КАФЕДРА ЦИФРОВОЇ ЕКОНОМІКИ ТА БІЗНЕС-АНАЛІТИКИ

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

ЗАТВЕРДЖУЮ
Декан

_____доц. А.В. Стасишин

“____” _____ 2023 р.

РОБОЧА 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

Робоча 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 – 40 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.

ЗМІСТ

1. ПОЯСНЮВАЛЬНА ЗАПИСКА 4
2. ОПИС ПРЕДМЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ 13
3. ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.....13
4. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ 14
5. СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ 15
6. ГРАФІК РОЗПОДІЛУ НАВЧАЛЬНОГО ЧАСУ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ ТА ВИДАМИ НАВЧАЛЬНОЇ РОБОТИ 23
7. КАЛЕНДАРНО-ТЕМАТИЧНИЙ ПЛАН АУДИТОРНИХ ЗАНЯТЬ.....24
7.1. Календарно-тематичний план лекційних занять.....24
7.2. Календарно-тематичний план лабораторних/семінарських занять, заліків по модулях, контрольних робіт 26
7.3. Графік консультацій 27
8.ПЕРЕЛІК ПИТАНЬ, ЩО ВИНОСЯТЬСЯ НА ПІДСУМКОВИЙ КОНТРОЛЬ.....27
9. МЕТОДИ ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ 32
9.1. Таблиця оцінювання (визначення рейтингу) навчальної діяльності студентів 32
9.2. Система нарахування рейтингових балів та критерії оцінювання знань студентів 33
9.3. Шкала оцінювання: Університету, національна шкала та ECTS 35
10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ 36
11. МЕТОДИКИ АКТИВІЗАЦІЇ ПРОЦЕСУ НАВЧАННЯ.....36
12. РЕСУРСИ МЕРЕЖІ ІНТЕРНЕТ 38
13. ЗМІНИ І ДОПОВНЕННЯ ДО РОБОЧОЇ ПРОГРАМИ 40

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. ОПИС ПРЕДМЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

“ Кіберпростір та протидія кіберзлочинності ”

<table>
<tr><th colspan="8">Характеристика навчальної дисципліни</th></tr>
<tr><td colspan="4">Шифр та найменування галузі знань:
05 „Соціальні та поведінкові науки”</td><td colspan="4">Цикл дисциплін за навчальним планом:
Цикл професійної та практичної підготовки</td></tr>
<tr><td colspan="4">Код та назва спеціальності:
051 „Економіка”</td><td colspan="4">Освітній ступінь:
магістр</td></tr>
<tr><td colspan="4">Спеціалізація:
„Інформаційні технології в бізнесі”</td><td colspan="4"></td></tr>
<tr><td colspan="4">Курс: 6
Семестр: I</td><td colspan="4">Методи навчання:
Лекції, лабораторні заняття, самостійна робота, робота в бібліотеці, Інтернеті тощо.</td></tr>
<tr><td>Кількість кредитів ECTS</td><td>Кількість годин</td><td>Кількість аудиторних годин</td><td>Лекції</td><td>Семінари, практичні, лабораторні</td><td>Заліки по модулях (контрольні роботи)</td><td>Самостійна робота студента (СРС)</td><td>Індивідуальна робота студента (ІНДЗ)</td></tr>
<tr><td>3</td><td>90</td><td>24</td><td>8</td><td>16</td><td>1</td><td>66</td><td>-</td></tr>
<tr><td colspan="2">Кількість тижневих годин</td><td colspan="2">Кількість змістових модулів (тем)</td><td colspan="2">Кількість модулів /контрольних робіт</td><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">3</td><td colspan="2">4</td><td colspan="2">1</td><td colspan="2">ПМК, залік</td></tr>
</table>

