



Наукові перспективи  
Видавнича група

№ 4 (32)

2024

# НАУКА і ТЕХНІКА

серія: право, серія: економіка, серія: педагогіка,  
серія: техніка, серія: фізико-математичні науки

СЬОГОДНІ



З Україною

в серці!



**Видавнича група «Наукові перспективи»**

**Громадська наукова організація «Всеукраїнська Асамблея  
докторів наук із державного управління»**

**Громадська організація «Асоціація науковців України»**

## ***«Наука і техніка сьогодні»***

*(Серія «Педагогіка», Серія «Право», Серія «Економіка»,  
Серія «Фізико-математичні науки», Серія «Техніка»)*

**Випуск № 4(32) 2024**

**Київ – 2024**

**Publishing Group «Scientific Perspectives»**

**Public Scientific Organization «Ukrainian Assembly of  
Doctors of Sciences in Public Administration»**

**Public organization «Association of Scientists of Ukraine»**

***"Science and technology today"***  
*("Pedagogy" series, "Law" series, "Economics" series,  
"Physical and mathematical sciences" series, "Technics" series)*

**Issue № 4(32) 2024**

**Kiev – 2024**



**«Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право»,  
Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»):  
журнал. 2024. № 4(32) 2024. С. 1275**



*Згідно наказу Міністерства освіти і науки України від 07.04.2022 № 320 журналу присвоєно категорію "Б" із економіки та педагогіки (спеціальності – 015 - Педагогічні науки; 076 - Економічні науки)*

*Згідно наказу Міністерства освіти і науки України від 06.06.2022 № 530 журналу присвоєно категорію "Б" із права (спеціальність – 081 Юридичні науки)*

*Згідно наказу Міністерства освіти і науки України від 10.10.2022 № 894 журналу присвоєно категорію "Б" із техніки (спеціальність - 122 Комп'ютерні науки)*

*Журнал видається за підтримки Міждержавної гільдії інженерів консультантів, Інституту філософії та соціології Національної Академії Наук Азербайджану (Баку, Азербайджан), Християнської академії педагогічних наук України та Всеукраїнської асоціації педагогів і психологів з духовно-морального виховання*

*Рекомендовано до видавництва Президією Всеукраїнської Асамблеї докторів наук з державного управління (Рішення від 24.04.2024, № 8/4-24)*



Журнал включено до міжнародної наукометричної бази Index Copernicus (IC), міжнародної пошукової системи Google Scholar та до міжнародної наукометричної бази даних Research Bible

**Головний редактор:** Сопілко Ірина Миколаївна - доктор юридичних наук, професор, Відмінник освіти України, Лауреат Премії Президента України для молодих вчених, Лауреат Премії Верховної Ради України найталановитішим молодим ученим в галузі фундаментальних і прикладних досліджень та науково-технічних розробок, академік Академії наук вищої школи України, Заслужений юрист України (Київ, Україна)

**Редакційна колегія:**

- Артемчук Володимир Олександрович - доктор технічних наук, старший науковий співробітник, старший науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (Київ, Україна)
- Бахов Іван Степанович – доктор педагогічних наук, професор, завідувач кафедри іноземної філології та перекладу Міжрегіональної академії управління персоналом (Київ, Україна)
- Будник Вікторія Анатоліївна - кандидат економічних наук, професор, професор кафедри бізнес-логістики та транспортних технологій Державного університету інфраструктури та технологій (Київ, Україна)
- Волк Павло Павлович – доцент кафедри водної інженерії та водних технологій Національного університету водного господарства та природокористування (Рівне, Україна)
- Гирка Ольга Ігорівна - кандидат технічних наук, доцент, доцент кафедри товарознавства, митної справи та управління якістю Львівського торговельно-економічного університету (Львів, Україна)
- Гнатюк Сергій Олександрович - кандидат технічних наук, доцент, заступник декана факультету аеронавігації, електроніки та телекомунікацій Національного авіаційного університету (Київ, Україна)
- Дацій Олександр Іванович - доктор економічних наук, професор, Заслужений працівник освіти України, завідувач кафедри фінансів, банківської та страхової справи Міжрегіональної академії управління персоналом (Київ, Україна)
- Двізінюк Михайло Михайлович - доктор фізико-математичних наук, професор, Завідувач відділу Відділу цивільного захисту та інноваційної діяльності Державної установи Інститут геохімії навколишнього середовища Національної академії наук України" (Київ, Україна)
- Дяденчук Альона Федорівна - кандидат технічних наук, старший викладач кафедри вищої математики і фізики Таврійського державного агротехнологічного університету імені Дмитра Моторного (Мелітополь, Україна)
- Забулонов Юрій Леонідович - доктор технічних наук, професор, Член-кореспондент НАН України, директор Державної установи «Інститут геохімії навколишнього середовища Національної академії наук України» (Київ, Україна)
- Ільїн Валерій Юрійович - доктор економічних наук, професор (Київ, Україна)
- Ільїна Анастасія Олександрівна - кандидат економічних наук, доцент, доцент кафедри публічного управління і адміністрування Національного торговельно-економічного університету (Київ, Україна)
- Кардаш Оксана Любомирівна – кандидат економічних наук, доцент кафедри комп'ютерних технологій та економічної кібернетики Навчально-наукового інституту автоматизації, кібернетики та обчислювальної техніки Національного університету водного господарства та природокористування (м. Рівне, Україна)
- Квасніков Володимир Павлович – доктор технічних наук, професор, завідувач кафедри комп'ютеризованих електротехнічних систем та технологій Національного авіаційного університету (Київ, Україна)

- Коваленко Валентин Васильович - доктор юридичних наук, професор, провідний науковий співробітник сектору авторського права та суміжних прав лабораторії авторського права та інформаційних технологій Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України (Київ, Україна)
- Коваленко Олена Михайлівна - кандидат педагогічних наук, провідний науковий співробітник відділу профільного навчання Інституту педагогіки НАПН України (Київ, Україна)
- Комнатний Сергій Олександрович - докторант кафедри філософії права та юридичної логіки Національної академії внутрішніх справ (Київ, Україна)
- Кравчук Володимир Миколайович — доктор юридичних наук, доцент, доцент кафедри конституційного, адміністративного та міжнародного права Волинського національного університету імені Лесі Українки (Луцьк, Україна)
- Кузьмич Людмила Володимирівна - доктор технічних наук, головний науковий співробітник Інституту водних проблем і меліорації Національної академії аграрних наук України (Київ, Україна)
- Куницький Сергій Олегович - кандидат технічних наук, старший дослідник, провідний науковий співробітник науково-дослідної частини Національного університету водного господарства та природокористування (Рівне, Україна)
- Лук'янчук Олександр Петрович — кандидат технічних наук, доцент, доцент кафедри будівельних, дорожніх, меліоративних, сільськогосподарських машин та обладнання Національного університету водного господарства та природокористування (Рівне, Україна)
- Маджд Світлана Михайлівна - доктор технічних наук, професор, професор кафедри зеленої економіки та економіки природокористування Державної екологічної академії післядипломної освіти та управління (Київ, Україна)
- Мануель Давид Массено - доцент відділу права та захисту даних, старший науковий співробітник і член координаційного комітету лабораторії UbiNET, запрошений член PDPC, член-консультант комісії цифрового права муніципальних адвокатських колегій Кампінаса та Прая-Гранде (Сан-Паулу), а також Комісії з інновацій, управління та технологій муніципальної адвокатської колегії Гуарульуса, коментатор ЮДА, почесний член IDEIA Institute, член Наукового комітету MICHN, член EDEN, член-кореспондент RedNAC, член UMAU, член-кореспондент UBAU (Португалія)
- Микитин Тарас Миронович - кандидат технічних наук, завідувач кафедри менеджменту Рівненського державного гуманітарного університету (Рівне, Україна)
- Миргород-Карпова Валерія Валеріївна - кандидат юридичних наук, заступник директора з наукової роботи, старший викладач кафедри адміністративного, господарського права та фінансово-економічної безпеки Сумського державного університету (Суми, Україна)
- Мізюк Вікторія Анатоліївна - кандидат педагогічних наук, доцент, декан факультету управління, адміністрування та інформаційної діяльності Ізмаїльського державного гуманітарного університету (Ізмаїл, Україна)
- Мірошніченко Валентина Іванівна - доктор педагогічних наук, професор, завідувач кафедри психології, педагогіки та соціально-економічних дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького (Хмельницький, Україна)
- Міхальський Томаш — доктор наук, доцент кафедри географії регіонального розвитку Гданського університету (Польща)
- Огієнко Микола Миколайович - кандидат технічних наук, професор кафедри організації авіаційних робіт та послуг Національного авіаційного університету (Київ, Україна)
- Одарченко Роман Сергійович - завідувач кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету (Київ, Україна)
- Оніщенко Наталія Миколаївна - доктор юридичних наук, професор, Заслужений юрист України, академік НАПН України, завідувач відділу теорії держави і права Інституту держави і права ім. В.М.Корецького НАН України (Київ, Україна)
- Опанасенко Володимир Миколайович — доцент кафедри комп'ютеризованих електротехнічних систем та технологій Національного авіаційного університету (Київ, Україна)
- Охрімченко (Жмурко) Тетяна Олександрівна - старший науковий співробітник кафедри комп'ютеризованих систем управління Національного авіаційного університету (Київ, Україна)
- Павлов Костянтин Володимирович — доктор економічних наук, професор, завідувач кафедри підприємництва і маркетингу Волинського національного університету імені Лесі Українки (Луцьк, Україна)
- Поліщук Віталій Васильович — кандидат сільськогосподарських наук, завідувач відділу зрошення, відділення меліорації Інституту водних проблем і меліорації Національної академії аграрних наук України (Київ, Україна)
- Приходькіна Наталія Олександрівна - доктор педагогічних наук, професор кафедри педагогіки, адміністрування і спеціальної освіти Навчально-наукового інституту менеджменту та психології ДЗВО «Університет менеджменту освіти» НАПН України (Київ, Україна)
- Стахова Анжеліка Петрівна — старший викладач кафедри комп'ютеризованих електротехнічних систем та технологій Національного авіаційного університету (Київ, Україна)
- Турчинова Ганна Володимирівна — кандидат педагогічних наук, доцент, декан факультету природничо-географічної освіти та екології Національного педагогічного університету імені М.П. Драгоманова (Київ, Україна)
- Фесенко Андрій Олексійович - кандидат технічних наук, асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. (Київ, Україна)
- Черненко Варвара Петрівна - кандидат фізико-математичних наук, доцент кафедри інформатики і вищої математики Кременчуцького національного університету імені Михайла Остроградського (Кременчук, Україна)
- Чернуха Надія Миколаївна — доктор педагогічних наук, професор, професор кафедри соціальної реабілітації та соціальної педагогіки Київського національного університету імені Тараса Шевченка (Київ, Україна)
- Чумак Оксана Володимирівна - доктор економічних наук, доцент, науковий співробітник відділу статистики і аналітики вищої освіти Державної наукової установи «Інститут освітньої аналітики», (Київ, Україна)
- Шандра Наталія Андріївна - кандидат педагогічних наук, доцент кафедри іноземних мов для природничих факультетів Львівського національного університету імені Івана Франка (Львів, Україна)
- Шеремет Інеса Володимирівна - кандидат педагогічних наук, доцент, доцент кафедри медикобіологічних та валеологічних основ охорони життя і здоров'я Національного педагогічного університету ім. М. П. Драгоманова (Київ, Україна)
- Якимчук Аліна Юріївна - доктор економічних наук, професор, Академік економічних наук України, професор кафедри державного управління, документознавства та інформаційної діяльності Національного університету водного господарства та природокористування (Рівне, Україна)
- Якимчук Олег Феодосійович - керівник групи білінгу Відділу бізнес-систем Департаменту інформаційних технологій ПРАТ «Рівнеобленерго» (Рівне, Україна)
- Яцишин Андрій Васильович - доктор технічних наук, старший науковий співробітник, провідний науковий співробітник Відділу цивільного захисту та інноваційної діяльності Державної установи Інститут геохімії навколишнього середовища Національної академії наук України (Київ, Україна)

