схожі на свої легітимні аналоги[11].

Шкідливе програмне забезпечення (malware): Шкідливе програмне

забезпечення включає в себе різні види програм, які створюються для порушення нормального функціонування комп'ютерних систем, викрадення даних або шантажу користувачів. Основні типи шкідливого програмного забезпечення включають віруси, троянські програми, шпигунські програми та руткити. Кіберзлочинці постійно шукають нові способи інфікування. Зокрема сучасні загрози поширюються через уразливості систем, уникаючи засобів безпеки, приховуються в пам'яті або імітують легітимні програми, щоб залишатися непоміченими. Однак найчастіше інфікування пристроїв відбувається через людську необережність. Спеціально розроблені електронні листи з небезпечними вкладеннями виявились ефективним та дешевим способом проникнення в систему жертв. Для цього зловмисникам потрібен лише один невірний клік користувача[12].

Крадіжка особистих даних: Злодії, які займаються викраденням даних, зазвичай, отримують особисту інформацію, таку як паролі, номери ID, кредитних карток або номери соціального страхування, та використовують ці дані від імені жертви. Викрадена конфіденційна інформація може бути використана для різних незаконних цілей, зокрема для отримання кредитів, здійснення онлайн-покупок або для отримання доступу до медичних та фінансових відомостей жертви. Крадіжка даних тісно пов'язана з фішингом та іншими методами соціальної інженерії, які часто використовуються для отримання конфіденційних відомостей жертви. Публічні профілі в соціальних мережах або інших популярних онлайн-сервісах також можуть стати джерелом даних для зловмисників. Після отримання потрібних фактів про жертву, зловмисники використовують її для замовлення товарів та доступу до онлайн-рахунків жертв. В свою чергу, жертви можуть зазнати фінансових втрат внаслідок несанкціонованого зняття коштів та покупок від їх імені[1].

Троянські програми: Подібно до троянського коня, відомого з давньогрецьких міфів, троян використовує маскування або неправильне перенаправлення, щоб приховати свою справжню функцію. Щоб ввести користувача в оману та змусити його відкрити шкідливий файл, загроза часто використовує різні методи. Для цих цілей троян також може використовувати інші програми. Сьогодні трояни є найпоширенішою категорією шкідливих програм, яка використовується для відкриття бекдорів, контролю інфікованого пристрою, видалення даних користувача та передачі їх зловмисникам, завантаження та запуску інших шкідливих програм у певній системі та інших цілей[10].

Віруси-вимагачі (ransomware): Цей вид шкідливого програмного забезпечення використовується кіберзлочинцями для вимагання коштів у жертв. Зазвичай, програма-вимагач блокує екран пристрою жертви або шифрує дані на диску, відображаючи вимогу про викуп із реквізитами платежу[9].

РОЗДІЛ 10.**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ**

Кіберзлочинність має значний вплив на різні аспекти суспільного життя, охоплюючи економічні, соціальні та психологічні наслідки. Її наслідки відчуваються не лише на рівні окремих осіб, але й на масштабі великих корпорацій, державних установ і суспільства в цілому.

Економічні наслідки: Кіберзлочинність завдає серйозних збитків економіці, зокрема у формі фінансових втрат. Згідно з даними досліджень, глобальні збитки від кіберзлочинності щорічно обчислюються трильйонами доларів США. Ці втрати виникають не лише внаслідок крадіжок даних та фінансових шахрайств, але також через витрати на відновлення інформаційних систем, удосконалення заходів безпеки та юридичні витрати. Компанії змушені інвестувати в кібербезпеку, щоб захистити свої дані, що може призвести до підвищення витрат на обслуговування бізнесу. У свою чергу, ці витрати можуть відображатися на ціні товарів і послуг, що негативно позначається на кінцевих споживачах.

Соціальні наслідки: Кіберзлочинність підриває рівень довіри в суспільстві. Коли особи стають жертвами шахрайства, це може призводити до втрати довіри до онлайн-сервісів, електронної комерції та навіть до державних установ, які зобов'язані забезпечувати безпеку своїх громадян.

Психологічні наслідки: Жертви кіберзлочинності часто відчувають психологічний дискомфорт, що може призводити до стресу, тривоги та депресивних станів. Втрата особистих даних або фінансових ресурсів може викликати почуття безпорадності та ізоляції. Багато осіб можуть почати уникати використання цифрових технологій.

