МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА
ФАКУЛЬТЕТ УПРАВЛІННЯ ФІНАНСАМИ ТА БІЗНЕСУ

КАФЕДРА ЦИФРОВОЇ ЕКОНОМІКИ ТА БІЗНЕС-АНАЛІТИКИ

ЗАТВЕРДЖУЮ

Декан

_____доц. А.В. Стасишин

“____” _____ 2023 р.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кіберпростір та протидія кіберзлочинності

(назва навчальної дисципліни)

галузь знань: 05 “Соціальні та поведінкові науки”
(шифри та найменування галузей знань)

спеціальність: 051 “Економіка”
(коди та найменування спеціальностей)

спеціалізація: Інформаційні технології в бізнесі
(найменування спеціалізацій)

освітній ступінь: магістр
(бакалавр/магістр)

форма навчання: денна
(денна, заочна)

ЛЬВІВ 2023

Програма навчальної дисципліни “Кіберпростір та протидія кіберзлочинності” для студентів, які навчаються за галуззю знань 05 “Соціальні та поведінкові науки” спеціальністю 051 “Економіка” спеціалізацією “Інформаційні технології в бізнесі” освітнього ступеня магістр.

28 серпня 2023 року – 21 с.

Розробник: Ярема О.Р., доцент кафедри цифрової економіки та бізнес аналітики, к.е.н., доцент.

Розглянуто та ухвалено на засіданні кафедри цифрової економіки та бізнес-аналітики
Протокол № 1 від “28” серпня 2023 р.

Завідувач кафедри _____ Шевчук І.Б.
(прізвище, ініціали)

Розглянуто та ухвалено Вченою радою факультету управління фінансами та бізнесу
Протокол № __ від “__” _____ 2023 р.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

Дисципліна "Кіберпростір та протидія кіберзлочинності" є важливим компонентом сучасної освіти, оскільки кіберпростір став неодмінною складовою нашого повсякденного життя, а віртуальні загрози стали серйозними проблемами для суспільства.

Актуальність дисципліни "Кіберпростір та протидія кіберзлочинності" у сучасному світі вкрай висока з численними обґрунтованими причинами:

1. Зростання кіберзлочинності: Злочини в кіберпросторі, такі як хакерські атаки, фішинг, кібер-викрадення даних та інші, стають все поширенішими та складнішими. Це завдає значних збитків як господарству, так і індивідуальним користувачам.

2. Зростання важливості інформації: В сучасному світі інформація має велику вартість. Кіберзлочинці цікавляться конфіденційними даними, бізнес-секретами, фінансовою інформацією та іншими важливими ресурсами. Захист цих даних стає надзвичайно важливим завданням.

3. Завдання державної та глобальної безпеки: Кіберзлочинність може бути використана для атак на державні інтереси, включаючи виборчі системи, критичну інфраструктуру та оборонні системи. Захист національної та глобальної безпеки потребує кваліфікованих фахівців у галузі кібербезпеки.

4. Запит на професійних фахівців у галузі кібербезпеки: Зростаюча кількість компаній та урядових організацій відділяє увагу кібербезпеці та постійно шукає висококваліфікованих спеціалістів, які

здатні захищати їхні інформаційні ресурси від атак.

5. Широкий спектр загроз: Загрози в кіберпросторі постійно змінюються та розвиваються, включаючи нові види атак та атаки, спрямовані на різні галузі та сектори. Перспектива розуміння та боротьби з цими загрозами важлива для сучасних фахівців у галузі інформаційної безпеки.

6. Законодавчі та регуляторні вимоги: Багато країн впроваджують закони та нормативи, які вимагають від організацій приділяти більше уваги кібербезпеці. Розуміння цих вимог та їх виконання є важливими аспектами для багатьох організацій.

7. Розвиток технологій: Швидкий розвиток інформаційних технологій створює нові можливості для кіберзлочинців. Фахівці з кібербезпеки мають залишатися в тренді з новітніми технологіями та методами атак для ефективної протидії.

Зважаючи на ці фактори, дисципліна "Кіберпростір та протидія кіберзлочинності" стає критично важливою для підготовки кваліфікованих фахівців, які можуть захищати інформацію, інфраструктуру та безпеку в цифровому світі.