3. 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

4. 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

6. ГРАФІК РОЗПОДІЛУ НАВЧАЛЬНОГО ЧАСУ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ ТА ВИДАМИ НАВЧАЛЬНОЇ РОБОТИ

№ розділу, теми (змістові модулі)	Назва розділу, теми (змістового модуля)	Кількість годин за ОПП			Розподіл аудиторних годин		
		всього	у тому числі		лекції	лабораторні	змістові модулі, (контрольні роботи)
			аудиторні	СРС/ ІР			
ЗАЛІКОВИЙ МОДУЛЬ № 1							
Тема 1.	Вступ до кіберпростору та кіберзлочинності	30	6	15	2	4	
Тема 2.	Кібербезпека в організаціях та суспільстві	30	6	17	2	4	
Тема 3.	Соціальна інженерія та Інтернет свобода: Ключові аспекти в цифровому віці	30	6	17	2	4	
Тема 4.	Сучасні Технології та Тренди в Кібербезпеці для Бізнесу та Безпеки Інформації	30	6	17	2	4	
Разом годин		**90**	**24**	**66**	**8**	**16**	

7. КАЛЕНДАРНО-ТЕМАТИЧНИЙ ПЛАН АУДИТОРНИХ ЗАНЯТЬ

7.1. Календарно-тематичний план лекційних занять

№ заня -ття	Тема та короткий зміст заняття	Кіль кість годи
1	2	3
ЗМІСТОВИЙ МОДУЛЬ № 1		
Тема 1.Вступ до кіберпростору та кіберзлочинності		**2**
1	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	2
Тема 2.Кібербезпека в організаціях та суспільстві		**2**
2	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.	2

1	2	3
Тема 3. Соціальна інженерія та Інтернет свобода: Ключові аспекти в цифровому віці		**2**
3	Індекс свободи в інтернеті. GDPR або General Data Protection Regulation. Соціальна інженерія. Тестування на проникнення	2
Тема 4.Сучасні Технології та Тренди в Кібербезпеці для Бізнесу та Безпеки Інформації		
4	Сучасні тренди та технології кібербезпеки. Топ-технології, що підкорюють бізнес сьогодення. Інструменти IDS та IPS для кращого аналізу мережі та безпеки. Безпека і кібербезпека смартфонів. Кібербезпека та інтернет речей: правовий аспект.	2

7.2. Календарно-тематичний план лабораторних/семінарських занять, заліків по модулях, контрольних робіт

№ заня-ття	Тема лабораторного/семінарського заняття. Контрольні роботи (заліки по модулях)	Кількість годин
1	2	3
ЗАЛІКОВИЙ МОДУЛЬ № 1		
1-2	Лабораторна робота №1. **Вступ до кіберпростору та кіберзлочинності**	**4**
	Усне опитування, перевірка виконаних завдань	2
	Заслуховування доповідей студентів з індивідуального завдання по даній темі	2
3-4	Лабораторна робота №2. **Кібербезпека в організаціях та суспільстві**	**4**
	Усне опитування, перевірка виконаних завдань	2
	Заслуховування доповідей студентів з індивідуального завдання по даній темі	2
5-6	Лабораторна робота №3. **Соціальна інженерія та Інтернет свобода: Ключові аспекти в**	**4**
	Усне опитування, перевірка виконаних завдань	2
	Заслуховування доповідей студентів з індивідуального завдання по даній темі	2
7	Лабораторна робота №4. **Сучасні Технології та Тренди в Кібербезпеці для Бізнесу та Безпеки Інформації**	**2**
	Усне опитування, перевірка виконаних завдань	1
	Заслуховування доповідей студентів з індивідуального завдання по даній темі	1
8	Заліковий модуль	2

7.3. Графік консультацій

№ з/п	Назва розділу, теми, зміст консультації	К-ть годин
1.	Консультація до тем 1-4	2
2.	Консультації по виконанню лабораторних робіт	4
	Разом годин	**6**

8.ПЕРЕЛІК ПИТАНЬ, ЩО ВИНОСЯТЬСЯ НА ПІДСУМКОВИЙ КОНТРОЛЬ

1. Що таке кіберпростір і які основні складові його структури?
2. Які переваги і недоліки використання кіберпростору в сучасному світі?
3. Які основні загрози безпеці в кіберпросторі?
4. Які види кіберзлочинності існують і як вони можуть впливати на суспільство?
5. Що таке хакерство і які можливі мотивації хакерів?
6. Які заходи безпеки можуть допомогти захистити комп'ютери та інформацію від кіберзлочинців?
7. Які ролі відіграють правоохоронні органи в боротьбі з кіберзлочинністю?
8. Яким чином організації можуть захищати свою мережеву безпеку?
9. Які популярні методи соціальної інженерії використовуються кіберзлочинцями?
10. Що таке фішинг та як його визнавати та уникати?
11. Які наслідки може мати кібератака на критичну інфраструктуру?
12. Які законодавчі засоби існують для боротьби з кіберзлочинністю в вашій країні?
13. Як можуть кіберзлочинці використовувати шифрування для своїх цілей, і як його можна перехопити?