Статті розміщені в авторській редакції. Відповідальність за зміст та орфографію поданих матеріалів несуть автори.

# ЗМІСТ

## СЕРІЯ «Право»

**Брисковська О.М., Бурак М.В., Дякін Я.О.**

*ПРОБЛЕМИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ЗЛОЧИНАМ В СУЧАСНИХ УМОВАХ*

19

**Головін Р.Г.**

*ОРЕНДНА ПЛАТА ЗА ЗЕМЛЮ: РОЗМІР ПЛАТЕЖУ ТА ПОДАТКОВІ НАСЛІДКИ*

31

**Дацюк Т.К., Сєребряк С.В., Божко Д.В.**

*ПРАВОВИЙ СТАТУС ОКУПОВАНИХ ТЕРИТОРІЙ ТА ЗАХИСТ ПРАВ ЇХНЬОГО НАСЕЛЕННЯ (УКРАЇНСЬКІ РЕАЛІЇ)*

45

**Коваленко І.А., Коваль О.М.**

*ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я*

60

**Концевич В.А.**

*МЕТАМОРФОЗИ ПРАВОВОЇ РЕАЛЬНОСТІ: НОВІТНІ ПРАВА ЛЮДИНИ*

69

**Кравчук В.О.**

*ПОРІВНЯЛЬНИЙ АНАЛІЗ СУДОВОЇ ПРАКТИКИ КРАЇН ЄВРОПЕЙСЬКОГО СОЮЗУ ТА УКРАЇНИ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ*

78

**Красицька Л.В.**

*ПРАВО БАТЬКІВ НА ВИЗНАЧЕННЯ МІСЦЯ ПРОЖИВАННЯ МАЛОЛІТНЬОЇ ДИТИНИ ТА СУМІЖНІ ПРАВОВІ ПОНЯТТЯ*

91

**Сафронова Г.В., Дацюк Т.К.**

*ОСНОВНІ ЗАКОНОМІРНОСТІ І ЗАГАЛЬНІ ПОНЯТТЯ ПРО ДЕРЖАВУ І ПРАВО ЯК ВИРІШАЛЬНИЙ ЧИННИК У ПІДГОТОВЦІ КВАЛІФІКОВАНОГО ПРАВООХОРОНЦЯ У КОНТЕКСТІ РЕАЛІЗАЦІЇ ПРАВозАСТОСОВНОЇ ДІЯЛЬНОСТІ*

104

**Сергієнко Н.А.**

*ВИПРАВЛЕННЯ ПОМИЛКИ У ВИКОНАВЧОМУ ДОКУМЕНТІ ТА ВИЗНАННЯ ВИКОНАВЧОГО ДОКУМЕНТА ТАКИМ, ЩО НЕ ПІДЛЯГАЄ ВИКОНАННЮ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ*

115

**Стешенко Т.В., Мацнєва О.В., Шмига В.О.** 126  
*КОМУНІКАЦІЇ ТА ВЗАЄМОДІЯ МІЖ ОРГАНАМИ МІСЦЕВОГО  
САМОВРЯДУВАННЯ ТА ГРОМАДСЬКІСТЮ*

**Стешенко Т.В., Лещенко О.Ю., Жилка М.П.** 141  
*СТАРОСТА ЯК ІНСТИТУЦІЯ У МІСЦЕВОМУ САМОВРЯДУВАННІ, ЙОГО  
РОЛЬ У КОМУНІКАЦІЇ МІЖ ВЛАДОЮ ТА ГРОМАДОЮ. ПОРІВНЯЛЬНИЙ  
ДОСВІД ПОЛЬЩІ*

**Холодов В.В.** 156  
*СИСТЕМА ПРИНЦИПІВ ПРОТИДІЇ ТЕРОРИСТИЧНІЙ ЗАГРОЗІ В  
УМОВАХ МІСЬКОГО СЕРЕДОВИЩА: КОНЦЕПТУАЛІЗАЦІЯ ПРАВ  
ЛЮДИНИ*

**Чурпіта Г.В., Білянська Н.В.** 163  
*ПРАВОВЕ РЕГУЛЮВАННЯ ВИЗНАННЯ НЕОБҐРУНТОВАНИМИ АКТИВІВ  
ТА ЇХ СТЯГНЕННЯ В ДОХІД ДЕРЖАВИ*

**Шепета О.В.** 172  
*ПОРІВНЯЛЬНА ОЦІНКА ПІДХОДІВ ДЕРЖАВНОГО ТА ПРИВАТНОГО  
СЕКТОРІВ ДО КАДРОВОЇ ПОЛІТИКИ ПРОВІДНИХ ДЕРЖАВ СВІТУ У  
СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*

**Яновицька А.В., Вовк М.З.** 185  
*ПРАВОВА ОХОРОНА ОБ'ЄКТІВ, ЗГЕНЕРОВАНИХ ШТУЧНИМ  
ІНТЕЛЕКТОМ ТА ЗАХИСТ МАЙНОВИХ ПРАВ НА НИХ*

### **СЕРІЯ «Економіка»**

**Dzhereleiko S.D., Nagachevska O.O.** 193  
*MANAGEMENT OF THE COMMERCIAL BANK'S FINANCIAL STABILITY AS A  
COMPONENT OF DEVELOPMENT AND COMPETITIVENESS STRATEGY*

**Strelchenko O.H., Bukhtiiarova I.H., Bukhtiiarov O.A., Strelchenko A.M.** 208  
*FEATURES OF THE IMPLEMENTATION OF DIGITAL CURRENCY VALUES:  
FUNDAMENTAL PROBLEMS AND PROSPECTS FOR IMPROVEMENT*

