МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Інна КОНДЮС
«29» серпня 2026 р.

ЗАТВЕРДЖУЮ
Перший проректор
_____ Надія КОВАЛЬЧУК
«29» серпня 2026 р.

СИЛАБУС

з освітнього компонента «Аналітик кібербезпеки»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра кібербезпеки

Силабус склав(ла) завідувач кафедри кібербезпеки, к.т.н., доцент Сергій КОСТЮЧКО

Силабус затверджений на засіданні кафедри кібербезпеки, протокол № 2 від «28» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Сергій КОСТЮЧКО

Розглянуто та схвалено групою забезпечення освітньої програми «Кібербезпека», протокол № 2 від «28» серпня 2026 р.

Гарант ОП «Кібербезпека» к.т.н., доцент Сергій КОСТЮЧКО

Схвалено науково-методичною радою університету, протокол № 1/а від «29» серпня 2026 р.

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/2315

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Аналітик кібербезпеки»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	12 Інформаційні технології / 125 Кібербезпека та захист інформації
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	5 кредитів ECTS / 150 годин, семестр 6
Форма контролю	екзамен
Викладач(і)	к.т.н., доцент Сергій КОСТЮЧКО

1. Мета і завдання дисципліни

Мета: Оволодіння основних концепцій безпеки інформації. Отримати навичок, необхідних для проведення моніторингу, виявлення, аналізу і нейтралізації загроз інформаційної безпеки.

Завдання: Поглиблення знань в області безпеки комп’ютерних мереж та систем. Предмет присвячений вивченню та засвоєнню сучасних технологій, які використовуються для організації кібербезпеки.

Пререквізити: Програмування та реверс-інжиніринг, Захист операційних систем, Аналіз великих даних, Системи моніторингу комп'ютерних систем та мереж

2. Компетентності

СК02 — Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК05 — Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК08 — Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

3. Структура дисципліни, розподіл годин, зв'язок тем з компетентностями

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
Змістовий модуль 1. Основи діяльності центру операцій безпеки (SOC) та захисту комп’ютерних мереж								
1	Тема 1. Основи безпеки SOC	2/–	2/0,5	6/10	10/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
2	Тема 2. Основи Windows та Linux	4/–	4/1	6/10	14/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
3	Тема 3. Мережеві протоколи та послуги	2/0,5	2/0,5	6/10	10/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
4	Тема 4. Інфраструктура комп'ютерних мереж	2/–	2/1	4/12	8/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
5	Тема 5. Принципи безпеки комп'ютерних мереж	2/0,5	2/0,5	6/12	10/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
Змістовий модуль 2. Виявлення кіберзагроз, моніторинг безпеки та реагування на інциденти								
6	Тема 6. Мережеві атаки	2/–	2/0,5	6/12	10/12,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
7	Тема 7. Захист комп'ютерних мереж	2/–	2/1	8/12	12/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
8	Тема 8. Криптографія	2/–	2/1	8/12	12/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
9	Тема 9. Безпека та аналіз кінцевих пристроїв	2/–	2/1	10/12	14/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
10	Тема 10. Моніторинг інформаційної безпеки	2/–	2/1	10/12	14/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
11	Тема 11. Аналіз даних про вторгнення	4/0,5	4/1	10/12	18/13,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
12	Тема 12. Обробка інцидентів	4/0,5	4/1	10/12	18/13,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08
	Разом	**30/2**	**30/10**	**90/138**	**150/150**			

Легенда: ЗК — загальна компетентність (номер за п. 2); СК — спеціальна (фахова) компетентність (номер за п. 2). Повне формулювання кожного коду наводиться в ОП / стандарті спеціальності.

Методи навчання: МН1 — словесний метод (лекція, дискусія, співбесіда тощо); МН2 — практичний метод (лабораторні та практичні заняття); МН3 — наочний метод (метод ілюстрацій і метод демонстрацій); МН4 — робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); МН5 — відеометод у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо).

Методи оцінювання: МО1 — екзамен; МО2 — усне або письмове опитування; МО4 — тестування; МО5 — командні проєкти.