14. Як важлива кібербезпека для індивідуальних користувачів в цифровому світі?

15. Як розвиток технологій може впливати на майбутню кіберзлочинність і як готуватися до цих змін?

16. Які ризики пов'язані з використанням глобальної мережі Інтернет?

17. Які види кіберзаходів існують для захисту особистих даних в Інтернеті?

18. Які міжнародні організації і ініціативи працюють над забезпеченням кібербезпеки на світовому рівні?

19. Які основні загрози і ризики пов'язані з кібербезпекою?

20. Які види кібератак ви знаєте і як вони можуть вплинути на організації?

21. Які наслідки може мати успішна кібератака для організації?

22. Які стратегії захисту від вірусів і малвару ви можете запропонувати?

23. Які принципи дії DDoS-атаки і як їх запобігти?

24. Які кроки слід вжити в разі кібератаки або витоку даних?

25. Які стандарти та законодавство визначають вимоги до кібербезпеки?

26. Що таке етичне ведення у кібербезпеці, і чому воно важливе?

27. Як ви розумієте поняття "соціальна інженерія" і як їй запобігти?

28. Які підходи до кібербезпеки існують в Україні та чому вони важливі?

29. Як можуть суспільство і громадськість сприяти кібербезпеці?

30. Які найбільш важливі тренди і нові технології в області кібербезпеки?

31. Як визначити потреби у кібербезпеці для конкретної організації?

32. Що таке "мультифакторна аутентифікація" і чому вона важлива для безпеки?

33. Які рекомендації ви маєте щодо створення безпечних паролів?

34. Які основні кроки для створення та впровадження політики кібербезпеки в організації?

35. Які переваги та обмеження має використання шифрування для захисту інформації?

36. Що таке "резервне копіювання" і чому це важливо для кібербезпеки?

37. Які сучасні методи інцидентного реагування і відновлення після кібератаки?

38. Як розуміти поняття "цифровий фірмовий слід" і як його захистити?

39. Які виклики пов'язані з кібербезпекою в хмарному обчисленні?

40. Як можуть кіберзагрози впливати на критичну інфраструктуру, таку як енергетика та транспорт?

41. Як організації можуть підготуватися до можливих майбутніх кібератак?

42. Які основні аспекти кібербезпеки важливі для державних органів та критичної інфраструктури?

43. Яким чином кібербезпека пов'язана з правами на приватність і громадянськими свободами?

44. Що таке Індекс свободи в інтернеті і як він розраховується?

45. Які основні складові оцінки свободи в інтернеті включає Індекс свободи в інтернеті?

46. Які країни відзначаються високими показниками свободи в інтернеті, і чому?

47. Як впливає цензура в інтернеті на громадянські свободи?

48. Що таке GDPR і які права воно надає громадянам Європейського Союзу?

49. Які основні вимоги GDPR щодо обробки особистих даних?

50. Які можливі наслідки порушення GDPR для організацій?

51. Які приклади атак, пов'язаних із соціальною інженерією, ви можете навести?

52. Як захищатися від атак соціальною інженерією?

53. Які етапи включає в себе процес тестування на проникнення?

54. Які інструменти та методики використовуються під час пентесту?

55. Які основні принципи етики пентесту?

56. Які переваги мають пентестери для виявлення вразливостей в інформаційних системах?

57. Яким чином соціальна інженерія може бути використана для зламу комп'ютерних систем?

58. Які правила треба дотримувати для забезпечення конфіденційності особистих даних відповідно до GDPR?

59. Які сфери життя охоплює індекс свободи в інтернеті?

60. Як впливає Індекс свободи в інтернеті на політику країн?

61. Які найважливіші аспекти безпеки інтернету слід враховувати в повсякденному використанні мережі?

62. Як можна захистити свою організацію від атак на проникнення?