**Березовська Н.І.** 217  
*СТАЛИЙ РОЗВИТОК У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ РОЗВИТКУ  
УКРАЇНИ*

**Бержанір І.А.** 231  
*ОРГАНІЗАЦІЯ ОБЛІКУ ВИТРАТ ПІДПРИЄМСТВА*

- Винничук Р.О., Нога А.Ю.** 242  
*ВИКОРИСТАННЯ ЧАТ-БОТІВ В HR-МЕНЕДЖМЕНТІ: АНАЛІЗ ВІТЧИЗНЯНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ*
- Гринь Д.В., Олійник Д.В., Горстка О.В.** 254  
*УМОВИ ТА ОХОРОНА ПРАЦІ ЯК ОБ'ЄКТ СОЦІАЛЬНО-ЕКОНОМІЧНОГО УПРАВЛІННЯ*
- Гук О.В.** 267  
*ІННОВАЦІЙНІ ПІДХОДИ ДО ФОРМУВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ МАЛИХ ТА СЕРЕДНІХ АГРАРНИХ ПІДПРИЄМСТВ*
- Дзвоник Р.Я.** 277  
*ПРИНЦИПИ ФОРМУВАННЯ І РОЗВИТКУ АНАЛІТИЧНОГО ІНСТРУМЕНТАРІЮ МЕНТИРИНГОВОЇ ДІЯЛЬНОСТІ НА ПІДПРИЄМСТВІ*
- Дробязко Л.В., Крамарева О.С.** 288  
*КОРПОРАТИВНЕ НАВЧАННЯ В СИСТЕМІ МЕТОДІВ РОЗВИТКУ ПРОФЕСІЙНИХ КОМПЕТЕНЦІЙ ПРАЦІВНИКІВ*
- Дяченко М.В.** 299  
*ФОРМУВАННЯ ІННОВАЦІЙНОЇ МОДЛІ РОЗВИТКУ АГРАРНОГО СЕКТОРУ УКРАЇНИ*
- Ільницький В.В.** 313  
*СИСТЕМА МІЖНАРОДНИХ ТРАНСПОРТНИХ ПЕРЕВЕЗЕНЬ В ЕКСТРЕМАЛЬНИХ УМОВАХ: СУТЬ ТА ЗМІСТ*
- Кондрат І.Ю., Озарків І.С.** 321  
*ІННОВАЦІЙНІ ІНСТРУМЕНТИ СТАЛОГО ФІНАНСУВАННЯ*
- Лезіна А.В.** 331  
*ВПЛИВ РИЗИКІВ ТА ЗАГРОЗ НА ПРОЦЕСИ ФОРМУВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ЕЛЕКТРОЕНЕРГЕТИЧНОЇ ГАЛУЗІ УКРАЇНИ*
- Мушеник І.М., Чернобай Л.М.** 344  
*АНАЛІЗ ВПЛИВУ ВІЙНИ НА МІЖНАРОДНІ ТРАНСПОРТНІ ПЕРЕВЕЗЕННЯ В УКРАЇНІ*
- Писаренко Н.В., Калінін А.М., Гуляєва Л.П., Ткаченко Я.С., Буткевич О.В., Медвідь Г.С.** 355  
*ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ЕКОЛОГІЧНОГО МАРКЕТИНГУ В КОНЦЕПЦІЇ ФОРМУВАННЯ ПОЛІТИКИ КОМПАНІЙ ЩОДО СТАЛОГО РОЗВИТКУ КОМПАНІЙ ТА ГРІНВОШИНГ*



- Помаза-Пономаренко А.Л., Тарадуда Д.В.** 371  
*ЗАКОРДОННИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ СОЦІАЛЬНОЇ БЕЗПЕКИ ШЛЯХОМ СТІЙКОГО ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ПІДВИЩЕНОЇ НЕБЕЗПЕКИ*
- Селюченко Н.Є., Селюченко М.О.** 385  
*КАПІТАЛЬНІ ІНВЕСТИЦІЇ У ТЕЛЕКОМУНІКАЦІЇ УКРАЇНИ: ДИНАМІКА ТА ВПЛИВ НА РЕЗУЛЬТАТИ ДІЯЛЬНОСТІ*
- Семененко Ю.С.** 396  
*ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ КОМАНД РОЗРОБКИ В ІТ КОМПАНІЯХ*
- Тоценко О.В., Богінська Л.О.** 411  
*РОЗВИТОК СИСТЕМИ ТРАНСПОРТНОГО ЗАБЕЗПЕЧЕННЯ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ АГРАРНОЇ СФЕРИ*
- Шульган М.Я.** 421  
*ОСОБЛИВОСТІ ТА УДОСКОНАЛЕННЯ СИНТЕТИЧНОГО І АНАЛІТИЧНОГО ОБЛІКУ ГОТОВОЇ ПРОДУКЦІЇ В БДЖІЛЬНИЦТВІ*
- Яновська В.П., Валявська Н.О., Парфентьєва О.Г., Медина А.П.** 441  
*МОВІЛІТУТЕСН У ПАСАЖИРСЬКИХ ПЕРЕВЕЗЕННЯХ: СТАВЛЕННЯ КОРИСТУВАЧІВ І НОВА ЯКІСТЬ ДЛЯ СТАЛОЇ МОБІЛЬНОСТІ*

### **СЕРІЯ «Педагогіка»**

- Kmit O.V.** 459  
*CREATING THE FREE-BULLYING EDUCATIONAL ENVIRONMENT OF PRIMARY SCHOOL*
- Matviienko L.H.** 473  
*PRINCIPLES OF INNOVATIVE PEDAGOGICAL ACTIVITY IN HIGHER EDUCATION INSTITUTIONS*
- Біда О.А., Кучай Т.П., Чичук А.П.** 486  
*ФОРМУВАННЯ ЕКОНОМІЧНОЇ КУЛЬТУРИ МАЙБУТНІХ ФАХІВЦІВ ЕКОНОМІЧНИХ СПЕЦІАЛЬНОСТЕЙ ЗАСОБАМИ АКМЕОЛОГІЧНОГО ПІДХОДУ*
- Білецька Л.С., Стасів Н.І.** 496  
*РОЗВИТОК ПАМ'ЯТІ ЯК ОДНОГО З КОМПОНЕНТІВ ЗАГАЛЬНОЇ КУЛЬТУРИ МИСЛЕННЯ УЧНІВ ПОЧАТКОВИХ КЛАСІВ*

- Василиків І.Б.** 508  
*ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНА КОМПЕТЕНТНІСТЬ ВЧИТЕЛЯ ПОЧАТКОВОЇ ШКОЛИ ЯК РЕЗУЛЬТАТ ПРОФЕСІЙНОЇ ПІДГОТОВКИ*
- Вітвицька С.С., Смаїлова Т.У.** 517  
*ПРОБЛЕМИ СІМЕЙНОГО ВИХОВАННЯ В ПЕДАГОГІЧНІЙ СПАДЩИНІ В. О. СУХОМЛИНСЬКОГО: ЕТНОПЕДАГОГІЧНІ ЗАСАДИ*
- Вакало Р.Ю.** 530  
*ФОРМУВАННЯ ПРОЄКТНОЇ КОМПЕТЕНТНОСТІ В МАЙБУТНІХ ФАХІВЦІВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ*
- Гораш К.В., Боднар А.М.** 537  
*ІННОВАЦІЙНЕ ОСВІТНЄ СЕРЕДОВИЩЕ ЗАКЛАДУ ВИЩОЇ ОСВІТИ ЯК СИСТЕМА ПІДГОТОВКИ СТУДЕНТІВ ДО НАВЧАННЯ ВПРОДОВЖ ЖИТТЯ*
- Гордєєва-Ковальчук Т.О., Костенко Л.В., Ороновський А.І., Цмур І.І.** 551  
*РОЛЬ ТЕХНОЛОГІЙ У СУЧАСНІЙ ДИРИГЕНТСЬКІЙ ПІДГОТОВЦІ МАГІСТРІВ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ*
- Горнар І.І.** 562  
*ВЗАЄМОЗВ'ЯЗОК АКТИВНОСТІ ТА ПРОФЕСІЙНОЇ САМОРЕАЛІЗАЦІЇ МАЙБУТНЬОГО ВИКЛАДАЧА*
- Грунник С.А.** 570  
*СУЧАСНИЙ УРОК МАТЕМАТИКИ В НУШ*
- Гужанова Т.С., Левик І.М.** 579  
*ЛЕПБУК ЯК ЕФЕКТИВНИЙ ЗАСІБ ФОРМУВАННЯ ЕКОЛОГІЧНИХ ЗНАТЬ У ДІТЕЙ ДОШКІЛЬНОГО ВІКУ*
- Дворська А.О.** 588  
*МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ФОРМУВАННЯ ГРОМАДЯНСЬКОЇ КУЛЬТУРИ МАЙБУТНІХ ФАХІВЦІВ АВІАЦІЙНОЇ ГАЛУЗІ*
- Дербак О.А., Печерна К.Ю., Яковлева Т.І.** 602  
*ВИКОРИСТАННЯ ОНЛАЙН ПЛАТФОРМ QUIZLET, WORDWALL ТА КАНОТ ПІД ЧАС ВИКЛАДАННЯ АНГЛІЙСЬКОЇ МОВИ ОНЛАЙН ДЛЯ МАЙБУТНІХ ПСИХОЛОГІВ*
- Дзюба П.М., Башнянин О.В.** 614  
*ЗАСТОСУВАННЯ ІНТЕРАКТИВНИХ МЕТОДІВ НАВЧАННЯ ПРИ ВИВЧЕНІ ДИСЦИПЛІНИ «ОСНОВИ БОЙОВОГО ЗАБЕЗПЕЧЕННЯ» В ПРОЦЕСІ ПІДГОТОВКИ МАЙБУТНІХ ОФІЦЕРІВ-ПРИКОРДОННИКІВ В УМОВАХ ВІЙНИ*

