КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1145
УДК 004.056.53:004.9:378.147

Кіцель Наталія Василівна
науковий співробітник відділу організації наукової діяльності
Кременчуцький льотний коледж
Харківського національного університету внутрішніх справ,Кременчук, Україна
ORCID:0000-0003-4414-7226
kitselnata@gmail.com

Борисенко Оксана Миколаївна
завідувач відділення практичного навчання
Кременчуцький льотний коледж
Харківського національного університету внутрішніх справ, Кременчук, Україна
ORCID ID: 0000-0002-7858-1349
o.borisenko.klk@gmail.com

РОЗРОБКА ЛАБОРАТОРНОГО ПРАКТИКУМУ З АНАЛІЗУ ТА ВИЯВЛЕННЯ ПРОГРАМ-ВИМАГАЧІВ ДЛЯ ОСВІТНІХ ПРОГРАМ З КІБЕРБЕЗПЕКИ

Анотація. У статті розглянуто проблему недостатнього рівня практичної підготовки здобувачів освіти у сфері кібербезпеки щодо аналізу та виявлення програм-вимагачів, які залишаються одним із найнебезпечніших та найдинамічніших видів шкідливого програмного забезпечення. Сучасні зразки ransomware характеризуються використанням складних механізмів шифрування, розгалуженої інфраструктури управління, вбудованих антианалізних функцій та здатністю обходити традиційні засоби захисту. У зв'язку з цим ефективна підготовка фахівців вимагає не лише теоретичних знань, а й сформованих практичних навичок роботи з інструментами статичного та динамічного аналізу, поведінкових методів виявлення загроз, побудови моделей класифікації шкідливої активності, застосування машинного та глибинного навчання, а також використання EDR- та SIEM-систем у контексті реальних кіберінцидентів. Метою дослідження є розроблення лабораторного практикуму, який забезпечує комплексне занурення здобувачів у процеси аналізу та виявлення програм-вимагачів і сприяє формуванню професійних компетентностей, необхідних для роботи у сфері кіберзахисту. У межах роботи обґрунтовано структуру та зміст лабораторних завдань, які охоплюють аналіз життєвого циклу ransomware-атак, дослідження поведінкових характеристик шкідливих процесів, роботу з тестовими вибірками та динамічними середовищами, побудову алгоритмів детектування на основі машинного навчання, формування та обробку датасетів, а також оцінювання точності та стійкості моделей виявлення. Запропонований практикум може бути інтегрований у навчальні дисципліни з кібербезпеки, цифрової криміналістики та аналізу шкідливого програмного забезпечення. Розроблений підхід сприяє удосконаленню професійної підготовки фахівців, підвищує рівень практичної складової освітнього процесу та створює умови для виконання студентських досліджень у сфері моделювання, аналізу та протидії сучасним кіберзагрозам. Результати роботи можуть бути використані в закладах вищої освіти, центрах підвищення кваліфікації та навчальних кіберполігонах для поглиблення практичних компетентностей майбутніх фахівців з кібербезпеки.

Ключові слова: програми-вимагачі; аналіз шкідливого ПЗ; виявлення загроз; машинне навчання; лабораторний практикум; кібербезпека; поведінковий аналіз; динамічний аналіз.

ВСТУП

Постановка проблеми. Зростання кількості та складності атак програм-вимагачів створює значні ризики для інформаційних систем та критичної інфраструктури. Сучасні зразки ransomware характеризуються високим рівнем автоматизації, застосуванням багатошарових технік шифрування, ускладненими антианалізними механізмами та здатністю обходити традиційні сигнатурні засоби захисту. У цих умовах особливої актуальності набуває підготовка фахівців, здатних аналізувати поведінкові ознаки шкідливих процесів, застосовувати методи статичного та динамічного аналізу, а також будувати моделі

виявлення на основі методів машинного навчання. Проте в освітніх програмах з кібербезпеки часто бракує практично орієнтованих лабораторних завдань, що дозволяли б студентам працювати з реальними даними, інструментами аналізу та середовищами моделювання загроз. Це зумовлює потребу у створенні структурованого лабораторного практикуму, спрямованого на формування компетентностей у сфері аналізу та виявлення програм-вимагачів.