63. Які зміни в кібербезпеці та приватності можна очікувати в майбутньому?

64. Що таке кібербезпека і чому вона важлива для сучасного суспільства?

65. Які основні загрози кібербезпеці існують сьогодні?

66. Які конкретні технології впливають на кібербезпеку бізнесу?

67. Як штучний інтелект впливає на конфіденційність і безпеку даних?

68. Які можливості пропонує генеративний штучний інтелект

для обробки даних?

69. Як чат-боти можуть бути використані для поліпшення користувацького досвіду (CX) та досвіду співробітників (EX)?

70. Дайте приклади сценаріїв використання блокчейну в бізнесі.

71. Які виклики і можливості з'являються завдяки цифровим технологіям у сфері охорони здоров'я?

72. Чому сталі технології стають пріоритетом для компаній?

73. Що таке система виявлення вторгнень (IDS) і як вона працює?

74. Які основні функції системи запобігання вторгненням (IPS)?

75. В чому полягає важливість IDS і IPS для кібербезпеки мережі?

76. Назвіть кілька популярних програмних рішень для IDS і IPS.

77. Які основні загрози для кібербезпеки смартфонів?

78. Які заходи можна прийняти для захисту свого смартфона від кіберзагроз?

79. Як правовий аспект впливає на кібербезпеку в Інтернеті речей (IoT)?

80. Які потенційні загрози інтернету речей можуть виникнути з точки зору конфіденційності та безпеки?

81. Які законодавчі заходи вже прийняті для забезпечення кібербезпеки в сфері IoT?

82. Які основні принципи кібербезпеки, які потрібно враховувати при роботі з сучасними технологіями?

83. Як бізнес може адаптувати свої стратегії для кращого захисту від кіберзагроз і використання сучасних технологій для своєї переваги?

9. МЕТОДИ ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

Оцінювання навчальної діяльності студентів здійснюється відповідно до «Положення про контроль та оцінювання навчальних досягнень студентів Львівського національного університету імені Івана Франка» від 01.03.2013 р. із змінами, затвердженими наказом ректора від 01.07.2015 р. № О-96, за 100-бальною системою (за шкалою ECTS та національною шкалою).

Система контролю знань студентів з навчальної дисципліни «Кіберпростір та протидія кіберзлочинності» складається з:

- поточного контролю;
- підсумкового контролю у вигляді заліку за семестровими підсумками.

Бали студентам нараховуються за:

- зроблені завдання на лабораторних/семінарських заняттях;
- індивідуальне завдання
- написання модульної контрольної роботи

Оцінювання рівня знань студентів на лабораторних заняттях проводиться за 5-ти бальною шкалою (від 1 до 5 балів)**.**

Порядок вивчення та оцінювання дисципліни доводиться до відома студентів протягом семестру.

9.1. Таблиця оцінювання (визначення рейтингу) навчальної діяльності студентів

	Поточний та модульний контроль		**РАЗОМ – 100 балів**
Лабораторні заняття	**ІНД ЗВД**	**КМР**	
40	**25**	**35**	

9.2. Система нарахування рейтингових балів та критерії оцінювання знань студентів

№ з/п	Види робіт. Критерії оцінювання знань студентів	Бали рейтингу	Максимальна кількість балів
1. Бали поточної успішності за участь у лабораторних заняттях			
Критерії оцінювання		**5 балів**	
лабораторна робота виконана у зазначений термін, у повному обсязі, без помилок		**5**	
лабораторна робота виконана у зазначений термін, у повному обсязі, але є незначні помилки		**4**	
лабораторна робота виконана у неповному обсязі, або (та) з порушенням терміну її виконання, або (та) при наявності значних помилок		**3**	
виконання пропущеної без поважних причин лабораторної роботи або повторне виконання незарахованої лабораторної роботи		**2**	
лабораторна робота не виконана або не зарахована		**0-1**	

№ з/п	Види робіт. Критерії оцінювання знань студентів	Бали рейтингу	Максимальна кількість балів
2. Індивідуальна робота студента (ІНДЗ)			
Критерії оцінювання		**25 балів**	
робота виконана та захищена згідно графіка, з поясненнями та висновками і в повному обсязі		**20-25**	
робота захищена, але виконана частково, з порушенням термінів або вимог		**12-19**	
робота не захищена та виконана частково, з порушенням термінів або вимог		**6-11**	
робота не захищена та виконана з порушенням Методичних рекомендацій		**1-5**	
робота не виконана.		**0**	