Вплив на державні установи: Державні структури також підпадають під загрозу кіберзлочинності, оскільки зловмисники можуть намагатися скомпрометувати дані або системи, що забезпечують національну безпеку. Атаки на критично важливу інфраструктуру, таку як енергетичні мережі, системи водопостачання або охорони здоров'я, можуть мати катастрофічні наслідки для суспільства. Злочинці можуть намагатися маніпулювати політичними процесами або створювати паніку в суспільстві через поширення дезінформації.

В Україні питання кібербезпеки регулюється низкою законодавчих актів, які визначають правові засади для забезпечення захисту інформаційних систем, даних та критичної інфраструктури від кіберзагроз. Основні нормативно-правові документи, що регулюють цю сферу, включають:

- Закон України "Про основи забезпечення кібербезпеки України". Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері,

основні засади координації їхньої діяльності із забезпечення кібербезпеки[6].

- Закон України "Про захист інформації в інформаційно-комунікаційних системах". Цей Закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах[3].

- Закон України "Про електронні довірчі послуги". Цей Закон визначає правові та організаційні засади електронної ідентифікації та надання електронних довірчих послуг, права та обов'язки суб'єктів відносин у сферах електронної ідентифікації та електронних довірчих послуг, порядок здійснення державного контролю за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг[2].

- Закон України "Про захист персональних даних". Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних[4].

- Закон України "Про національну безпеку України". Цей Закон відповідно до статей 1, 2, 17, 18 і 92 Конституції України визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз. Цим Законом визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони. [5].

- Постанови Кабінету Міністрів України – на рівні виконавчої влади розроблені різні нормативно-правові акти, які регламентують питання кібербезпеки, зокрема, функціонування Національної поліції, Служби безпеки України та інших органів у контексті протидії кіберзлочинності.

З метою забезпечення ефективного виконання законодавства у сфері кібербезпеки Україна прагне посилити співпрацю з міжнародними партнерами, зокрема з такими організаціями, як НАТО, Європейський Союз та ООН. Ця взаємодія включає обмін передовими практиками, досвідом і технологіями для посилення спроможності у протидії кіберзагрозам та адаптації до глобальних викликів у сфері інформаційної безпеки. Одночасно здійснюються заходи щодо вдосконалення національної законодавчої бази, що сприяє своєчасному оновленню правових норм та підвищенню здатності

РОЗДІЛ 10.**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ**

реагувати на нові виклики й загрози кібербезпеки.

Міжнародна співпраця в боротьбі з кіберзлочинністю є важливим елементом забезпечення глобальної кібербезпеки. Країни об'єднують зусилля для створення спільних нормативних стандартів, оперативного обміну інформацією та поширення найкращих практик у цій сфері. Такі міжнародні організації, як Інтерпол, Європол та Організація Об'єднаних Націй, відіграють ключову роль, розробляючи рекомендації та стандарти, що сприяють єдиному підходу до захисту від кіберзагроз.

Міжнародне співробітництво також передбачає спеціалізовані освітні програми для фахівців з кібербезпеки. Зокрема, країни проводять спільні тренінги та навчання, що дозволяє підвищити професійний рівень працівників як у державному секторі, так і в приватних компаніях. Такий підхід сприяє ефективному обміну знаннями і досвідом та створенню єдиного фронту протидії кіберзлочинності на міжнародному рівні.

Для захисту особистих файлів і конфіденційної інформації необхідно дотримуватись комплексних заходів кібербезпеки:

1. Забезпечення безпечного з'єднання. Для введення конфіденційних даних у мережі Інтернет рекомендовано користуватися виключно захищеними з'єднаннями, такими як домашня чи корпоративна мережа. У разі потреби використання публічних мереж Wi-Fi, зокрема тих, що не захищені паролем, слід скористатися віртуальною приватною мережею (VPN) для шифрування переданих даних і зниження ризику їх перехоплення.

2. Встановлення захисного програмного забезпечення. Для запобігання проникненню шкідливого програмного забезпечення та несанкціонованому доступу до пристроїв необхідно застосовувати багаторівневе антивірусне програмне забезпечення. Важливо регулярно оновлювати операційну систему та інші програми для усунення вразливостей, що можуть бути використані зловмисниками.