4. Результати навчання

ПРН05. адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

ПРН14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

ПРН19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

ПРН22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

ПРН26. впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

ПРН27. вирішувати задачі захисту потоків даних в інформаційних, інформаційнотелекомунікаційних (автоматизованих) системах;

ПРН28. аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;

ПРН41. забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

ПРН42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

ПРН46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

ПРН47. вирішувати задачі захисту інформації, що обробляється в інформаційнотелекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

ПРН48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційнотелекомунікаційних системах;

5. Цілі сталого розвитку

ЦСР 8 – Гідна праця та економічне зростання

ЦСР 9 – Промисловість, інновації та інфраструктура

ЦСР 16 – Мир, справедливість та сильні інститути

6. Неформальна освіта

Рекомендовані курси, тренінги, стажування та інші: результати навчання, здобуті у формальній, неформальній чи інформальній освіті, можуть бути визнані відповідно до процедур ЛНТУ. Підтвердженнями можуть бути сертифікати тематичних тренінгів, вебінарів чи онлайн-курсів разом з описом досягнутих результатів навчання та, за потреби, коротке верифікаційне завдання або портфоліо.

7. Критерії та форми контролю

Оцінювання — за 100-бальною шкалою (національна шкала / ЄКТС). Підсумковий бал = поточний контроль (30 %) + модульний контроль (30 %) + екзамен (40 %).

Академічна доброчесність: самостійне виконання завдань; коректне посилання на джерела; позначення частин тексту, згенерованих засобами ШІ. Порушення академічної доброчесності не толеруються.

8. Зміст тем

Тема 1. Основи безпеки SOC

Поняття та призначення центру операцій безпеки (Security Operations Center, SOC). Основні завдання та функції SOC. Організаційна структура SOC. Ролі та обов’язки аналітиків SOC різних рівнів. Основні принципи інформаційної безпеки. Модель CIA (конфіденційність, цілісність, доступність). Поняття загроз, вразливостей і ризиків. Основні етапи виявлення та реагування на інциденти. Інструменти та технології SOC. Основи управління подіями інформаційної безпеки.

Тема 2. Основи Windows та Linux

Архітектура операційних систем Windows і Linux. Основні компоненти операційних систем. Файлові системи та структура каталогів. Облікові записи користувачів і групи. Управління правами доступу. Робота з командним рядком Windows та оболонкою Bash у Linux. Основні системні команди. Управління процесами та службами. Налаштування мережевих параметрів. Журнали системних подій. Основи адміністрування та забезпечення безпеки операційних систем.

Тема 3. Мережеві протоколи та послуги

Моделі OSI та TCP/IP. Основні принципи передавання даних у комп’ютерних мережах. Протоколи Ethernet, IP, TCP, UDP, ICMP та ARP. IP-адресація та підмережі. Принципи маршрутизації. Мережеві порти та сокети. Протоколи прикладного рівня DNS, DHCP, HTTP, HTTPS, FTP, SSH та SMTP. Принципи функціонування мережевих служб. Засоби аналізу мережевого трафіку. Основи діагностики мережевих з’єднань.

Тема 4. Інфраструктура комп’ютерних мереж

Поняття та компоненти мережевої інфраструктури. Фізична і логічна топології мереж. Активне та пасивне мережеве обладнання. Комутатори, маршрутизатори, міжмережеві екрани та точки бездротового доступу. Локальні та глобальні мережі. Віртуальні локальні мережі (VLAN). Принципи сегментації мережі. Мережі DMZ. Основи віртуалізації мережевої інфраструктури. Хмарні мережеві середовища. Принципи забезпечення відмовостійкості та доступності мережевих ресурсів.

Тема 5. Принципи безпеки комп’ютерних мереж

Основні загрози безпеці комп’ютерних мереж. Політики та механізми мережевої безпеки. Принцип мінімальних привілеїв. Багаторівневий захист (Defense in Depth). Модель нульової довіри (Zero Trust). Автентифікація, авторизація та облік дій користувачів (AAA). Контроль доступу до мережевих ресурсів. Захист мережевого периметра. Основи безпечного налаштування

мережевих пристроїв. Управління вразливостями. Оцінювання ризиків інформаційної безпеки.