- Дзюбенко І.А., Бялик О.В.** 625  
*ДЕМОКРАТИЧНИЙ ШКІЛЬНИЙ КЛІМАТ ЛІЦЕЮ ЯК ЗАПОРУКА  
ФОРМУВАННЯ ГРОМАДЯНСЬКОСТІ УЧНІВСЬКОЇ МОЛОДІ*
- Добров В.Я.** 638  
*СТУДЕНТОЦЕНТРИЗМ ЯК ІННОВАЦІЯ ТА КОНЦЕПТУАЛЬНА ОСНОВА  
СУЧАСНОЇ ЄВРОПЕЙСЬКОЇ ПОЛІТИКИ У СФЕРІ ВИЩОЇ ОСВІТИ*
- Заболотний С.М., Тушко К.Ю., Тушко Д.А.** 651  
*ДО ПРОБЛЕМИ ФОРМУВАННЯ ПРОФЕСІЙНОЇ РЕФЛЕКСІЇ ФАХІВЦІВ  
СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ*
- Карп Р.В.** 660  
*ОСНОВНІ ПРОБЛЕМИ ІНТЕРНАЦІОНАЛІЗАЦІЇ СИСТЕМИ ВИЩОЇ  
ОСВІТИ: АКАДЕМІЧНА МОБІЛЬНІСТЬ СТУДЕНТІВ*
- Кравченко Т.В.** 668  
*ІННОВАЦІЙНІ МЕТОДИКИ ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ ТА  
ДОПОВНЕНОЇ РЕАЛЬНОСТІ В ПІДГОТОВЦІ МАЙБУТНІХ ПЕДАГОГІВ*
- Медведєва М.О., Ковальов Л.Є., Побережець І.І.** 680  
*АНАЛІЗ МОЖЛИВОСТЕЙ БІБЛІОТЕК RUTNOM ПРИ ВИВЧЕНІ КУРСУ  
«МАТЕМАТИЧНЕ ПРОГРАМУВАННЯ»*
- Мотрук В.Г.** 690  
*ФОРМУВАННЯ ЛІНГВОКУЛЬТУРНОЇ КОМПЕТЕНТНОСТІ В МАЙБУТНІХ  
ФАХІВЦІВ ЕКОНОМІЧНОГО ПРОФІЛЮ*
- Ніколаєску І.О., Михальчук О.О., Нікітська Ю.М.** 698  
*МЕТОДИЧНИЙ ПОТЕНЦІАЛ ВІРТУАЛЬНИХ ЕКСКУРСІЙ ЯК  
ІННОВАЦІЙНОГО ЗАСОБУ НАВЧАННЯ СЛАБОЗОРИХ ДІТЕЙ*
- Семко Л.В.** 710  
*ОСОБЛИВОСТІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ІНСТРУМЕНТАЛІСТІВ-  
ВИКОНАВЦІВ У КОНТЕКСТІ ФІЗІОЛОГІЧНОЇ, ІНТЕЛЕКТУАЛЬНОЇ І  
ПСИХОЕМОЦІЙНОЇ СКЛАДОВИХ*
- Тушко К.Ю., Ковальська І.Е., Гапоненко Н.П., Кульчицький О.М.** 721  
*ДИДАКТИЧНІ АСПЕКТИ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ДО  
МІЖКУЛЬТУРНОЇ КОМУНІКАЦІЇ*
- Цапко А.М., Білецька С.А., Ковтун А.В.** 731  
*ТРАНСФОРМАЦІЯ СИСТЕМИ ОСВІТИ В УМОВАХ ШТУЧНОГО  
ІНТЕЛЕКТУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ*

**Шевчук Л.Д., Бобовський Р.П., Солопко І.О., Овсієнко Ю.І.** 744  
*ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ НАВЧАННЯ МАТЕМАТИКИ  
В ЗАКЛАДАХ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ: ПРОБЛЕМИ І  
ПЕРСПЕКТИВИ*

**Шеховцова В.І., Малькова І.А.** 760  
*ІНДИВІДУАЛЬНИЙ ПІДХІД ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО  
ВИБОРУ ЗАКЛАДУ ВИЩОЇ ОСВІТИ*

**Штефан Л.В.** 775  
*ПІДГОТОВКА МАЙБУТНІХ ПСИХОЛОГІВ У КОНТЕКСТІ ВИКЛИКІВ  
СЬОГОДЕННЯ*

**Яцюта М.С.** 785  
*СУЧАСНІ ЦІННОСТІ ЯКІ НАБУВАЮТЬ ПІДЛІТКИ У ПРОЦЕСІ  
НАВЧАННЯ В ЗАКЛАДАХ СЕРЕДНЬОЇ ОСВІТИ. ВПЛИВ НА ПІДЛІТКІВ  
ПРОПАГАНДИ ТА ПРОТИДІЯ ЇЙ*

### **СЕРІЯ «Техніка»**

**Burda Yu.O., Pivnenko Yu.O., Cherednik A.D., Svyntarenko M.S.** 794  
*MODELING OF MODERN TECHNOLOGICAL FEATURES OF  
THERMODYNAMIC ANALYSIS OF GAS CLEANING SYSTEMS*

**Dzhoha O.V.** 802  
*ENVIRONMENTAL CHARACTERISTICS OF HUMAN LIFE ACTIVITIES*

**Furtat I.E., Furtat Yu.O.** 815  
*KINETICS OF NON-ISOTHERMAL ADSORPTION FROM LIMITED VOLUME*

**Havrysh B.M., Logoyda M.M., Kustra N.O.** 823  
*DIGITAL PRINTING AS AN INTEGRAL PART OF MULTI-CHANNEL  
COMMUNICATION*

**Krasnyuk M.T., Elishys D.O.** 833  
*PERSPECTIVES AND PROBLEMS OF BIG DATA ANALYSIS & ANALYTICS  
FOR EFFECTIVE MARKETING OF TOURISM INDUSTRY*

**Shkvarnytska T.Yu., Yehorov S.V., Kataiev D.A., Kataieva M.O.,  
Molchanova K.V.** 858  
*SYNTHESIS OF ANALOG MATCHED FILTERS FOR SIGNALS OF DIFFERENT  
DURATIONS*

**Бондаренко Т.В., Шкітов А.А., Шаповал В.М., Шевага В.В., Нещерет І.Г., Цикало Ю.Г., Кузнецов В.М., Чайка Є.І., Гоменюк В.М., Поліщук С.А., Підкова О.І., Лазута Р.Р.** **871**

*МОБІЛЬНІ ОСОБЛИВОСТІ КІБЕРБЕЗПЕКИ ЩОДО ШТУЧНОГО ІНТЕЛЕКТУ У ПОВОЄННІЙ УКРАЇНІ: ВИКЛИКИ ТА СТРАТЕГІЇ*

**Гарбич-Мошора О.Р., Столярчук І.Д., Лешко Р.Я., Британ В.Б., Гольський В.Б., Біліонюк Я.Г.** **882**

*РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ ДЛЯ ТРЕКІНГУ ТА КОНТРОЛЮ РОБОТИ НАД ЗАВДАННЯМИ*

**Гладка Ю.А., Галіцин В.Є.** **894**

*ПРОТИДІЯ ВИКОРИСТАННЮ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК РІЗНОВИДУ КІБЕРАТАК*

**Горбатенко А.А.** **909**

*ПІДХОДИ ДО ЗНИЖЕННЯ ПРИРОДНОГО ШУМУ В ГРУПОВИХ РЕКОМЕНДАЦІЙНИХ СИСТЕМАХ*

**Драглюк Ю.Ю., Драглюк О.В., Коваленко І.Г., Пилипчук Ю.В., Краснобокий А.В., Зінченко М.О., Яковчук О.В., Лазута Р.Р., Макаруч В.І.** **923**

*ОБІРУНТУВАННЯ ШЛЯХІВ СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ЕКСТРЕНОЇ ЕВАКУАЦІЇ ПОРАНЕНИХ ТА МЕДИЧНОГО ЗАБЕЗПЕЧЕННЯ У ЗОНІ ПРОВЕДЕННЯ БОЙОВИХ ДІЙ*

**Драглюк Ю.Ю., Скрипніков М.С., Гонга С.А., Коваленко І.Г., Пилипчук Ю.В., Краснобокий А.В., Панкратова А.А., Зінченко М.О., Яковчук О.В., Лазута Р.Р.** **933**

*СИСТЕМА УПРАВЛІННЯ ЕКСТРЕНОЮ ЕВАКУАЦІЄЮ ПОРАНЕНИХ ТА МЕДИЧНОГО ЗАБЕЗПЕЧЕННЯ У ЗОНІ ПРОВЕДЕННЯ БОЙОВИХ ДІЙ, СУЧАСНИЙ СТАН ТА ШЛЯХИ УДОСКОНАЛЕННЯ*

**Дубук В.І., Ковівчак Я.В., Царів О.І.** **943**

*РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ОРЕНДОЮ НЕРУХОМОГО МАЙНА*

**Івахненко Є.І., Скоробогата М.В., Огренич Є.В.** **959**

*ОСОБЛИВОСТІ ПРАКТИКИ ВИКЛАДАННЯ НАУКОВО-ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ В УМОВАХ ПІДГОТОВКИ ЗДОБУВАЧІВ ІНЖЕНЕРНИХ СПЕЦІАЛЬНОСТЕЙ*

**Коваль О.Є., Загородніх В.В., Коваленко І.Г., Штонда Р.М., Черниш Ю.О.,  
Прис Г.П., Зінченко М.О., Яковчук О.В., Лазута Р.Р., Бондаренко Л.О.,  
Руденко В.І.** 971

*ДОСЛІДЖЕННЯ ПИТАНЬ ВПРОВАДЖЕННЯ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ  
ПРИСТРОЇВ (EDR ТА XDR) В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ  
СИСТЕМАХ ЗБРОЙНИХ СИЛ УКРАЇНИ*

**Коваль О.Є., Коваленко І.Г., Нещерет І.Г., Терещенко Т.П., Прис Г.П.,  
Зінченко М.О., Яковчук О.В., Лазута Р.Р., Бондаренко Л.О., Руденко В.І.,  
Строкоус А.О.** 981

*РОЛЬ ТА МІСЦЕ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ (EDR ТА XDR)  
В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ЗБРОЙНИХ СИЛ  
УКРАЇНИ*

**Ковальчук Є.Я., Козловський С.Й.** 992

*ОСОБЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ  
ПРИЙНЯТТЯ РІШЕНЬ НА БАЗІ БЛОКЧЕЙН І ВЕЛИКИХ ДАНИХ*

**Корнієнко О.Б., Скоробогата М.В., Бовкун С.А.** 1005

*РОЗВИТОК ПРОФЕСІЙНИХ НАВИЧОК ЧЕРЕЗ ПРАКТИЧНІ ЗАНЯТТЯ З  
КРЕСЛЕННЯ ТА ІНЖЕНЕРНОЇ ГРАФІКИ*

**Костюк Ю.В., Войткевич А.А.** 1017

*ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ВІЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ  
ПОРУШНИКІВ ДЛЯ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ*