Предмет навчальної дисципліни

Ця дисципліна спрямована на вивчення та розуміння кіберпростору та кіберзлочинності. Основні аспекти цієї дисципліни включають:

- Вивчення структури та функціонування кіберпростору, включаючи мережі, інтернет, обчислювальні системи та інші компоненти цифрового середовища.
- Аналіз різних видів кіберзлочинності, таких як хакерство, фішинг, віруси, атаки на мережі та інші, а також їх вплив на організації та індивідів.
- Вивчення методів та засобів захисту інформації та інфраструктури від кібератак, включаючи застосування шифрування, файрволів, антивірусних програм та інших технічних засобів.
- Розгляд законодавчих та регуляторних аспектів, які відносяться до кібербезпеки та кіберзлочинності, включаючи правові стандарти та норми поведінки в цифровому середовищі.
- Розуміння етичних питань, пов'язаних з використанням кіберпростору, та підтримання етичних стандартів в цифровому світі.
- Вивчення методів та засобів для захисту особистих даних та збереження приватності в інтернеті.
- Аналіз питань, пов'язаних із кібербезпекою на національному та міжнародному рівнях, включаючи аспекти кібервійни та кібердипломатії.

Дисципліна "Кіберпростір та протидія кіберзлочинності" важлива у сучасному світі, де інформаційні технології мають велике значення, а загрози в кіберпросторі постійно зростають. Фахівці, які володіють знаннями у цій галузі, мають важливий внесок у забезпечення безпеки інформації та інфраструктури.

Мета навчальної дисципліни

Мета дисципліни "Кіберпростір та протидія кіберзлочинності" полягає в наданні студентам глибокого розуміння кіберпростору та кіберзлочинності, а також розвитку навичок і компетенцій, необхідних для ефективного захисту інформації, інфраструктури та безпеки в цифровому середовищі.

Вимоги до знань і умінь

Вивчення навчальної дисципліни “Кіберпростір та протидія кіберзлочинності” передбачає досягнення такого кваліфікаційного рівня підготовки магістра, за якого він повинен отримати:

а) знання

- Основ інформатики: Студенти повинні мати базове розуміння комп'ютерних систем, операційних систем, мереж, програмування та інших аспектів інформатики.
- Основ кібербезпеки: Розуміння основних термінів і концепцій у галузі кібербезпеки, таких як аутентифікація, авторизація, шифрування, загрози, інциденти та інше.
- Основ мереж і інтернету: Розуміння архітектури мереж, принципів роботи Інтернету та основних мережевих протоколів.
- Основ законодавства та регуляції: Розуміння основних правових та регуляторних аспектів, пов'язаних з кібербезпекою та кіберзлочинністю.

б) уміння:

- Захист інформації: Здатність розробляти та реалізувати заходи для захисту інформації від несанкціонованого доступу, витоку даних та інших загроз.
- Виявлення і реагування на кіберзлочинність: Здатність виявляти потенційні кібератаки, аналізувати їх та вживати заходи для реагування на інциденти.
- Етична поведінка в кіберпросторі: Дотримання етичних норм та стандартів використання кіберпростору, у тому числі пов'язаних із захистом інформації та безпекою.
- Комунікаційні навички: Здатність ефективно комунікувати з іншими фахівцями, як у сфері кібербезпеки, так і в організаціях та громадськості.
- Розуміння законодавства та регуляції: Здатність визначати відповідність дій та практик законодавству та регуляторним вимогам в галузі кібербезпеки.

Вимоги можуть бути дуже конкретними і можуть включати знання певних програмних засобів для кібербезпеки, навички аналізу кіберзагроз, здатність розробки планів кіберзахисту тощо. Важливо, щоб студенти були готові до вивчення складних технічних та правових аспектів кібербезпеки та кіберзлочинності.

Місце навчальної дисципліни в структурно-логічній схемі

Навчальна дисципліна взаємопов'язана із такими дисциплінами як «Інформаційні та комунікаційні технології», «Інформаційні системи в управлінні», «Комп'ютерні мережі», «Цифрова економіка», «ІТ-Право»

Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни.

При вивченні дисципліни «Кіберпростір та протидія кіберзлочинності» здобувачі вищої освіти набувають такі компетентності (здатність):

ІК1 – Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в економічній сфері, які характеризуються комплексністю та невизначеністю умов, що передбачає застосування теорій та методів економічної науки.