Тема 6. Мережеві атаки

Класифікація мережевих атак. Основні етапи реалізації кібератак. Розвідка та сканування мережевої інфраструктури. Атаки типу DoS та DDoS. Атаки Man-in-the-Middle (MITM). ARP Spoofing та DNS Spoofing. Атаки на мережеві служби та протоколи. Перехоплення мережевого трафіку. Атаки на автентифікацію. Шкідливе програмне забезпечення та його поширення мережею. Модель Cyber Kill Chain. Тактики й техніки зловмисників за MITRE ATT&CK. Основні індикатори компрометації (IoC).

Тема 7. Захист комп'ютерних мереж

Методи та засоби захисту мережевої інфраструктури. Міжмережеві екрани (Firewall) та їх класифікація. Системи виявлення та запобігання вторгненням (IDS/IPS). Основи налаштування правил фільтрації трафіку. Списки контролю доступу (ACL). Сегментація мережі та ізоляція критичних ресурсів. Захищені віртуальні приватні мережі (VPN). Технології захисту бездротових мереж. Захист DNS та інших мережевих служб. Управління оновленнями та вразливостями. Перевірка ефективності мережевих засобів захисту.

Тема 8. Криптографія

Основні поняття криптографічного захисту інформації. Симетричне та асиметричне шифрування. Криптографічні алгоритми AES та RSA. Криптографічні хеш-функції. Алгоритми SHA-2 та SHA-3. Цифрові підписи. Інфраструктура відкритих ключів (PKI). Цифрові сертифікати X.509. Протоколи TLS та IPsec. Захищені канали передавання даних. Управління криптографічними ключами. Використання криптографічних механізмів для забезпечення конфіденційності, цілісності та автентичності інформації.

Тема 9. Безпека та аналіз кінцевих пристроїв

Поняття кінцевого пристрою (Endpoint). Основні загрози безпеці робочих станцій і серверів. Захист операційних систем Windows та Linux. Антивірусні системи та засоби Endpoint Protection Platform (EPP). Системи виявлення та реагування на загрози кінцевих пристроїв (EDR). Моніторинг процесів, служб і мережевих з'єднань. Аналіз системних журналів Windows Event Log та Linux Syslog. Використання Sysmon для контролю подій Windows. Виявлення підозрілої активності. Аналіз механізмів закріплення шкідливого програмного забезпечення. Основи цифрової криміналістики кінцевих пристроїв.

Тема 10. Моніторинг інформаційної безпеки

Поняття та завдання моніторингу інформаційної безпеки. Джерела даних для моніторингу. Централізоване збирання та оброблення журналів подій. Архітектура систем управління інформацією та подіями безпеки (SIEM). Принципи роботи SIEM-систем. Основи використання Wazuh, Splunk та Elastic Security. Нормалізація та кореляція подій. Налаштування правил виявлення загроз. Моніторинг мережевої активності. Формування сповіщень про інциденти. Інформаційні панелі (Dashboard) та візуалізація подій безпеки. Визначення ключових показників ефективності моніторингу.

Тема 11. Аналіз даних про вторгнення

Основні джерела інформації про вторгнення. Аналіз мережевого трафіку та пакетів даних. Використання Wireshark для дослідження мережевої активності. Аналіз журналів мережевих пристроїв і серверів. Виявлення аномалій та підозрілих подій. Аналіз індикаторів компрометації (IoC) та індикаторів атак (IoA). Кореляція подій з різних джерел. Використання MITRE ATT&CK для класифікації виявлених загроз. Основи Threat Intelligence. Виявлення хибнопозитивних і хибнонегативних спрацювань. Формування висновків за результатами аналізу вторгнень.

Тема 12. Обробка інцидентів

Поняття інциденту інформаційної безпеки. Класифікація та визначення критичності інцидентів. Життєвий цикл реагування на інциденти. Основні положення NIST SP 800-61. Підготовка до реагування. Виявлення, аналіз та підтвердження інцидентів. Локалізація загроз. Усунення наслідків компрометації. Відновлення працездатності інформаційних систем. Збереження

цифрових доказів. Документування інцидентів. Формування звітів SOC-аналітика. Процедури ескалації інцидентів. Використання сценаріїв реагування (Playbooks). Основи автоматизації реагування за допомогою SOAR. Аналіз причин інцидентів та розроблення заходів запобігання їх повторенню.