Аналіз останніх досліджень і публікацій. Проблематика виявлення програм-вимагачів та їх дослідження в освітньому середовищі активно розвивається в останнє десятиліття, що зумовлено стрімким поширенням сімейств ransomware, зростанням складності їхніх механізмів прихованості та інтенсивністю атак на критичну інфраструктуру. У фундаментальних оглядових роботах з кібербезпеки, зокрема у [1, 3], підкреслюється, що сучасні підходи до протидії шкідливому ПЗ мають інтегрувати моделювання поведінки загроз, методи машинного навчання та інструменти аналізу шкідливого коду. Це створює підґрунтя для формування лабораторних практикумів, що поєднують теоретичні та практичні аспекти дослідження програм-вимагачів.

Ґрунтовний внесок у вивчення принципів функціонування ransomware зроблено в роботах, що висвітлюють їхню еволюцію, методи шифрування та механізми уникнення виявлення. Зокрема, автори [4, 6] деталізують найпоширеніші тактики приховування, включно з антиемуляційними та антианалізними механізмами, що значно ускладнюють створення ефективних засобів виявлення. Водночас у [7] наголошується, що традиційні сигнатурні підходи стають малоефективними через швидку модифікацію зразків шкідливого ПЗ, а тому освітні програми мають орієнтуватися на поведінкові та гібридні методології.

Дослідження, присвячені застосуванню машинного навчання, зокрема [7, 9], демонструють потенціал таких моделей у виявленні аномалій у файловій активності, операціях шифрування та мережевій поведінці. Проте автори також підкреслюють обмеження, серед яких недостатність репрезентативних датасетів і висока ймовірність хибнопозитивних спрацювань. Ці висновки є суттєвими при розробленні лабораторних матеріалів, що мають включати роботу з різними видами вибірок, інструментами балансування даних і методами оцінювання якості моделей.

Окрему групу становлять дослідження щодо методик зворотного інжинірингу та динамічного аналізу шкідливого ПЗ. У [9] описано приклади навчальних середовищ, що імітують безпечні лабораторії (malwarelabs) для роботи з реальними зразками. Наголошено на важливості побудови ізольованих віртуальних середовищ, де студенти можуть досліджувати ланцюги зараження, поведінку програм-вимагачів у системі, моделі шифрування та механізми поширення. Подібні рекомендації важливі при розробці практикуму, орієнтованого на майбутніх фахівців із кібербезпеки.

Суттєвою складовою сучасних досліджень є прикладні розробки щодо захисту корпоративних та критичних систем, зокрема методи оцінювання ризиків і реагування на інциденти. У роботі [9] акцентується увага на важливості моделювання сценаріїв атак та навчання фахівців на реалістичних прикладах. Це підкреслює актуальність створення комплексного лабораторного практикуму, який охоплює як технічні, так і організаційні аспекти протидії ransomware.

Таким чином, аналіз сучасної наукової літератури свідчить про наявність значного масиву досліджень, присвячених окремим технічним або методологічним аспектам виявлення та аналізу програм-вимагачів. Водночас питання інтеграції цих напрацювань у структуровані лабораторні комплекси для освітніх програм висвітлене недостатньо. Це формує наукову нішу для розробки системного, методично обґрунтованого практикуму, який поєднує сучасні підходи до дослідження, аналізу та виявлення ransomware і сприяє підготовці кваліфікованих фахівців з кібербезпеки.

Метою роботи є розроблення лабораторного практикуму з аналізу та виявлення програм-вимагачів для освітніх програм з кібербезпеки, який включає методичні рекомендації, приклади лабораторних робіт, опис необхідних інструментів та алгоритмів аналізу, а також практичні підходи до побудови моделей виявлення ransomware у навчальному процесі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Розробка лабораторного практикуму з аналізу та виявлення програм-вимагачів стала результатом комплексного дослідження сучасних тенденцій розвитку ransomware, методів їх детекції та актуальних освітніх підходів у сфері кібербезпеки. Аналіз наукових джерел показав, що ефективне навчання в цій галузі потребує поєднання інструментального, методичного та практично орієнтованого складників [1-7, 8, 10, 11]. На основі цих положень було сформовано структуру лабораторного практикуму, логіку його побудови та методичне забезпечення.