**Костюк Ю.В., Кравченко Д.В.** 1033

*МЕТОДИ ЗАХИСТУ ДАНИХ НА ПІДПРИЄМСТВАХ СОЦІАЛЬНОЇ СФЕРИ*

**Костюк Ю.В., Криворучко О.В., Десятко А.М., Захаров Р.Г.** 1048

*РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У ЗАКЛАДІ  
ВИЩОЇ ОСВІТИ ІЗ ЗАСТОСУВАННЯМ ПРОЕКТНО-ОРІЄНТОВАНОГО ТА  
КОМПЕТЕНТІСНОГО ПІДХОДІВ*

**Костюк Ю.В., Шапран В.О.** 1069

*ТЕХНОЛОГІЇ ВІЯВЛЕННЯ АНОМАЛЬНИХ ПОДІЙ ТА СИГНАТУР В  
РЕАЛЬНОМУ ЧАСІ*

**Криворучко О.В., Гнатченко Д.Д., Костюк Ю.В., Лук'янець Б.Б.** 1085

*ІНФОРМАЦІЙНО-УПРАВЛЯЮЧІ СИСТЕМИ АВТОМАТИЗАЦІЇ БІЗНЕС-  
ПРОЦЕСІВ ПІДПРИЄМСТВА НА МОБІЛЬНИХ ПЛАТФОРМАХ*

**Кузьменко О.П., Скрипніков М.С., Гонта С.А., Коваленко І.Г., Зінченко М.О.,  
Яковчук О.В., Лазута Р.Р., Макарчук В.І., Міночкін А.І.** 1102

*ДОСЛІДЖЕННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ ДЛЯ  
ОРГАНІЗАЦІЇ МОБІЛЬНИХ МЕРЕЖ ДОСТУПУ ТА ПЕРЕДАЧІ ДАНИХ  
ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ*

- Лецишин М.М., Шпак О.І.** 1115  
*ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ОПТИМІЗАЦІЇ V2X КОМУНІКАЦІЇ В КОНТЕКСТІ РОЗВИТКУ АВТОНОМНОГО ТРАНСПОРТУ*
- Ліман В.В., Польова О.Л., Іванчук Я.В.** 1132  
*ОСНОВНІ ЕТАПИ СТВОРЕННЯ ВЕБ-САЙТУ ДЛЯ ГОТЕЛЬНОГО ПІДПРИЄМСТВА*
- Макушенко Т.В., Десятниченко О.В.** 1147  
*ЕВОЛЮЦІЯ ХЕШ-ТАБЛИЦЬ ТА ЇХ ВПЛИВ НА СУЧАСНЕ ПРОГРАМУВАННЯ*
- Мамон О.В., Мунтян Л.Я., Іваненко Р.О.** 1155  
*ТЕХНОЛОГІЧНІ Й СОЦІАЛЬНІ ВИКЛИКИ РОЗВИТКУ WEB 3.0: АНАЛІЗ ТА ПРОГНОЗИ*
- Мулеса О.Ю., Кикина Є.Б.** 1171  
*РОЗРОБКА МЕТОДУ НЕЧІТКОЇ КЛАСИФІКАЦІЇ ДЛЯ ВИБОРУ ОТРИМУВАЧІВ СОЦІАЛЬНИХ ПОСЛУГ*
- Павлова Н.Л., Перепічко М.Є.** 1182  
*КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ ОБРОБКИ ВАНТАЖІВ В МОРСЬКОМУ ПОРТУ*
- Потапова Н.А., Волонтир Л.О., Частоколенко І.П., Григоренко М.С.** 1192  
*МЕТОД ІНТЕРПОЛЯЦІЇ ДЛЯ ПРОГНОЗУВАННЯ МЕТРИК ВИКОРИСТАННЯ ХМАРНИХ ОБЧИСЛЕНЬ В СТАТИСТИЧНОМУ НАВЧАННІ*
- Романюк А.А.** 1206  
*СИСТЕМНА ІНТЕГРАЦІЯ ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМ: СУЧАСНІ ВИКЛИКИ ТА СТРАТЕГІЇ УСПІХУ*
- Сурков К.Ю., Ізвалов О.В., Книшук А.В., Сорокун С.В.** 1220  
*ОСНОВНІ КІБЕРЗАГРОЗИ В ПРОЦЕСІ РОЗРОБКИ ІНТЕРНЕТ-СТОРІНОК*
- Усок С.О., Заморський С.М., Левківський І.М., Коваленко І.Г., Ковальчук Б.П., Волошин В.В., Зінченко М.О., Яковчук О.В., Лазута Р.Р., Кокошинський В.В., Думітраш В.О.** 1229  
*ПІДХІД ДО УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СЛУЖБОВИХ ОСІБ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ ТА ЗБРОЙНИХ СИЛ УКРАЇНИ*

**Фісюк А.О., Стойчев М.І.**

*АНАЛІЗ МОЖЛИВОСТІ ЗАСТОСУВАННЯ ПОЗАШТАТНИХ РАДІОАМАТОРСЬКИХ АНТЕН ДЛЯ НАПРАВЛЕНОГО УКХ РАДІОЗВ'ЯЗКУ В ІНТЕРЕСАХ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ*

1239

**Хрущак С.В., Бойко О.Р., Терьохіна М.Ю.**

*БЕЗПЕКОВИЙ МОНІТОРИНГ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ EBRF*

1251

### ***СЕРІЯ « Фізико-математичні науки »***

**Британ В.Б., Ольшанецький А.І., Столярчук І.Д., Лешко Р.Я., Карпин Д.С.,  
Гарбич-Мошора О.Р.**

*РОЗРОБКА ВЕБ-ДОДАТКУ ДЛЯ ДИСТАНЦІЙНОГО НАВЧАННЯ*

1263



УДК 004.056

[https://doi.org/10.52058/2786-6025-2024-4\(32\)-1251-1262](https://doi.org/10.52058/2786-6025-2024-4(32)-1251-1262)

**Хрущак Сергій Вікторович** кандидат технічних наук, старший викладач кафедри комп'ютерних наук та економічної кібернетики, Вінницький національний аграрний університет вул. Сонячна, 3, м. Вінниця, 21012, тел.: (097) 947-33-50, <https://orcid.org/0009-0007-9452-4372>

**Бойко Олексій Романович** кандидат технічних наук, старший викладач кафедри комп'ютерних наук та економічної кібернетики, Вінницький національний аграрний університет вул. Сонячна, 3, м. Вінниця, 21012, тел.: (067) 366-68-11, <https://orcid.org/0009-0008-1135-6594>

**Терьохіна Мар'яна Юріївна** студентка кафедри комп'ютерних наук та економічної кібернетики, Вінницький національний аграрний університет, вул. Сонячна, 3, м. Вінниця, 21012, тел.: (096) 871-07-08, <https://orcid.org/0009-0001-2776-0929>

## БЕЗПЕКОВИЙ МОНІТОРИНГ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ eVRF

**Анотація.** У статті розглянуто використання систем, заснованих на технології eVRF для забезпечення безпекового моніторингу в інформаційних системах, а саме запобіганню використанню прихованих каналів передачі даних за допомогою ICMP трафіку. eVRF (розширений фільтр пакетів Берклі) – це сучасна технологія, що дозволяє безпечно виконувати код у віртуальній машині всередині ядра Linux чи завантаженим безпосередньо на мережеву карту й таким чином надає багато можливостей по розширенню ядра, без необхідності внесення змін у саме ядро. З часом ця технологія стала ключовою для побудови багатьох сучасних систем моніторингу подій ядра та мережі. Описано призначення та можливості технології eVRF, зокрема її використання для моніторингу події системи, включаючи мережевий трафік та системні виклики, для вчасного виявлення потенційних загроз.

Проведено аналіз методів початкового зараження систем основними найбільш вживаними фреймворками віддаленого керування та ботнетами і виділено шляхи покращення для їх виявлення. Основна увага у статті приділяється розробці механізму, який може виявляти і аналізувати ICMP пакети в реальному часі для визначення потенційних замаскованих каналів зараження мережі, не накладаючи значного навантаження на систему. Описано підхід до розробки та впровадження програми з використанням eVRF,

що забезпечує фільтрацію та обробку ICMP трафіку в мережі. Проведено тестування розробленої системи з використанням

Висвітлено можливі проблеми, які можуть виникнути під час реалізації системи моніторингу на основі eBPF та розглядаються можливі напрями подальших досліджень у цій галузі. Ця стаття може бути використана фахівцями з інформаційної безпеки та адміністраторами комп'ютерних мереж, які цікавляться використанням передових технологій для забезпечення безпеки даних та інформаційних систем.

**Ключові слова:** моніторинг, eBPF, інформаційні системи, виявлення загроз, кіберзахист, розширення ядра, ICMP.

**Khrushchak Sergii Victorovich** PhD, senior teacher of Computer Sciences and economical cybernetics, Vinnytsia National Agrarian University, 3 Sonyachna St., Vinnytsia, 21012, tel. (097) 947-33-50, <https://orcid.org/0009-0007-9452-4372>

**Boiko Oleksii Romanovich** PhD, senior teacher of Computer Sciences and economical cybernetics, Vinnytsia National Agrarian University, 3 Sonyachna St., Vinnytsia, 21012, tel. (067) 366-68-11, <https://orcid.org/0009-0008-1135-6594>

**Teryokhina Maryana Yuriivna** student of Computer Sciences and economical cybernetics, Vinnytsia National Agrarian University, 3 Sonyachna St., Vinnytsia, 21012, tel. (097) 947-33-50, <https://orcid.org/0009-0007-9452-4372>

## SECURE MONITORING OF INFORMATIONAL SYSTEMS USING EBPF

**Abstract.** The article discusses the use of a system based on eBPF technology to provide security monitoring in information systems, namely, preventing the use of closed data transmission channels using ICMP traffic. eBPF (Extended Berkeley Packet Filter) is a state-of-the-art technology that allows code to be safely maintained in a virtual machine inside the Linux kernel or loaded over a network card and thus provides many features for the extended kernel without having to make changes to the kernel itself. Over time, this technology has become key to building many modern kernel and network event monitoring systems. The capabilities of eBPF technology are described and assigned, including its use for event monitoring systems, including network traffic and system calls, for early detection of existing threats.