9. Опис ІЗ/КПІЗ

Не передбачено навчальним планом.

10. Загальні вимоги

Освітній процес регулюється академічними правилами ЛНТУ. Здобувачі освіти зобов’язані ознайомитися з вимогами, визначеними Кодексом академічної доброчесності ЛНТУ та Політикою етичного використання штучного інтелекту в ЛНТУ, і дотримуватися принципів академічної доброчесності та етичного використання штучного інтелекту в освітній діяльності.

Академічна доброчесність. Учасники освітнього процесу зобов’язані дотримуватися Закону України «Про академічну доброчесність» від 18.12.2025 № 4742-IX та внутрішніх нормативних документів ЛНТУ. Не допускаються академічний плагіат, фабрикація, фальсифікація, привласнення авторства, несамостійне виконання завдань, а також недоброчесне використання результатів, згенерованих штучним інтелектом.

Використання штучного інтелекту. Інструменти штучного інтелекту можуть використовуватися для пошуку ідей, пояснення методів, попереднього структурування, мовного редагування та допоміжного аналізу неконфіденційних даних, якщо конкретне завдання не передбачає повністю самостійного виконання. Здобувач освіти має зазначати використаний інструмент, мету та етап його застосування, перевіряти факти й розрахунки та самостійно обґрунтовувати висновки.

11. Література

І. Навчально-методичні матеріали та розробки

Праці автора силабуса:

1. IoT-технології для кіберфізичних систем : конспект лекцій для здобувачів другого (магістерського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузь знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія денної та заоч. форм навч. / уклад. С. В. Гринюк. Луцьк : ЛНТУ, 2026. 48 с. URL: https://repository.lntu.edu.ua/handle/123456789/4406.

2. Програмування на Python : метод. вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 (F) Інформаційні технології денної та заоч. форм навч. / уклад.: С. М. Костючко, Л. М. Конкевич. Луцьк : ЛНТУ, 2026. 60 с. URL: https://repository.lntu.edu.ua/handle/123456789/3352.

ІІ. Наукові праці

Праці автора силабуса:

3. Tkachuk A., Polishchuk M., Polishchuk L., Kostiuchko S., Hryniuk S., Konkevych L. Investigation of DC-AC converter with microcontroller control of inverter frequency. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2025. Vol. 15, No. 1. P. 55–61. URL: https://repository.lntu.edu.ua/handle/123456789/2012.

4. Bahniuk N., Terletskyi T., Kaidyk O., Kostiuchko S., Kondius I. Solving operational tasks in the design of video surveillance systems. CEUR Workshop Proceedings : Applied Information Technologies and Artificial Intelligence Systems. 2025. P. 332–342. URL: https://ceur-ws.org/Vol-4160/paper20.pdf.

5. Khrystynets N., Melnyk K., Lavrenchuk S., Miskevych O., Kostiuchko S. Multiprocessing as a Way to Optimize Queries. Advances in Transdisciplinary Engineering. 2024. No. 48. P. 455–464. DOI: https://doi.org/10.3233/ATDE231357.

6. Римчук І., Костючко С., Поліщук М., Гринюк С., Конкевич Л. Безпека комунікаційних

процесів з використанням візуальної криптографії. Кібербезпека: освіта, наука, техніка. 2024. № 2(26). С. 258–267. URL: https://repository.lntu.edu.ua/handle/123456789/4595.

7. Каган І., Костючко С. CRM-системи як інструмент підвищення ефективності бізнесу. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 52. С. 5–9. DOI: https://doi.org/10.36910/6775-2524-0560-2023-52-01.

8. Polishchuk M., Grinyuk S., Kostiuchko S., Tkachuk A., Savaryn P. Tesla Switch of 4 Batteries Based on the Arduino Uno Board. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2023. Vol. 13, No. 3. P. 111–116. DOI: https://doi.org/10.35784/iapgos.4051.