ЗК3 − Здатність до абстрактного мислення, аналізу та синтезу.

ЗК5 − Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК8 − Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК9 − Здатність до адаптації та дій в новій ситуації.

ЗК10 − Здатність бути критичним і самокритичним.

СК13 − Здатність проводити економічний аналіз функціонування та розвитку суб'єктів господарювання, оцінку їх конкурентоспроможності.

СК14 − Здатність поглиблено аналізувати проблеми і явища в одній або декількох професійних сферах з врахуванням економічних ризиків та можливих соціально-економічних наслідків.

СК17 − Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями.

Програмні результати навчання:

ПР05 − Застосовувати аналітичний та методичний інструментарій для обґрунтування пропозицій та прийняття управлінських рішень різними економічними агентами (індивідуумами, домогосподарствами, підприємствами та органами державної влади).

ПР06 − Використовувати професійну аргументацію для донесення інформації, ідей, проблем та способів їх вирішення до фахівців і нефахівців у сфері економічної діяльності.

ПР10 − Проводити аналіз функціонування та розвитку суб'єктів господарювання, визначати функціональні сфери, розраховувати відповідні показники які характеризують результативність їх діяльності.

ПР13 − Ідентифікувати джерела та розуміти методологію визначення і методи отримання соціально-економічних даних, збирати та аналізувати необхідну інформацію, розраховувати економічні та соціальні показники.

ПР25 − Розуміти структуру, основні принципи діяльності та бізнес-процеси суб'єктів ІТ-індустрії.

Результати навчання

В результаті вивчення навчальної дисципліни "Кіберпростір та протидія кіберзлочинності" студенти зможуть досягти наступних цілей та результатів:

1. Розуміння кіберпростору та кіберзлочинності: Студенти зможуть отримати глибоке розуміння сутності та особливостей кіберпростору, а також різних видів кіберзлочинності.

2. Знання про загрози і вразливості: Студенти будуть знати основні загрози та вразливості, які існують в кіберпросторі, і зможуть ідентифікувати їх.

3. Виявлення та аналіз кібератак: Студенти навчаться виявляти та аналізувати кібератаки, включаючи хакерські атаки, фішинг, віруси та інші види кіберзлочинності.

4. Захист і кібербезпека: Студенти будуть здатні розробляти та впроваджувати заходи забезпечення кібербезпеки, включаючи використання шифрування, файрволів, антивірусних програм та інших технічних засобів.

5. Легітивні аспекти та етика: Студенти будуть розуміти законодавчі та регуляторні аспекти, пов'язані з кібербезпекою та кіберзлочинністю, і дотримуватися етичних стандартів в цифровому середовищі.

6. Захист даних та приватності: Студенти навчаться методам та засобам захисту особистих даних та збереження приватності в інтернеті.

7. Кібернаціональна та кіберміждержавна безпека: Студенти будуть розуміти аспекти кібербезпеки на національному та міжнародному рівнях, включаючи питання кібервійни та кібердипломатії.

8. Комунікаційні навички: Студенти навчаться ефективно комунікувати з іншими фахівцями у галузі кібербезпеки та з громадськістю щодо питань кіберзлочинності.

9. Підготовка до захисту від кіберзагроз: Студенти будуть готові реагувати на кібератаки та інциденти, розробляти плани захисту та відновлення після інцидентів.

10. Професійний розвиток: Дисципліна сприятиме професійному розвитку студентів в галузі кібербезпеки і підготовці до роботи в цій галузі.
Опанування навчальною дисципліною повинно забезпечувати необхідний рівень сформованості вмінь:

Назва рівня сформованості вміння	**Зміст критерію рівня сформованості вміння**
1.Репродуктивний	Вміння відтворювати знання, передбачені даною програмою
2. Алгоритмічний	Вміння використовувати знання в практичній діяльності при розв'язуванні типових ситуацій
3. Творчий	Здійснювати евристичний пошук і використовувати знання для розв'язання нестандартних завдань та проблемних ситуацій

Програма складена на **3 кредити**

Форми контролю – проміжний модульний контроль, залік.

2. ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Номер теми	Назва теми
Тема 1.	Вступ до кіберпростору та кіберзлочинності
Тема 2.	Кібербезпека в організаціях та суспільстві
Тема 3.	Соціальна інженерія та Інтернет свобода: Ключові аспекти в цифровому віці
Тема 4.	Сучасні Технології та Тренди в Кібербезпеці для Бізнесу та Безпеки Інформації

3. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Вступ до кіберпростору та кіберзлочинності

Пояснення важливості кіберпростору та кібербезпеки в сучасному світі.Визначення кіберпростору та його складових частин. Кіберзлочинність. Визначення кіберзлочинності та її вплив на суспільство. Обговорення різних типів кіберзлочинів, таких як хакерство, фішинг, віруси, шпигунство тощо. Приклади відомих кібератак та їх наслідки. Заходи протидії кіберзлочинності. Законодавство та міжнародні стандарти у сфері кібербезпеки. Кіберзлочинність в Україні

Тема 2. Кібербезпека в організаціях та суспільстві

Що потрібно знати бізнесу про кібербезпеку? Види кіберзагроз, їх наслідки та поради щодо захисту. Секрети успіху України та українського бізнесу в боротьбі проти кібератак російських агресорів. Як захистити ваш бізнес від кіберзагроз? Війна росії проти України: хронологія кібератак.

Тема 3. Соціальна інженерія та Інтернетсвобода: Ключові аспекти в цифровому віці

Індекс свободи в інтернеті. GDPR або General Data Protection Regulation. Соціальна інженерія. Тестування на проникнення

Тема 4. Сучасні Технології та Тренди в Кібербезпеці для Бізнесу та Безпеки Інформації

Сучасні тренди та технології кібербезпеки. Топ-технології, що підкорюють бізнес сьогодення. Штучний інтелект змінить конфіденційність і безпеку даних. Генеративний ШІ відкриє нову цінність даних. Чат-боти нарешті довели свою корисність і можливості в CX/EX. Блокчейн для створення бізнес-кейсів. Цифрові технології стимулюють трансформацію охорони здоров'я. Сталі технології стануть пріоритетом для компаній. Інструменти IDS та IPS для кращого аналізу мережі та безпеки. Що таке система виявлення вторгнень (IDS)? Що таке система запобігання вторгненням (IPS)? Чим можуть допомогти IDS та IPS? Приклади програмних рішень IDS та IPS. Безпека і кібербезпека смартфонів. Кібербезпека та інтернет речей: правовий аспект.

5. СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Альварез Р., Стілл Дж. Кібербезпека для початківців. – Харків: Видавництво "Сміт", 2020. – 240 с.
2. Браун К. Кіберзагрози: Технологія та захист. – Львів: Світ книг, 2017. – 240 с.
3. Власко С. Защита персональных данных: чей опыт может пригодиться Украине. Европейская правда. 2018. URL: https://www.eurointegration.com.ua/ rus/experts/ 2018/01/16/ 7076152/.

4. Галак М. Кіберзлочини: Методи, суб'єкти та вимоги для доказу. – К.: Видавництво "Юрінком Інтер", 2018. – 224 с.

5. Гібсон, Д. Кібербезпека і захист від кіберзагроз. – Львів: Видавництво "Спадок", 2020. – 296 с.

6. Елущенко Н. Что такое интернет вещей? Даже ваша бабушка это поймет. AIN. 2018. URL: https://ain.ua/special/what-is-iot/.

7. Європейський Союз, Офіційний текст Регламенту GDPR. European Data Protection Board

8. Картер, Дж. Кіберзахист в корпоративному середовищі. – Харків: Видавництво "ІнфоПрос", 2019. – 320 с.

9. Кейсер Е. В. Кіберзлочинність і право: Посібник для юристів. – К.: Юрінком Інтер, 2019. – 192 с.

10. Кеннеді, Д., О'Горман, Д., та Вінні, Д. "Metasploit: The Penetration Tester's Guide."

11. Кодекс України про адміністративні правопорушення (статті 1 - 212-24): Закон від 07 груд. 1984 р. № 8073-X. Відомості Верховної Ради Української РСР. 1984. Додаток до № 51. Ст. 1122.

12. Конституція України від 28 чер. 1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

13. Кримінальний кодекс України від 05 квіт. 2001 р. №2341-111. Відомості Верховної Ради України. 2001. № 25-26. Ст. 131.