An analysis of the methods of initial infection of the system by the main most used remote control frameworks and botnets was carried out and ways of improvement for their implementation were removed. The main focus of the paper is to develop a mechanism that can detect and analyze ICMP packets in real-time to

identify detected masked network infection channels without imposing significant system load. An approach to the development and implementation of a program using eBPF, which provides filtering and processing of ICMP traffic in the network, is described. The developed system was tested using

Problems that may arise during the implementation of the eBPF-based monitoring system are identified, and opportunities for further research in this area are considered. This article can be used by information security professionals and computer network administrators who are interested in using advanced technologies to ensure the security of data and information systems.

**Keywords:** security monitoring, eBPF, informational systems, threat detection, cyber protection, kernel extensions, ICMP.

**Постановка проблеми.** Забезпечення безпеки інформаційних систем є надзвичайно важливим та складним завданням для організацій у різних галузях. З урахуванням постійно зростаючого рівня загроз та все більш складних кібератак стає критичним використання передових технологій, які пропонують надійні засоби раннього виявлення загроз та захисту від них. Однією з таких технологій, яка привернула значну увагу в останні роки, є eBPF (розширений фільтр пакетів Berkeley). Це технологія спочатку розроблена для фільтрації мережових пакетів у ядрі Linux, однак з часом вона перетворилась на універсальний інструмент для моніторингу будь-яких подій в ядрі системи в реальному часі. У цій статті досліджено можливості eBPF та їх застосування в сфері безпеки інформаційних систем на прикладі виявлення зловмисного ICMP трафіку.

**Аналіз останніх досліджень і публікацій.** eBPF є порівняно новою технологією, яка відкрила безліч можливостей для створення засобів моніторингу та безпеки, які мають кращу швидкодію, більше контекстної інформації та безпечніші в використанні, порівняно з існуючими на той час системами. Проблемою застосування технології eBPF займалися такі світові експерти, як Джонатан Корбет [1], Гійом Фурньєр [2], та провідних компаній, таких як Google, Datadog, Amazon. Серед українських дослідників використання eBPF для виявлення вірусів-вимагачів займалися Журавчак Д, Кійко Е., Дудикевич В. [3].

В даній статті розглянуто використання eBPF для виявлення та боротьби з методами зараження та підвищення привілеїв, які застосовуються в популярних CC (Command and conquer) системах та піднімається питання більш тісної інтеграції розроблених модулів з наявними системами безпекового моніторингу.

**Мета статті** – проаналізувати сучасні підходи до застосування технології eBPF для виявлення та боротьби з кіберзагрозами з використанням засобів прихованого віддаленого адміністрування та розробити модуль для їх

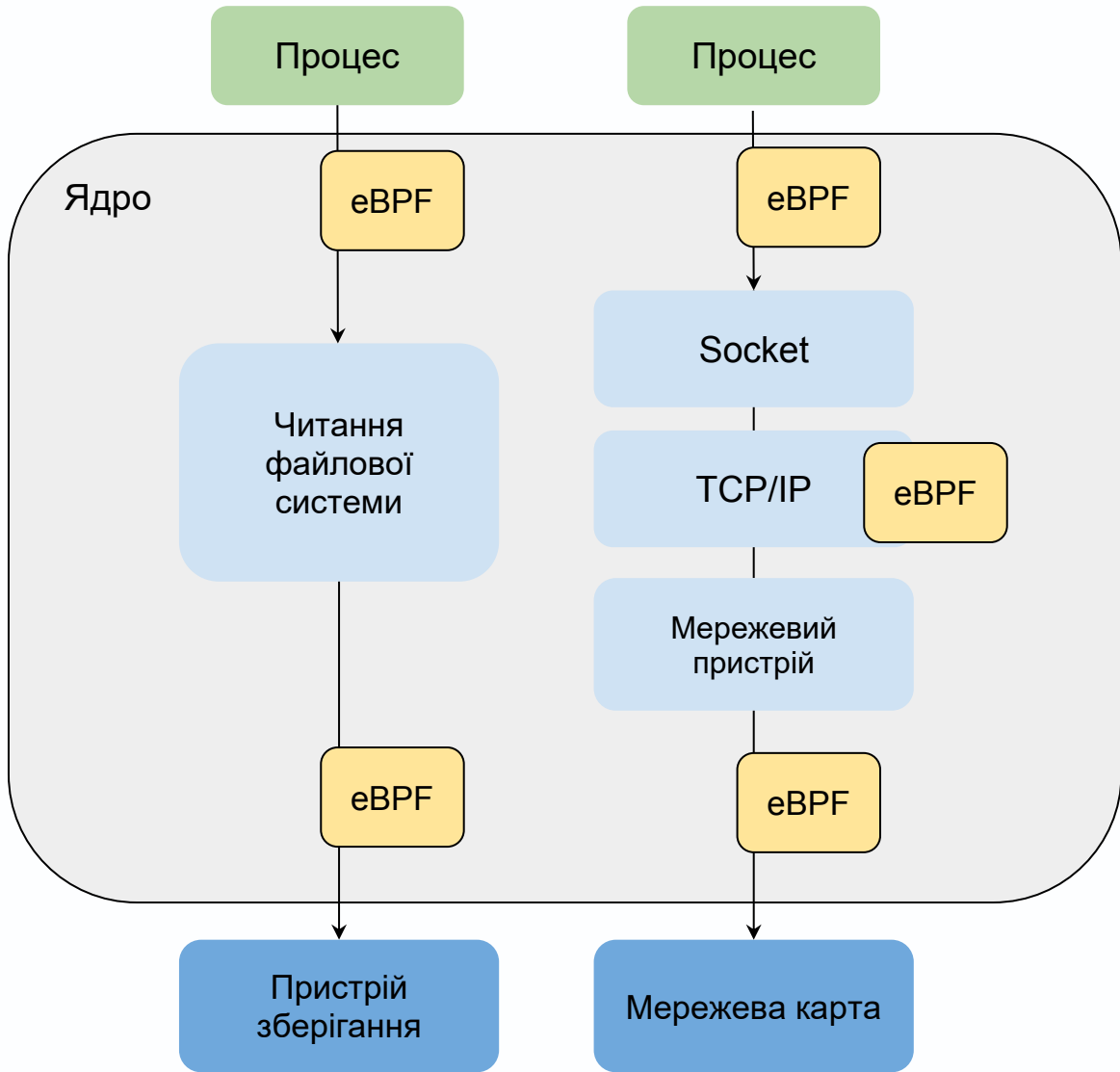
виявлення. Дослідити методи та проблеми інтеграції отриманого рішення з існуючими системами моніторингу.

**Виклад основного матеріалу.** eBPF (розширений фільтр пакетів Берклі) – це технологія ядра Linux, яка дозволяє динамічне та ефективно відстеження різноманітних подій системи, таких як мережеві пакети, виклики функцій та інші системні події. Ця технологія започаткована як розширення існуючої з 1992 року технології BPF (фільтр пакетів Берклі), яка використовувалась для обробки та фільтрації мережевих пакетів, однак її можливості зараз виходять далеко за рамки роботи з пакетами й дозволяють отримати доступ до будь-яких системних викликів, що відбуваються в ядрі Linux.

Однією з основних переваг eBPF є можливість динамічно завантажувати та вивантажувати програми, які виконуються в просторі ядра та отримують доступ до обмеженого набору його функцій без необхідності написання та підтримки модулів ядра, чи навіть його перезавантаження. Це значно прискорює інновації, оскільки будь-які зміни в самому ядрі системи це довгий процес що також несе багато потенційних безпекових ризиків, також саме ядро змінюється й тому вбудовані модулі потребують постійної підтримки. Саме тому останнім часом з'явилося багато систем, які використовують eBPF для моніторингу, телеметрії, відладки чи обробки мережевого трафіку, таких як Cilium, Falco, Pixie, Tetragon та інші. В основному це розробки в екосистемі Linux, часто інтегровані з існуючими популярними системами оркестрації контейнерів [2], однак також ведеться робота по інтеграції даної технології з ядром Windows [4].

Технологічно eBPF є віртуальною машиною, вбудованою в ядро системи, тобто eBPF програми виконуються в обмеженому оточенні всередині ядра. Перед виконанням програма проходить статичний аналізатор, який перевіряє, що програма є направленим ациклічним графом, виявляє потенційні проблеми та гарантує, що програма не коректно працюватиме для всіх станів та виконається за кінцевий проміжок часу. Так, наприклад, розмір стеку кожної програми eBPF не може перевищувати 512 кілобайт, та є обмеження на виконання циклів [5]. Хоча ці обмеження можуть здаватися дуже обмежувальними, саме вони є причиною популярності eBPF у засобах трасування та моніторингу. Вони забезпечують безпеку програми та знижують навантаження на систему. Самі програми eBPF можуть бути написані мовою, схожою на мову C з певними обмеженнями, і скомпільовані у байт-код, який може безпечно виконуватися в ядрі. Для виконання програм застосовується JIT (Just-in-Time) компілятор, який трансліює байт-код програм в машинні інструкції, отримуючи код по швидкодії близький до нативних програм. Крім того, eBPF має низькі накладні витрати, що означає, що його можна

використовувати в ситуаціях, де важливою є продуктивність системи [6, 7]. Програми eBPF, встановлені в контексті виконання в режимі ядра, можуть під'єднуватися до різних обробників викликів ядра і викликати різноманітні допоміжні API, надані програмним інтерфейсом eBPF (рис. 1).