3. Застосування надійних паролів. Рекомендується створювати унікальні, довгі паролі для кожного облікового запису, уникаючи використання однакових паролів для різних сервісів. Для підвищення безпеки доцільно використовувати двофакторну аутентифікацію та спеціалізовані менеджери паролів, які сприяють зберіганню складних комбінацій.

4. Попередження фішингових атак. Для зниження ризику фішингових атак необхідно ретельно перевіряти електронні листи і посилання, зокрема у випадку запитів на введення облікових даних. Не слід переходити за підозрілими посиланнями чи завантажувати файли з невідомих джерел.

5. Регулярне резервне копіювання даних. Для мінімізації втрат у разі втрати чи пошкодження файлів слід здійснювати регулярне резервне копіювання даних на окремих носіях або у хмарних сховищах.

6. Моніторинг фінансових рахунків. Регулярний перегляд банківських та

кредитних рахунків дозволяє вчасно виявити підозрілі транзакції. Установлення лімітів на певні операції може допомогти запобігти несанкціонованому використанню коштів.

7. Контроль конфіденційної інформації. При утилізації або передачі пристроїв необхідно попередньо очищати їх від особистих даних. Фізичні документи, що містять конфіденційні відомості, слід безпечно знищувати, щоб виключити можливість їх несанкціонованого використання.

8. Обмеження поширення інформації в соціальних мережах. Публікація конфіденційних даних у соціальних мережах повинна бути мінімізована, оскільки така інформація може бути використана для отримання несанкціонованого доступу.

Комплексна реалізація наведених рекомендацій дозволить суттєво підвищити рівень безпеки та знизити ризик втрати чи компрометації особистих даних у цифровому середовищі.

Висновки. Висновки з проведеного аналізу свідчать про те, що кіберзлочинність стала невід'ємною частиною сучасного суспільства, суттєво впливаючи на різні його аспекти. У світлі стрімкого розвитку технологій і постійної еволюції злочинних схем, необхідність у формуванні ефективних заходів протидії кіберзлочинності стає дедалі актуальнішою. Держави повинні вжити рішучих заходів для адаптації своїх законодавств до нових викликів, а також розвивати міжнародну співпрацю у цій сфері, оскільки кіберзлочини часто виходять за межі національних кордонів.

З огляду на серйозність цієї проблеми, необхідно вжити комплексних заходів для боротьби з кіберзлочинністю. Це включає в себе удосконалення існуючого законодавства, розробку нових стратегій кібербезпеки, навчання та підвищення обізнаності населення про потенційні загрози. Міжнародна співпраця також є важливою для обміну інформацією та кращих практик у боротьбі з кіберзлочинністю.

Узагальнюючи, для ефективної протидії кіберзлочинності необхідно не лише покращувати технічні засоби захисту, але й формувати системний підхід до дослідження цього явища, що дозволить зрозуміти його природу, механізми та наслідки. Тільки спільними зусиллями держав, бізнесу та суспільства можливо створити безпечніше цифрове середовище, яке відповідає вимогам сучасного світу.

Список використаних джерел:

- [1] Викрадення даних. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/krazha-dannykh/>.
- [2] Закон України "Про електронні довірчі послуги". URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.
- [3] Закон України "Про захист інформації в інформаційно-комунікаційних системах". URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

РОЗДІЛ 10.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

- [4] Закон України "Про захист персональних даних". URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
- [5] Закон України "Про національну безпеку України". URL: <https://ips.ligazakon.net/document/T182469?an=429>.
- [6] Закон України "Про основи забезпечення кібербезпеки України". URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
- [7] Комп'ютерний вірус. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/kompyuternyy-virus/>.
- [8] Національна стратегія кібербезпеки України. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7>.
- [9] Програми-вимагачі. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/programma-vumogatel/>.
- [10] Троян. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/troyan/?srsId=AfmBOoqSupkZKDcG22eKs2Af-iE__ju2GAdyDGXB54fzFsAaQmTIJ18F.
- [11] Фішинг. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/?srsId=AfmBOoqlr2EIUCoqEX8nC8LojgMy11yLdkyoozI5acU6dT685ixWKckS>.
- [12] Шкідливі програми. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/vredonosnyye-programmy/>.
- [13] Якщо уявити Кіберзлочинність як країну це була б третя економіка світу. URL: <https://10guards.com/ua/blog/2022/08/08/cybercrime-as-empire-would-be-the-worlds-third-largest-economy/>.