9. Kostiuchko S., Polishchuk M., Zabolotnyi O., Tkachuk A., Twarog B. The Auxiliary Parametric Sensitivity Method as a Means of Improving Project Management Analysis and Synthesis of Executive Elements. Emerging Technologies in Computing / eds. M. H. Miraz, G. Southall, M. Ali, A. Ware, S. Soomro. Cham : Springer, 2021. (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering ; vol. 395). P. 92–103. DOI: https://doi.org/10.1007/978-3-030-90019-9_8.

10. Kostiuchko S., Kyryliuk L., Chernyashchuk N., Bortnyk K., Hrunjuk S. Wireless access point with multilayer data protection algorithm. Computer-integrated technologies: education, science, production. 2021. No. 42. P. 147–151. DOI: https://doi.org/10.36910/6775-2524-0560-2021-42-21.

11. Костючко С. М., Багнюк Н. В., Кузьмич О. І., Поліщук М. М., Кирилюк Л. М. Біометрична ідентифікація засобами Python та Raspberry Pi. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2021. Вип. 42. С. 142–146. DOI: https://doi.org/10.36910/6775-2524-0560-2021-42-20.

Праці інших авторів:

12. Ситник В. Ф., Писаревська Т. А., Єрьоміна Н. В., Краєва О. С. Основи інформаційних систем : навч. посіб. Київ : КНЕУ. 250 с.

13. Kostiuk Y., Bebeshko B., Kriuchkova L., Lytvynov V., Oksanych I., Skladannyi P., Khorolska K. Information protection and data exchange security in wireless mobile networks with authentication and key exchange protocols. Cybersecurity: Education, Science, Technique. 2024. No. 1(25). P. 229–252. DOI: https://doi.org/10.28925/2663-4023.2024.25.229252.

14. Adenubi A. O., Oduroye A. P. Data security in big data: challenges, strategies, and future trends. International Journal of Research in Education, Humanities and Commerce. 2024. Vol. 5, No. 2. P. 1–15. DOI: https://doi.org/10.37602/ijrehc.2024.5201.

15. Li X., Wang Z., Leung V. C. M., Ji H., Liu Y., Zhang H. Blockchain-empowered data-driven networks. ACM Computing Surveys. 2021. Vol. 54, No. 3. P. 1–38. DOI: https://doi.org/10.1145/3446373.

16. Yeoh W., Liu M., Shore M., Jiang F. Zero trust cybersecurity: critical success factors and a maturity assessment framework. Computers & Security. 2023. Art. no. 103412. DOI: https://doi.org/10.1016/j.cose.2023.103412.

17. Prince N. U., Faheem M. A., Khan O., Hossain K., Alkhayyat A., Hamdache A., Elmouki I. AI-powered data-driven cybersecurity techniques: boosting threat identification and reaction. Nanotechnology Perceptions. 2024. Vol. 20, No. S10. P. 332–353. DOI: https://doi.org/10.62441/nano-ntp.v20is10.25.

18. Mataz A., Haripriya V. Enhancing data protection through advanced encryption or improving data security with advanced encryption. International Journal of Innovative Research in Computer and Communication Engineering. 2024. Vol. 12, No. 3. P. 1710–1715. DOI: https://doi.org/10.15680/ijircce.2024.1203056.

19. Szumelda P., Orzechowski N., Rawski M., Janicki A. VHS-22 – A very heterogeneous set of network traffic data for threat detection. EICC 2022: European Interdisciplinary Cybersecurity Conference. New York : ACM, 2022. DOI: https://doi.org/10.1145/3528580.3532843.

20. De Carvalho Bertoli G., Pereira Junior L. A., Saotome O., Dos Santos A. L., Verri F. A. N., Marcondes C. A. C., Barbieri S., Rodrigues M. S., Parente De Oliveira J. M. An end-to-end framework for machine learning-based network intrusion detection system. IEEE Access. 2021. Vol. 9. P.

106790–106805. DOI: https://doi.org/10.1109/access.2021.3101188.

21. Hulak H. M., Zhiltsov O. B., Kyrychok R. V., Korshun N. V., Skladannyi P. M. Information and Cyber Security of the Enterprise : textbook. Lviv : Marchenko T. V., 2024.