Формування структури та логіки побудови практикуму. Проєктування практикуму розпочалося з визначення концептуальних засад, серед яких ключове значення отримали:

– безпечний обіг шкідливих зразків;
– формування компетентностей з аналізу та виявлення ransomware;
– застосування сучасного інструментарію статичного, динамічного та поведінкового аналізу;
– включення моделей машинного навчання, цифрової криміналістики та аналізу сценаріїв атак [1-5, 8].

У результаті було побудовано структуру лабораторного практикуму, яка представлена на рис. 1. Вона охоплює всі етапи роботи з програмами-вимагачами – від первинного аналізу виконуваних файлів до криміналістичного відновлення артефактів після інциденту.

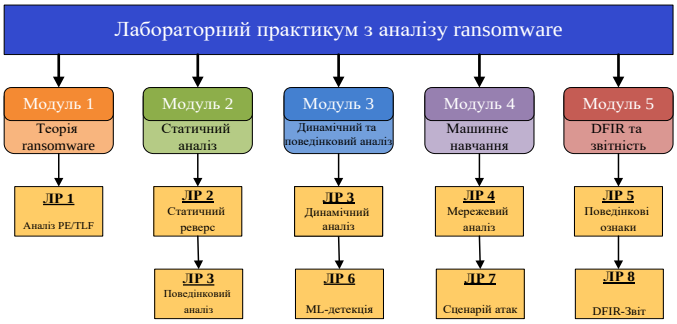

Рис. 1.Структура лабораторного практикуму з ransomware

Структура передбачає поступове ускладнення завдань, що відповідає принципам competency-basedlearning та забезпечує формування стійких практичних навичок, рекомендованих у сучасних дослідженнях [3, 5].

Методична побудова лабораторних робіт. Подальший етап роботи полягав у конкретизації навчальних цілей і визначенні переліку лабораторних робіт. В основу було покладено рекомендації досліджень щодо використання статичних та динамічних методів аналізу [1, 2, 4], а також поведінкових моделей і алгоритмів машинного навчання [3, 5, 8, 11].

До практикуму включено вісім лабораторних робіт:

1. ЛР1. Аналіз структури виконуваних файлів (PE/ELF) – ознайомлення з файловими форматами, виявлення підозрілих секцій, імпортів та рядків.
2. ЛР2. Статичний реверсинг – аналіз імпортів, рядків, ресурсів та пошук криптографічних компонентів.
3. ЛР3. Динамічний аналіз – вивчення поведінки шкідливої програми у контрольованому середовищі.
4. ЛР4. Аналіз мережевої активності – виявлення C2-з'єднань, TOR-комунікацій та аномальних DNS-запитів (зокрема, DGA, що підтверджується роботами [4, 6]).
5. ЛР5. Виявлення поведінкових ознак ransomware – визначення патернів шифрування, масового перейменування файлів, модифікації тіньових копій.
6. ЛР6. Побудова моделей машинного навчання – формування наборів ознак та оцінювання моделей (рекомендовано у [1-3, 8, 11]).
7. ЛР7. Моделювання шляху атаки (killchain) – дослідження сценаріїв проникнення й поширення.
8. ЛР8. Цифрова криміналістика – збір артефактів після атаки та підготовка звіту.

Кожна лабораторна робота містить покрокові методичні інструкції, необхідний перелік програмних засобів, вимоги до звітності та зразки команд, систематизовані у табл. 1. Це забезпечує єдність методичного підходу, спрощує роботу викладача і допомагає студентам працювати з інструментами без додаткових пояснень.