3. Заліковий модуль № 1	
Критерії оцінювання	**35 балів**
Встановлено 3 рівні складності завдань. **1. Перший рівень (завдання 1) – завдання із вибором відповіді – тестові завдання.** Завдання з вибором відповіді на теоретичне питання вважається виконаним правильно, якщо в картці тестування записана правильна відповідь.	**25*1=25**
2. Другий рівень (завдання 2) – завдання на відповідність. Завдання з на відповідність відповіддю вважається виконаним правильно, якщо студент обрав вірні визначення, які підходять для потрібного терміну.	**3*2=6**
3. Третій рівень (завдання 3) – завдання з короткою. Завдання з коротокою відповіддю вважається виконаним правильно, якщо студент дав вірні визначення, посилання, тлумачення, коментарі.	**2*2=4**

Підсумкова оцінка за результатами поточного контролю освітньої діяльності студентів (РПК) за семестр визначається як сума балів за лабораторні заняття за 5-ти бальною шкалою + виконання індивідуального завдання + плюс бали за модульну контрольну роботу.

РПК = лаб 1 + лаб 2 + лаб 3 + лаб 4 + ІНД ЗВД + модульна контрольна робота

Максимальна кількість балів за результатами: поточного контролю − 100;

9.3. Шкала оцінювання: Університету, національна шкала та ECTS

Студенти, що отримали сумарний бал в межах від 21 до 50 за національною шкалою, отримують оцінку FX за шкалою ECTS та скеровуються на повторне складання іспиту.

Оцінка в балах	Оцінка за шкалою ECTS	Визначення	Оцінка за національною системою	
90-100	**A**	**Відмінно (EXCELENT)** − відмінне виконання з незначною кількістю неточностей	**Відмінно**	5
81-89	**B**	**Дуже добре (VERY GOOD)** − вище середніх стандартів, але з деякими неточностями	**Дуже добре**	4
71-80	**C**	**Добре (GOOD)** − в цілому змістовна і правильна робота з певною кількістю значних неточностей	**Добре**	
61-70	**D**	**Задовільно (SATISFACTORY) –** непогано, але зі значною кількістю недоліків	**Задовільно**	3
51-60	**E**	**Достатньо (SUFFICIENT) –** виконання відповідає мінімальним критеріям	**Достатньо**	
21-50	**FX**	**Незадовільно (FAIL)** − необхідна ще певна додаткова робота для успішного складання екзамену	**Незадовільно**	2
0-20	**F**	**Незадовільно (FAIL)** − необхідна серйозна подальша робота, обов'язковий повторний курс	**Незадовільно (повторний курс)**	

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчально-методичне та наукове забезпечення кредитно-модульної системи організації навчального процесу з навчальної дисципліни "Кіберпростір та протидія кіберзлочинності" включає:

- державні стандарти освіти;
- навчальні та робочі навчальні плани;
- навчальну програму;
- робочу програму;
- плани лабораторних/семінарських робіт
- завдання для підсумкового модульного контролю;
- законодавчі та інструктивно-методичні матеріали;
- підручники і навчальні посібники.

11. МЕТОДИКИ АКТИВІЗАЦІЇ ПРОЦЕСУ НАВЧАННЯ

Проблемні лекції направлені на розвиток логічного мислення студентів. Коло питань теми обмежується двома-трьома ключовими моментами. При читанні лекцій студентам даються питання для самостійного обмірковування. Студенти здійснюють коментарі самостійно або за участю викладача.

Робота в малих групах дає змогу структурувати лабораторні заняття за формою і змістом, створює можливості для участі кожного студента в роботі за темою заняття, забезпечує формування особистісних якостей та досвіду спілкування.

Мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже обмежений проміжок часу, обговорити і здійснити їх селекцію

Кейс-метод – розгляд, аналіз конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності.

Презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань тощо.