14. Ландіні, М. Інформаційна безпека: Захист даних і систем. – Дніпро: Видавництво "Престиж", 2018. – 224 с.

15. Макдональд Г. Кіберзлочинність: Підручник для студентів. – Львів: Видавництво Львівської політехніки, 2017. – 312 с.

16. Маріч, А., та інші. "GDPR: Регламент про захист персональних даних."

17. Мітнік, К., та Саймонс, В. "The Art of Deception: Controlling the Human Element of Security."

18. Мюррей, Дж., Баулинг, К. Кіберзахист і кіберзлочинність: Теорія і практика. – К.: Видавництво "ІнфоДім", 2022. – 368 с.

19. Ньюман М. Історія кіберзлочинності: Від комп'ютерних вайрусів до кібервійн. – К.: Видавництво "Наукова думка", 2019. – 368с.

20. Пригула П. 5 проблем интернета вещей, которые предстоит решить. CNews. 2016. URL: https://www.cnews.ru/articles/2016-05-27_5_ problem_ intemeta_veshchej_kotorye_ predstoit_ reshit.

21. Про захист персональних даних: Закон України від 01 чер. 2010 р. № 2297-VI. Відомості Верховної Ради України. 2010. №34. Ст. 481.

22. Сімсон Г., Сталлінгс В. Основи комп'ютерної безпеки. – Харків: Основа, 2019. – 384 с.

23. Сімсон, Г., Хакер, Е. Кіберзахист: Засоби та методи. – К.: Видавництво "Техніка", 2021. – 448 с.

24. Сміт П. Інформаційна безпека та захист даних. – Дніпро: Діалектика, 2021. – 312 с.

25. Сталлінгс В. А. Кібербезпека: Вступ до інформаційної безпеки. – К.: Навчальний центр "Ельга", 2018. – 432 с.

26. Технология «Интернет вещей»: автоматизация настоящего благодаря разработкам будущего. IT рейтинг UA. 2020. URL: https://it-

rating.in.ua/ tehnologiya-intemet-veschey-avtomatizatsiya-nastoyaschego-blagodarya- razrabotkam-buduschego.

27. Хедні, К., та Вільямс, П. "Social Engineering: The Art of Human Hacking."

28. Хілько В. І. Кіберзахист: Теорія і практика. – К.: Видавництво "Логос", 2020. – 288 с.

29. Холлінс Т. Ж. Кіберзлочинність і кібербезпека: Основи, виклики та рішення. – Дніпро: Видавництво "Ліга-Прес", 2021. – 416 с.

30. Центр досліджень армії, конверсії та роззброєння. Штучний інтелект на сторожі безпеки даних: інноваційні технології та хмарні сервіси допомагають забезпечити кібербезпеку [Електронний ресурс] Режим доступу: https://cacds.org.ua/штучний-інтелект-на-сторожі-безпеки-д

31. A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things / G. Frieder, D. Puschmann, P. Barnaghi, F. Carrez. IEEE Internet of Things Journal. 2015. №2. С. 340-354. https://doi.org/ 10.1109/ ЛОТ.2015.2411227

32. A Strategic Compass for Security and Defence, EEAS, March 2022.

33. Activation of first capability developed under PESCO points to strength of cooperation in cyber defence, EDA, February 2022.

34. Antoniuk, D., DDoS attacks hit Ukrainian government websites, The Record, February 2022.

35. Attribution to Russia of malicious cyber activity against Ukraine, Australian government, February 2022.

36. Brumfield, C., Russia-linked cyber-attacks on Ukraine: A timeline, CSO, April 2022.

37. Cerulus, L., How Ukraine became a test bed for cyberweaponry, Politico, February 2019.

38. Cerulus, L., Ukraine is getting pummeled with cyber-attacks. What's the West to do?, Politico, February 2022.

39. Cimpanu, C., Hackers deface Ukrainian government websites, The Record, January 2022.

40. Cimpanu, C., Ukraine reports cyber-attack on government document management system, Zdnet, February 2021.

41. Clayton, M., Russia Hammers Ukraine With Massive Cyber-Attack, Business Insider, March 2014.

42. Corewin: сучасні тренди кібербезпеки. [Електронний ресурс] Режим доступу: https://corewin.ua/blog/cybersecurity-trends/

43. Datami: захист вашого бізнесу в інтернеті. Безпека і кібербезпека смартфонів. [Електронний ресурс] Режим доступу: https://datami.ua/bezpeka-i-kiberbezpeka-smartfoniv/

44. Deputy Secretary General stresses NATO will continue to increase Ukraine's cyber defences, NATO, January 2022.

45. EU imposes the first ever sanctions against cyber-attacks, Council of the European Union, July 2020.

46. Fendorf, K. and Miller, J., Tracking Cyber Operations and Actors in the Russia-Ukraine War, Council on Foreign Relations, March 2022.