**Рис.1.** Виклики ядра Linux, які можуть бути перехоплені в eBPF

Найбільш очевидним використанням eBPF є моніторинг і забезпечення безпеки мережі. Це зумовлено тим, що першопочатково BPF був доданий до ядра саме для фільтрації мережових пакетів. Однак eBPF також може бути використаний для забезпечення виконання політик безпеки шляхом блокування або модифікації певних системних подій на основі попередньо визначених правил. Це дозволяє забезпечувати дотримання внутрішніх політик безпеки та реагувати на потенційні загрози автоматично.

В нашому випадку дослідження фокусується на безпеці під час виконання програм, яка полягає в ранньому виявленні наперед заданих індикаторів, які можуть означати, що систему скомпроментовано. При спрацюванні індикаторів система або ж група реагування на інциденти може вчасно вжити контрзаходи та нівелювати загрозу. Зазвичай такі індикатори збирають як на рівні всієї мережі, це зазвичай моніторинг мережевого трафіку в критичних точках інфраструктури та виявлення аномальної мережевої активності чи відомих шкідливих сигнатур. Або ж системи для виявлення ненормальної поведінки процесів на рівні окремого хоста, як то доступ до системних API або підозрілих змін у використанні ресурсів. Інформація з усіх елементів мережі зазвичай збирається і обробляється централізованого на одному сервері чи кластері й такі системи називають системами виявлення вторгнень – IDS.

Основну увагу в дослідженні приділено саме протидії початковому зараженню відомими системами C2 (Command and Conquer). Це зазвичай готові фреймворки дозволяють атакуючим віддалено виконувати віддалені команди (RAT) на інфікованих машинах, стежити за їх станом, збирати необхідні дані як про машину так і мережу. Ці фреймворки відіграють важливу роль у координації і керуванні мережами інфікованих пристроїв, які часто називаються ботнетами. Згідно останніх досліджень Spamhouse найбільш популярними фреймворками для зараження систем та створення ботнетів серед досліджених 8438 заражень, наразі є Cobalt Strike, Qakbot, AsyncRAT, Sliver так інші [8]. Ці програми зазвичай мають складні механізми для уникнення виявлення і видалення антивірусними системами, які включають шифрування деяких компонентів, зміна та перекомпіляція вихідного коду під конкретні зараження та інше.

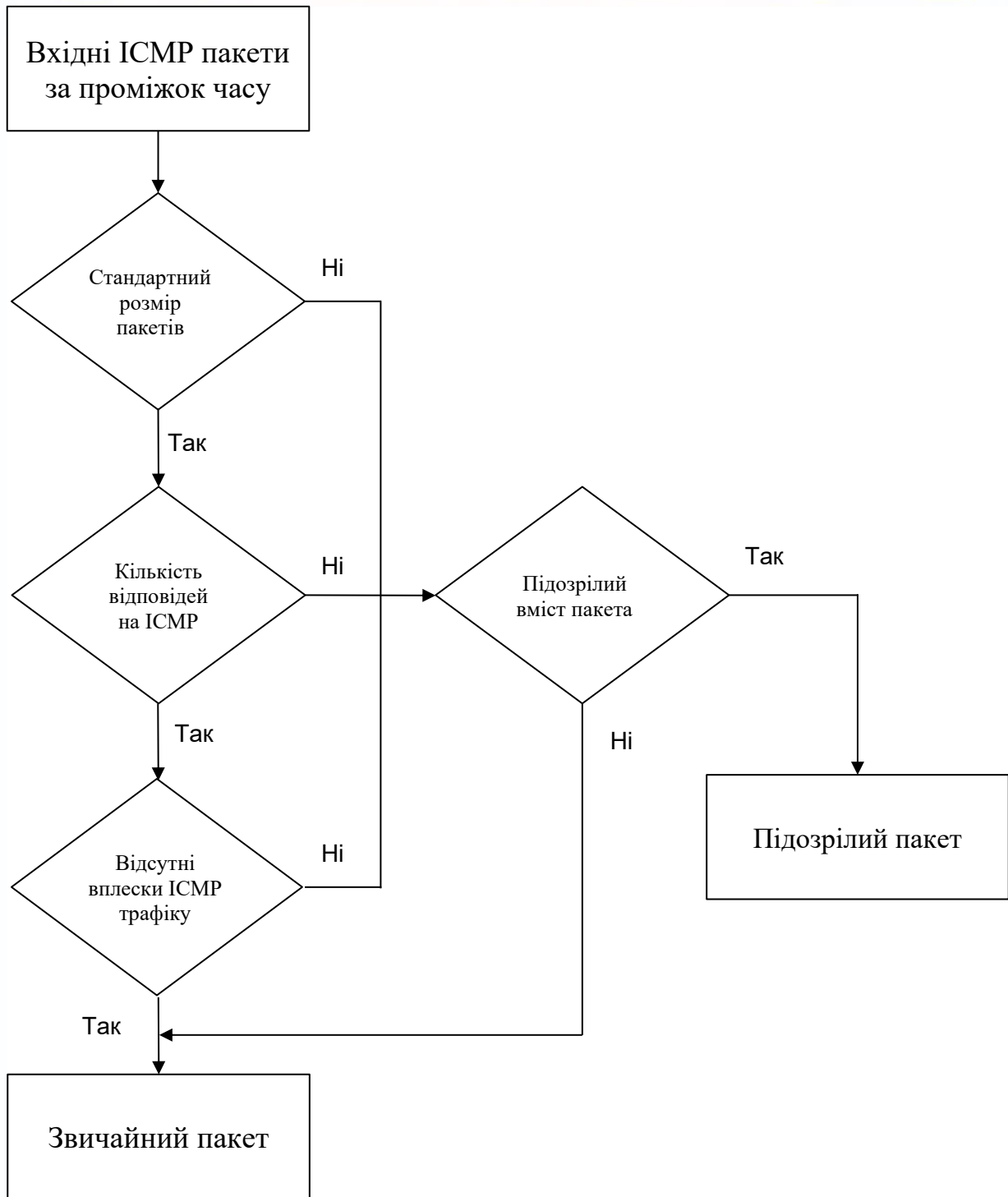
Для початкового зараження можуть використовуватись різні методики такі як фішинг, соціальна інженерія, макроси чи відомі вразливості в системах. Однак всі згадані системи відносяться до post-exploitation фреймворків, тобто спільною їх характеристикою є те, що вони поетапно розгортаються на вже початково інфікованих пристроях з використанням завантажувачів. Завантажувачі відіграють ключову роль в доставці та активації компонентів C2, оскільки самі компоненти зазвичай досить об'ємні та легше виявляються, щоб використовуватись на початкових етапах зараження. Зазвичай завантажувачі при початковому запуску одразу перевіряють наявність антивірусних систем, завантажують та налаштовують персистентність та запуск коду самого фреймворку. При цьому часто використовуються такі техніки як DLL-ін'єкції чи завантаження шкідливого коду в простір легітимного процесу системи (process hollowing) [9]. Зазвичай існуючі файрволи та IDS досить непогано виявляють роботу завантажувачів в мережі, що змушує зловмисників до застосування більш складних технік для запобігання виявленню шкідливого

трафіку, як наприклад використання нестандартних способів передачі трафіку для завантаження компонентів С2 [3].

Одним із таких способів, що робить виявлення складним є використання ICMP трафіку для завантаження тіла основного вірусу [10]. Такий підхід зазвичай дозволяє обійти правила файрволів, оскільки вони вважатимуть що це цілком легітимний трафік. Для виявлення та знешкодження таких завантажувачів необхідно проаналізувати вміст пакетів та виявити патерни, що вказуватимуть на те, що вони відносяться до зловмисних програм. Це якраз підпадає під основне застосування eVFP.

Для початку проведемо аналіз, як використання ICMP трафіку дозволяє непомітно передавати корисне навантаження. Протокол ICMP відноситься до мережевого рівня і в основному застосовується, як засіб передачі інформації про помилки та виключення при роботі протоколу IP, що дозволяє підтримувати стабільність та ефективність IP-мережі. Для передачі даних за допомогою ICMP може використовуватись підхід зі створення таємних каналів на основі ICMP Echo пакетів, які зазвичай використовуються командою ping [11]. Заборона таких прихованих каналів є складною задачею, оскільки зловмисні програми можуть використовувати як шифрування трафіку, для унеможливлення його виявлення так і вводити додаткові затримки в передачу, щоб зробити всплески трафіку менш помітними. До того ж існує багато легітимних ICMP запитів, які використовують великі ICMP пакети, тому навіть часткові обмеження ICMP трафіку можуть вплинути на функціональність всієї мережі.

Для реалізації системи виявлення шкідливого ICMP трафіку скористаємось методом, запропонованому в [12]. Для досягнення максимальної швидкодії даний метод застосовує поступовий підхід до аналізу пакетів, спочатку застосовуючи найпростіші перевірки й пакетів й переходячи до більш складних, якщо на ранніх етапах пакет було помічено як підозрілий. Основний алгоритм методу наведено на рис.2.