Банки візуального супроводження – сприяють активізації творчого сприйняття змісту дисципліни за допомогою наочності:

- Навчально-методичні матеріали з вивчення навчальної дисципліни.
- Інтерактивні посібники, підручники .

Використання навчальних технологій для активізації процесу навчання з дисципліни

Тема 1.Вступ до кіберпростору та кіберзлочинності	
Презентації	Пояснення важливості кіберпростору та кібербезпеки в сучасному світі. Обговорення різних типів кіберзлочинів, таких як хакерство, фішинг, віруси, шпигунство тощо.
Проблемні лекції	Заходи протидії кіберзлочинності. Законодавство та міжнародні стандарти у сфері кібербезпеки.
Кейс-метод	Приклади відомих кібератак та їх наслідки. Кіберзлочинність в Україні
Тема 2.Кібербезпека в організаціях та суспільстві	
Проблемні лекції	Як захистити ваш бізнес від кіберзагроз? Війна росії проти України: хронологія кібератак.
Презентації	Секрети успіху України та українського бізнесу в боротьбі проти кібератак російських агресорів.
Тема 3. Соціальна інженерія та Інтернет свобода: Ключові аспекти в цифровому віці	
Презентації	Індекс свободи в інтернеті. GDPR або General Data Protection Regulation.
Проблемні лекції	Тестування на проникнення
Тема 4.Сучасні Технології та Тренди в Кібербезпеці для Бізнесу та Безпеки Інформації	
Презентації	Сучасні тренди та технології кібербезпеки Безпека і кібербезпека смартфонів.
Проблемні лекції	Завантажувачі ОС
Кейс-метод	Кібербезпека та інтернет речей: правовий аспект.

12. РЕСУРСИ МЕРЕЖІ ІНТЕРНЕТ

Ресурси мережі Інтернет	Ресурси мережі Факультету з навчальної дисципліни
1.CyberScoop: Новини та аналітика про кібербезпеку. [Електронний ресурс]. Режим доступу: https://www.cyberscoop.com 2.Krebs on Security: Блог Браяна Кребса, відомого журналіста в галузі кібербезпеки. [Електронний ресурс]. Режим доступу: https://krebsonsecurity.com 3.Threatpost: Новини та аналітика про кібербезпеку, включаючи останні загрози та вразливості. [Електронний ресурс]. Режим доступу: https://threatpost.com 4. Dark Reading: Ресурс, що присвячений новинам та аналітиці у галузі інформаційної безпеки. [Електронний ресурс]. Режим доступу: https://www.darkreading.com 5. SANS Institute: Організація, яка пропонує навчання та ресурси з кібербезпеки, включаючи блог та вебінари. [Електронний ресурс]. Режим доступу: https://www.sans.org 6. The Hacker News: Новини про кібербезпеку та інформаційні технології. [Електронний ресурс]. Режим доступу: https://thehackernews.com 7. Cybersecurity and Infrastructure Security Agency (CISA): Офіційний веб-сайт американської агентури CISA з інформацією та рекомендаціями з кібербезпеки. [Електронний ресурс]. Режим доступу: https://www.cisa.gov 8. OWASP (Open Web Application Security Project): Ресурс, присвячений веб-додаткам та їхній безпеці, з багатьма корисними матеріалами та проектами. [Електронний ресурс]. Режим доступу: https://owasp.org 9. Cybersecurity and Technology News - Reddit:	– Навчальна програма з навчальної дисципліни „ Кіберпростір та протидія кіберзлочинності " – Робоча програма з навчальної дисципліни " Кіберпростір та протидія кіберзлочинності " – Підручники – Засоби діагностики знань студентів з навчальної дисципліни

Спільнота на Reddit, де обговорюються новини та теми з кібербезпеки. [Електронний ресурс]. Режим доступу: https://www.reddit.com/r/cybersecurity/) 10. Cybersecurity Podcasts: Є багато цікавих подкастів про кібербезпеку, такі як "Security Now," "Darknet Diaries," "CyberWire," та інші.	

13. ЗМІНИ І ДОПОВНЕННЯ ДО РОБОЧОЇ ПРОГРАМИ

№ з/п	Зміни і доповнення до робочої програми (розділ, тема, зміст змін і доповнень)	Навчальний рік	Підпис завідувача кафедри
1	2	3	4