47. Freedom House, "Freedom on the Net" Reports. Global Internet Freedom Consortium.

48. Harding, L., Ukraine hit by 'massive' cyber-attack on government websites, The Guardian, January 2022.

49. Hern, A., Ukrainian blackout caused by hackers that attacked media company, researchers say, The Guardian, January 2016.

50. Holland, Steve. and Pearson J., US, UK: Russia responsible for cyber-attack against Ukrainian banks, Reuters, February 2022.

51. Hybrid CoE continues to work to support European security and Ukraine, Hybrid CoE, March 2022.

52. Internet of Things (IoT). European Union Agency for Cybersecurity. 2018. URF: https://www.enisa.europa.eu/topics/iot-and-smart- infrastructures/iot.

53. Ishak, N., Is Russia holding back from cyberwar?, Vox, March 2022.

54. Kagubare, I., US, EU cyber investments in Ukraine pay off amid war, The Hill, March 2022.

55. Legal service: Кібербезпека бізнесу під час війни [Електронний ресурс]. Режим доступу: https://mklegalservice.com/tpost/k123zz39h1-kberbezpeka-bznesu-pd-chas-vini

56. Madiega, T., Russia's war on Ukraine: The digital dimension, EPRS, March 2022.

57. Madnick, S., What Russia's Ongoing Cyber-attacks in Ukraine Suggest About the Future of Cyber Warfare, Harvard Business Review, March 2022.

58. Menn, J., Hacking Russia was off-limits. The Ukraine war made it a free-for-all, Washington Post, May 2022.

59. Miller, M., Despite years of preparation, Ukraine's electric grid still an easy target for Russian hackers, Politico, February 2022.

60. NotPetya, CyberLaw, May 2019.

61. NotPetya, Five Facts to Know About History's Most Destructive Cyber-attack, HYPR, June 2017.

62. Offensive Security. Документація та інструкції Metasploit Framework.

63. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da). European Parliament and of the Council. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

64. Resolution of 1 March 2022 on the Russian aggression against Ukraine (2022/2564(RSP)), European Parliament, 1 March 2022.

65. Resolution of 11 February 2021 on the implementation of the EU Association Agreement with Ukraine (2019/2202(INI)), European Parliament, 11 February 2022.

66. Scroxton, A., Ukraine joins Nato cyber knowledge hub, Computer Weekly, March 2022.

67. Techukraine.net. 8 інструментів IDS та IPS для кращого аналізу мережі та безпеки [Електронний ресурс] Режим доступу: https://techukraine.net/8-інструментів-ids-та-ips-для-кращого-аналізу

68. Terazus: Бізнес, технології. Топ-технології, що підкорюють бізнес цього року [Електронний ресурс] Режим доступу: https://terazus.com/uk/1164-top-texnologii-scho-pidkorjujut-biznes-tsjogo-roku

69. UK assesses Russian involvement in cyber attacks on Ukraine, Foreign, Commonwealth & Development Office and National Cyber Security Centre, United Kingdom, February 2022.

70. Ukraine accuses Russian networks of new massive cyber attacks, Reuters, February 2022.

71. Ukraine power cut 'was cyber-attack', BBC, January 2017.

72. Ukraine: Timeline of Cyber-attacks on critical infrastructure and civilian objects, CyberPeace Institute, April 2022.

73. Vazquez, M., Judd D., Lyngaas S. and Cohen, Z., Biden warns business leaders to prepare for Russian cyber attacks, CNN Politics, March 2022.

74. What is a DDoS attack?, Cloud Flare.

75. Wiper Attacks, Firewalls Security Blog.

76. Wolff, J., Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine, Time, March 2022