Таблиця 1

Методичні інструкції до лабораторних робіт

ЛР	Мета	Основні кроки виконання	Інструменти	Очікуваний результат
1	2	3	4	5
ЛР 1	Аналіз структури виконуваних файлів (PE/ELF)	1. Відкрити файл у PE-Studio або DetectItEasy. 2. Перевірити заголовки та секції на аномалії. 3. Переглянути імпорти та рядки на підозрілі елементи.	PE-Studio, DetectItEasy, Hex-редактор	Таблиця підозрілих ознак, перелік API, підозрілі рядки

Продовження таблиці 1

1	2	3	4	5
ЛР 2	Статичний реверс	1. Імпортувати файл у Ghidra/IDA. 2. Виконати автоматичний аналіз коду. 3. Виявити функції шифрування та ключові API-виклики.	Ghidra, IDA Free	Перелік функцій шифрування, алгоритм роботи шкідливого ПЗ
ЛР 3	Динамічний аналіз	1. Розгорнути VM із встановленою ОС. 2. Запустити зразок у ізольованому середовищі. 3. Відслідкувати зміни у файловій системі та процеси.	VirtualBox/VMware, Procmon, Process Explorer	Хронологія виконання зразка, зміни файлів/реєстру
ЛР 4	Аналіз мережевої активності	1. Захопити мережевий трафік у Wireshark. 2. Виявити підозрілі з'єднання та домени. 3. Проаналізувати пакети та протоколи.	Wireshark, NetworkMiner	Звіт із виявленими C2-з'єднаннями та аномаліями трафіку
ЛР 5	Виявлення поведінкових ознак ransomware	1. Аналіз логів і процесів на повторювані патерни. 2. Формування правил поведінки. 3. Перевірка правил на тестових даних.	Procmon, PowerShell, SIEM	Набір правил поведінкової детекції, протестовані сигнатури
ЛР 6	Побудова ML-моделі	1. Формування датасету ознак. 2. Навчання моделей RandomForest/SVM/LSTM. 3. Оцінка метрик (Accuracy, F1).	Python, scikit-learn, TensorFlow, Jupyter	Навчена модель з метриками ефективності
ЛР 7	Моделювання сценарію розповсюдження	1. Симуляція фішингової атаки або RDP-брутфорсу. 2. Фіксація подій і логів. 3. Побудова діаграми killchain.	PowerShell, EventViewer	Діаграма ланцюга атаки, рекомендації з hardening
ЛР 8	DFIR та підсумковий звіт	1. Створення знімку диска/пам'яті. 2. Витяг артефактів. 3. Підготовка звіту DFIR з доказовою базою.	Autopsy, FTK Imager	Аналітичний звіт із висновками та доказами

Інтеграція практикуму у навчальний процес. Особливу увагу приділено методиці впровадження практикуму в освітні програми з урахуванням сучасних вимог до підготовки фахівців з кібербезпеки. Практикум розглядається не як окремий елемент дисципліни, а як системоутворювальна складова, що поєднує теоретичні знання з практичними навичками та формує професійні компетентності. Впровадження здійснюється поетапно: від ознайомлення з базовими поняттями та інструментами до моделювання комплексних сценаріїв реагування на кіберінциденти. Такий підхід забезпечує поступове ускладнення матеріалу та сприяє формуванню стійких практичних умінь.

Розроблена схема передбачає поєднання:

– індивідуальних завдань, що спрямовані на формування навичок роботи з інструментами аналізу шкідливого програмного забезпечення, моніторингу мережевої активності, виявлення та локалізації загроз. На цьому етапі студенти виконують лабораторні роботи з чітко визначеними інструкціями, що дозволяє відпрацювати базові технічні прийоми, навчитися працювати з професійним програмним забезпеченням і документувати результати своєї діяльності;

– групових кейсів, орієнтованих на відтворення реальних інцидентів кібербезпеки. Студенти працюють у командах, розподіляючи ролі (аналітик, спеціаліст з реагування, експерт з цифрової криміналістики тощо), що сприяє розвитку навичок комунікації, координації дій та прийняття рішень в умовах обмеженого часу. Кейс-метод дозволяє моделювати повний цикл реагування на інцидент – від первинного виявлення до підготовки аналітичного звіту та рекомендацій щодо запобігання подібним атакам у майбутньому;

– дослідницьких елементів, зокрема аналізу нових зразків і трендів ransomware (з імітацією рекомендацій [5, 7, 10]). Цей компонент спрямований на розвиток критичного мислення, уміння працювати з відкритими джерелами інформації, проводити порівняльний аналіз та формулювати власні висновки. Студенти отримують завдання дослідити актуальні зразки шкідливого ПЗ, визначити їхні особливості, механізми поширення та вплив на інформаційні системи, а також запропонувати практичні заходи протидії.