**Рис.2.** Блок схема алгоритму перевірки ICMP пакета

Для перевірки потоку ICMP пакетів застосовується алгоритм плаваючого вікна, яке розбиває неперервний потік пакетів на окремі набори елементів, обмежені розміром вікна. Для кожного вікна відбувається два етапи перевірки. Під час першого етапу перевіряється розмір поля даних ICMP



пакету, в більшості випадків його розмір має бути 32 байти для Windows машин та 56 байт для Linux. Наступна перевірка підраховує кількість відповідей до кожного ICMP echo запиту, яких зазвичай повинно бути не більше одного й останньою перевіркою є порівняння частоти ICMP запитів з заданим пороговим значенням. Якщо будь-яка з зазначених умов не виконується, алгоритм переходить до наступного етапу, який потребує більш складної перевірки вмісту пакету.

Другим етапом перевірки є аналіз вмісту пакетів. Зазвичай операційні системи використовують ICMP пакети, які відповідають певному шаблону специфічному для операційної системи. Однак щоб не зменшити час обробки пакету перевірка відповідності шаблону може відбуватись тільки для частини пакету.

Для реалізації eBPF програми обрано фреймворк bcc, який дозволяє інтегрувати eBPF підпрограму в основну програму написану на Python. eBPF, яка відбирає ICMP пакети, та передає тільки необхідні в підпрограму на Python виглядає наступним чином:

```
#include <linux/if_ether.h>
#include <linux/in.h>
#include <bcc/proto.h>

int icmp_tracer(struct __sk_buff *skbuff) {
    u8 *cursor = 0;
    struct ethernet_t *eth_packet = cursor_advance(cursor,
sizeof(*eth_packet));
    if (eth_packet->type != ETH_P_IP) return 0;
    struct ip_t *ip_packet = cursor_advance(cursor, sizeof(*ip_packet));
    if (ip_packet->nextp != IPPROTO_ICMP) return 0;
    struct icmp_t *icmp_packet = cursor_advance(cursor, sizeof(*icmp_packet));
    if (icmp_packet->type != 0 && icmp_packet->type != 43) return 0;
    return -1;
}
```

Підпрограма дозволяє відібрати тільки ICMP echo пакети й передати їх на статистичну обробку в Python. Результат функції визначає чи пакет буде передано на подальшу обробку чи буде відкинтий. Передача пакету між eBPF, що знаходиться в просторі ядра в користувацький простір відбувається через RAW-сокет та є повільним процесом, тому eBPF підпрограма повинна по можливості максимально відфільтровувати пакети й передавати в основну програму тільки ті, які дійсно вважаються підозрілими. Однак, на жаль, можливості віртуальної машини обмежені й наявні структури не дозволяють повністю реалізувати зазначений алгоритм, змушуючи переносити більшість коду в користувацький простір, що негативно впливає на швидкість перевірки.

В користувацькому просторі програма записує пакети разом з часом отримання в циклічний буфер, та опрацьовує їх відповідно до попередньо

наведеного алгоритму [12]. Поточна реалізація в разі детекції підозрілого трафіку виводить повідомлення в консоль, яке може бути перехоплено й відправлено в IDS.

Для перевірки реалізації було використано 2 віртуальних машини з Windows 10 та Ubuntu 22.04. Весь аналіз трафіку відбувався на Linux машині. Для генерації легітимного трафіку використовувалась стандартна утиліта `ping`, для генерації зловмисного трафіку використовувався модифікований код утиліти `ICMP-Shellcode-Loader`, в якій прибрано виконання завантаженої програми. Ця утиліта застосовується як основа для створення ICMP завантажувачів основного коду C2. В якості даних застосовувались генератор випадкових чисел та звичайні текстові файли. В лабораторних умовах системі вдалось повністю відрізнити зловмисний трафік від звичайного. Для більш точної оцінки необхідно покращувати маскування трафіку в застосованій утиліті. Результат спрацювання детектора при виявленні підозрілого трафіку можна побачити на рис. 3.

```
[bpf λ sudo ./packet-monitor.py  
Suspicious packet detected from IP 10.14.1.31  
Suspicious packet detected from IP 10.14.1.31  
Suspicious packet detected from IP 10.14.1.31  
Suspicious packet detected from IP 10.14.1.31  
Suspicious packet detected from IP 10.14.1.31  
Suspicious packet detected from IP 10.14.1.31
```

**Рис.3.** Результат детекції підозрілого ICMP трафіку

Загалом, розвиток eVRF відкриває широкі можливості для створення інноваційних та ефективних інструментів моніторингу, відстеження та забезпечення безпеки як для класичних, так і для сучасних контейнеризованих середовищ, а програмний інтерфейс дозволяє отримати інформацію, яка до цього була недоступна. Вбудований статичний аналізатор програм дозволяє виправити більшість складних помилок ще на етапі розробки. Однак інтерфейс містить й певні обмеження з якими довелося зіштовхнутись під час реалізації. Серед них обмежені можливості для зберігання даних між різними викликами eVRF підпрограми, нестабільний API, який може відрізнятись для різних версій ядер, що зумовлено стрімким розвитком технології, однак укладнює підтримку різних версій операційних систем. Також

**Висновки.** Технологія eVRF є потужним інструментом для забезпечення безпеки інформаційних систем. Вона надає можливість обробляти та аналізувати події ядра системи та мережі в реальному часі, з контекстною інформацією, що не була доступна до цього. Що дозволяє вчасно реагувати на потенційні загрози безпеки, порівняно з традиційними методами, як реалізація

модуль ядра, eBPF є ефективнішим та більш гнучким інструментом, який дозволяє розгортати нові заходи захисту та реагувати на кіберзагрози значно швидше. Описане рішення можна використовувати за основу для розробки більш комплексних систем визначення атак та для детекції інших варіантів прихованої передачі даних.

Подальшим напрямом досліджень може бути інтеграція eBPF програм з існуючими системами IDS, а також інтеграція існуючих eBPF рішень з Windows. Цікавим також є виявлення підозрілої активності окремих процесів, як то використання RAW сокетів чи певних системних викликів.

### *Література:*

1. Jonathan Corbet. Writing your own security module. <https://lwn.net/Articles/674949>, 2016.
2. Guillaume Fournier. Runtime Security Monitoring with eBPF. SSTIC, 2020.
3. Журавчак, Д. Використання EBPF для ідентифікації вірусів-вимагачів, що використовують DNS-запити DGA / Журавчак Даниїл, Кійко Едуард, Дудикевич Валерій // Information Technology and Security. – 2023. – Vol. 11, Iss. 2 (21). – Pp. 166–174
4. eBPF for Windows <https://microsoft.github.io/ebpf-for-windows/>
5. Marta Rybczyńska. Bounded loops in eBPF. <https://lwn.net/Articles/794934>, 2019.
6. Lorenzo Fontana and David Calavera. Linux Observability with BPF. November 2019.
7. eBPF Linux: How It Works, Use Cases & Best Practices URL: <https://www.aquasec.com/cloud-native-academy/devsecops/ebpf-linux/>
8. Spamhause Botnet Threat Update Q2 2023 <https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf>
9. Reviewing Qakbot loader sequences: <https://www.connectwise.com/blog/cybersecurity/reviewing-qakbot-loader-sequences-part-1>
10. Practical Insider Threat Penetration Testing Cases with Scapy <https://medium.com/swlh/practical-insider-threat-penetration-testing-cases-with-scapy-shell-code-and-protocol-evasion-e18d43d50da>
11. Covert Channel over ICMP <https://www.exploit-db.com/docs/english/18581-covert-channel-over-icmp.pdf>
12. Sirine Sayadi, Tarek Abbes, Adel Bouhoula. Detection of Covert Channels Over ICMP Protocol. 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Oct 2017, Hammamet, Tunisia. pp.1247-1252, 10.1109/AICCSA.2017.60. hal-02381398
13. Combining System Visibility and Security Using eBPF URL: <https://ceur-ws.org/Vol-2315/paper05.pdf>

### *References:*

1. Jonathan Corbet. Writing your own security module. <https://lwn.net/Articles/674949>, 2016.
2. Guillaume Fournier. Runtime Security Monitoring with eBPF. SSTIC, 2020.
3. Журавчак, Д. Використання EBPF для ідентифікації вірусів-вимагачів, що використовують DNS-запити DGA / Журавчак Даниїл, Кійко Едуард, Дудикевич Валерій // Information Technology and Security. – 2023. – Vol. 11, Iss. 2 (21). – Pp. 166–174
4. eBPF for Windows <https://microsoft.github.io/ebpf-for-windows/>
5. Marta Rybczyńska. Bounded loops in eBPF. <https://lwn.net/Articles/794934>, 2019.
6. Lorenzo Fontana and David Calavera. Linux Observability with BPF. November 2019.

7. eBPF Linux: How It Works, Use Cases & Best Practices URL: <https://www.aquasec.com/cloud-native-academy/devsecops/ebpf-linux/>
8. Spamhause Botnet Threat Update Q2 2023 <https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf>
9. Reviewing Qakbot loader sequences: <https://www.connectwise.com/blog/cybersecurity/reviewing-qakbot-loader-sequences-part-1>
10. Practical Insider Threat Penetration Testing Cases with Scapy <https://medium.com/swlh/practical-insider-threat-penetration-testing-cases-with-scapy-shell-code-and-protocol-evasion-e18d43d50da>
11. Covert Channel over ICMP <https://www.exploit-db.com/docs/english/18581-covert-channel-over-icmp.pdf>
12. Sirine Sayadi, Tarek Abbas, Adel Bouhoula. Detection of Covert Channels Over ICMP Protocol. 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Oct 2017, Hammamet, Tunisia. pp.1247-1252, 10.1109/AICCSA.2017. 60. hal-02381398
13. Combining System Visibility and Security Using eBPF URL: <https://ceur-ws.org/Vol-2315/paper05.pdf>