Окремо передбачено інтеграцію результатів практикуму в систему оцінювання навчальних досягнень. Оцінювання здійснюється комплексно – з урахуванням технічної правильності виконання завдань, якості аналітичних висновків, рівня командної взаємодії та здатності аргументовано презентувати результати. Це стимулює студентів не лише до технічного виконання завдань, а й до глибшого осмислення отриманого досвіду.

Такий підхід дозволяє адаптувати практикум як для бакалаврського рівня (з акцентом на формування базових компетентностей), так і для підготовки магістрів (із розширенням дослідницької складової та елементів самостійного проєктування рішень), що підтверджується міжнародними дослідженнями з кібербезпекової освіти [3, 11]. У результаті забезпечується цілісна підготовка фахівців, здатних ефективно діяти в умовах реальних кіберзагроз та швидкої еволюції цифрового середовища.

Оцінювання результатів навчання. Для уніфікації оцінювання було розроблено систему критеріїв, узагальнену в табл. 2. Вона враховує:

– коректність аналізу статичних і поведінкових артефактів;
– точність застосування методів ML;
– здатність пояснювати отримані результати;
– оформлення звітності та дотримання методичних вимог.

Таблиця 2

Уніфікована схема оцінювання результатів навчання

ЛР	Критерій оцінювання	Максимум балів
ЛР1	Повнота аналізу секцій та імпортів	5
	Коректність пояснень підозрілих елементів	5
ЛР2	Ідентифікація функцій шифрування	10
ЛР3	Точність логування процесів	10
	Дотримання правил безпеки	5
ЛР4	Виявлення підозрілих мережевих з’єднань	10
	Якість аналізу пакетів	5
ЛР5	Побудова правил поведінкової детекції	10
	Тестування правил на наборі даних	5
ЛР6	Коректність підготовки датасету	5
	Якість навченої ML-моделі (F1, Accuracy)	10
ЛР7	Повнота ланцюга атаки (killchain)	10
	Якість рекомендацій	5
ЛР8	Якість артефактів у звіті	10
	Відповідність формату DFIR-звіту	5
	Максимальна оцінка:	120 балів

Такі критерії відповідають рекомендаціям сучасних робіт з оцінювання якості машинного навчання та цифрової криміналістики [1, 3, 5, 8, 11].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження розроблено методично обґрунтований лабораторний практикум з аналізу та виявлення програм-вимагачів, який може бути інтегрований в освітні програми з кібербезпеки. На основі сучасних підходів до статичного, динамічного та поведінкового аналізу ransomware сформовано структуру лабораторного комплексу, що передбачає використання безпечного віртуалізованого середовища, спеціалізованих інструментів дослідження шкідливого ПЗ та навчальних кейсів, наближених до реальних інцидентів.

Лабораторні роботи спрямовані на формування практичних навичок виявлення шкідливої активності, аналізу програмної структури, ідентифікації аномальних патернів і застосування моделей

машинного навчання для детекції програм-вимагачів. Доведено, що впровадження практикуму сприяє розвитку компетентностей у сфері інцидент-реагування, цифрової криміналістики та поведінкового аналізу шкідливого програмного забезпечення.

Запропонована методика підвищує ефективність практичної підготовки фахівців з кібербезпеки, інтегрує сучасні дослідницькі підходи в навчальний процес і створює основу для подальшого вдосконалення курсів з аналізу шкідливого ПЗ та протидії кіберзагрозам. Подальші дослідження доцільно спрямувати на розширення лабораторного комплексу шляхом інтеграції методів машинного та глибинного навчання для виявлення складних зразків ransomware і моделювання більш реалістичних сценаріїв кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alraizza, A., & Algarni, A. (2023). Ransomware detection using machine learning: A survey. *Big Data and Cognitive Computing, 7*(3), 143. https://doi.org/10.3390/bdcc7030143
2. Hussain, A., Saadia, A., Alhussein, M., Gul, A., & Aurangzeb, K. (2024). Enhancing ransomware defense: Deep learning-based detection and family-wise classification of evolving threats. *PeerJ Computer Science, 10*, e2546. https://doi.org/10.7717/peerj-cs.2546
3. Jawad, S., & Ahmed, H. M. (2024). Machine learning approaches to ransomware detection: A comprehensive review. *International Journal of Safety and Security Engineering, 14*(6), 1963-1973. https://doi.org/10.18280/ijsse.140630
4. Zhuravchak, D. (2024). Monitoring ransomware using extended Berkeley Packet Filter (eBPF) and machine learning. *Science-Based Technologies, 60*(4), 352-363. https://doi.org/10.18372/2310-5461.60.18029
5. Ispahany, J., Islam, M. R., Islam, M. Z., & Khan, M. A. (2024). Ransomware detection using machine learning: A review, research limitations and future directions. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3397921
6. Zhuravchak, D., Kiiko, E., & Dudykevych, V. (2023). Using eBPF to identify ransomware that uses DGA DNS queries. *Information Technology and Security, 11*(2), 166-174. https://doi.org/10.20535/2411-1031.2023.11.2.293760
7. Lysenko, S., Atamaniuk, O., Bokhonko, O., & Vorobiyov, V. (2023). Method for detection of ransomware cyber threats based on honeypot: State-of-the-art. *Herald of Khmelnytskyi National University. Technical Sciences, 317*(1),300-309. https://doi.org/10.31891/2307-5732-2023-317-1-300-309
8. Haponenko, O. I., Marchenko, V. V., & Gaidur, G. I. (2020). Advantages and disadvantages of honeypot traps for hackers. *Modern Information Security*. https://doi.org/10.31673/2409-7292.2020.025968
9. Zhuravchak, D., Dudykevych, V., & Tolkachova, A. (2023). Study of the structure of the system for detecting and preventing ransomware attacks based on endpoint detection and response. *Cybersecurity: Education, Science, Technique, 3*(19), 69-82. https://doi.org/10.28925/2663-4023.2023.19.6982
10. Rele, M., Samuel, J., Patil, D., & Krishnan, U. (2025). Exploring ransomware detection based on artificial intelligence and machine learning. *Procedia Computer Science, 252*, 548–556. https://doi.org/10.1016/j.procs.2025.01.014
11. Kritika, E. (2024). A comprehensive literature review on ransomware detection using deep learning. *Cyber Security and Applications*, 100078. https://doi.org/10.1016/j.csa.2024.100078

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Nataliia Kitsel
Researcher
Kremenchuk flight college Kharkiv National University of Internal Affairs, Kremenchuk, Ukraine
ORCID:0000-0003-4414-7226
kitselnata@gmail.com

Borysenko Oksana
Head of the Practical Training Department
Kremenchuk flight college Kharkiv National University of Internal Affairs, Kremenchuk, Ukraine
ORCID ID: 0000-0002-7858-1349
o.borisenko.klk@gmail.com

DEVELOPMENT OF A LABORATORY WORKSHOP ON ANALYSIS AND DETECTION OF RANKING PROGRAMS FOR CYBERSECURITY EDUCATIONAL PROGRAMS

Abstract. The article addresses the issue of insufficient practical training of cybersecurity students in analyzing and detecting ransomware, which remains one of the most dangerous and rapidly evolving types of malicious software. Modern ransomware samples employ advanced encryption mechanisms, extensive command-and-control infrastructures, built-in anti-analysis techniques, and capabilities for bypassing traditional security tools. Consequently, effective specialist training requires not only theoretical knowledge but also well-developed practical skills in using static and dynamic analysis tools, behavioral threat detection methods, models for classifying malicious activity, machine learning and deep learning techniques, as well as EDR and SIEM systems in the context of real cyber incidents. The purpose of the study is to develop a laboratory practicum that provides comprehensive immersion into the processes of ransomware analysis and detection, contributing to the formation of the professional competencies required in the field of cyber defense. The paper substantiates the structure and content of laboratory tasks covering the analysis of the ransomware attack lifecycle, investigation of behavioral characteristics of malicious processes, work with test datasets and dynamic environments, development of machine-learning-based detection algorithms, dataset creation and processing, and evaluation of model accuracy and robustness. The proposed practicum can be integrated into academic courses on cybersecurity, digital forensics, and malware analysis. The developed approach enhances the quality of professional training, strengthens the practical component of the educational process, and creates conditions for student research in modeling, analyzing, and countering modern cyber threats. The results may be applied in higher education institutions, professional training centers, and cyber ranges to deepen the practical competencies of future cybersecurity specialists.

Key words: ransomware; malware analysis; threat detection; machine learning; laboratory practicum; cybersecurity; behavioral analysis; dynamic analysis.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Alraizza, A., & Algarni, A. (2023). Ransomware detection using machine learning: A survey. *Big Data and Cognitive Computing, 7*(3), 143. https://doi.org/10.3390/bdcc7030143
2. Hussain, A., Saadia, A., Alhussein, M., Gul, A., & Aurangzeb, K. (2024). Enhancing ransomware defense: Deep learning-based detection and family-wise classification of evolving threats. *PeerJ Computer Science, 10*, e2546. https://doi.org/10.7717/peerj-cs.2546
3. Jawad, S., & Ahmed, H. M. (2024). Machine learning approaches to ransomware detection: A comprehensive review. *International Journal of Safety and Security Engineering, 14*(6), 1963-1973. https://doi.org/10.18280/ijsse.140630
4. Zhuravchak, D. (2024). Monitoring ransomware using extended Berkeley Packet Filter (eBPF) and machine learning. *Science-Based Technologies*, *60*(4), 352-363. https://doi.org/10.18372/2310-5461.60.18029
5. Ispahany, J., Islam, M. R., Islam, M. Z., & Khan, M. A. (2024). Ransomware detection using machine learning: A review, research limitations and future directions. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3397921

6. Zhuravchak, D., Kiiko, E., & Dudykevych, V. (2023). Using eBPF to identify ransomware that uses DGA DNS queries. *Information Technology and Security*, *11*(2), 166-174. https://doi.org/10.20535/2411-1031.2023.11.2.293760
7. Lysenko, S., Atamaniuk, O., Bokhonko, O., & Vorobiyov, V. (2023). Method for detection of ransomware cyber threats based on honeypot: State-of-the-art. *Herald of Khmelnytskyi National University. Technical Sciences, 317*(1),300-309. https://doi.org/10.31891/2307-5732-2023-317-1-300-309
8. Haponenko, O. I., Marchenko, V. V., & Gaidur, G. I. (2020). Advantages and disadvantages of honeypot traps for hackers. *Modern Information Security*. https://doi.org/10.31673/2409-7292.2020.025968
9. Zhuravchak, D., Dudykevych, V., & Tolkachova, A. (2023). Study of the structure of the system for detecting and preventing ransomware attacks based on endpoint detection and response. *Cybersecurity: Education, Science, Technique, 3*(19), 69-82. https://doi.org/10.28925/2663-4023.2023.19.6982
10. Rele, M., Samuel, J., Patil, D., & Krishnan, U. (2025). Exploring ransomware detection based on artificial intelligence and machine learning. *Procedia Computer Science*, *252*, 548–556. https://doi.org/10.1016/j.procs.2025.01.014
11. Kritika, E. (2024). A comprehensive literature review on ransomware detection using deep learning. *Cyber Security and Applications*, 100078. https://doi.org/10.1016/j.csa.2024.100078

Отримано редакцією журналу / Received: 22.02.26
Прорецензовано / Revised: 02.03.26
Схвалено до друку / Accepted: 25.06.26