ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____ проф. Лазур В.Ю.
"29" 04 2022 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Виявлення та попередження кіберінцидентів»

Рівень вищої освіти	**другий (магістерський)**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Освітня програма	**Безпекаінформаційних і комунікаційних систем**
Статус дисципліни	**обов'язкова**
Мова навчання	**українська**

Ужгород – 2022

Робоча програма навчальної дисципліни "**Виявлення та попередження кіберінцидентів**" для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека** освітньої програми **«Безпека інформаційних і комунікаційних систем»**.

Розробник: **Юркович Наталія Василівна**, доцент кафедри твердотільної електроніки та інформаційної безпеки, кандидат фізико-математичних наук.

Робочу програму розглянуто та затверджено на засіданні кафедри твердотільної електроніки та інформаційної безпеки

Протокол № 7 від « 28 » 04 2022 року.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету

Протокол № 10 від « 29 » 04 2022 року

Голова науково-методичної комісії факультету _____ Карбованець М.І.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 3,5</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 105</td><td>1-й</td><td></td></tr>
<tr><td>Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="6">Тижневих годин для денної форми навчання – 6,5 :

аудиторних – 2,5
самостійної роботи студента – 4</td><td>1-й</td><td></td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>18 год.</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td>24 год.</td><td>-</td></tr>
<tr><td colspan="2">Лабораторні:</td></tr>
<tr><td>Вид підсумкового контролю: іспит</td><td>-</td><td></td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>63 год.</td><td></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «**Виявлення та попередження кіберінцидентів**» є забезпечення студентів комплексними знаннями для виявлення, попередження правопорушень, вчинених із застосуванням інформаційних технологій. Основну увагу приділено підвищенню рівня загального розуміння зв'язків між злочинами, інформаційними технологіями та кіберзлочинністю і визначенню шляхів взаємодії у виявленні, попередженні та розслідувані таких злочинів.

Відповідно до Стандарту вищої освіти України для другого (магістерського) рівня спеціальності «Кібербезпека», вивчення дисципліни сприяє формуванню у здобувачів другого рівня вищої освіти таких компетентностей:

Інтегральна: Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності:

- КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
- КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
- КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

Фахові компетенції (ФК):

- КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
- КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
- КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
- КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовами вивчення навчальної дисципліни " **Виявлення та попередження кіберінцидентів** " є опанування таких навчальних дисциплін освітньої програми:

Інформаційні технології, Комп'ютерні мережі, Стеганографія, Інформаційно-комунікаційні системи.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Безпека інформаційних і комунікаційних систем»,** вивчення навчальної дисципліни **"Виявлення та попередження кіберінцидентів"** повинно забезпечити досягнення здобувачами вищої освіти таких результатів навчання (РН):

Програмні результати навчання	Шифр ПРН
Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	РН6
Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	РН8
Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	РН10
Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	РН11
Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	РН12
Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	РН15
Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	РН17
Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти	РН22

гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	
Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	РН23

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «**Виявлення та попередження кіберінцидентів**»:

Очікувані результати навчання з дисципліни	**Шифр ПРН**
Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	РН6
Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	РН8
Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	РН10
Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	РН11
Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	РН12

Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	РН15
Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	РН17
Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	РН22
Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	РН23

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання
Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

- поточний контроль успішності: стандартизовані тести, реферати, практичні роботи, презентації результатів виконаних завдань та досліджень, захист практичних робіт;
- модульні контрольні роботи;
- підсумковий контроль: іспит.

Форми поточного контролю та критерії оцінювання результатів навчання

- вибіркове усне опитування;
- фронтальне стандартизоване усне та/або письмове опитування за основними питаннями теми заняття;
- тестування;

- перевірка якості виконання завдань для самостійної роботи, зокрема за конспектами матеріалів;
- оцінювання якості та повноти виконання завдань модульної контрольної роботи;
- оцінювання якості та повноти виконання практичних робіт.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота								**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	60	**100**
5	5	5	5	5	5	5	5		

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота								**Модульна контрольна робота**	**Сума**
Т9	Т10	Т11	Т12	Т13	Т14	Т15	Т16	60	**100**
5	5	5	5	5	5	5	5		

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Практичні заняття (допуск, виконання та захист)	6	30	6	30
Поточна контрольна робота	1	10	1	10
Модульна контрольна робота		60		60
Разом		100		100

Критерії оцінювання модульної контрольної роботи

Модульна контрольна робота проводиться у письмовій формі шляхом відповідей на два теоретичні та одне практичне завдання або у виді тестів. Кожна відповідь оцінюється певною кількістю балів. Максимальна кількість балів за кожний модуль становить 100 балів. Мінімальна кількість балів, за якої робота вважається виконаною, становить 60 балів. При оцінюванні знань враховується в першу чергу повнота, правильність і вичерпність відповідей на

поставлені в модульних контрольних роботах запитання. Оцінка виставляється за 100-бальною шкалою та національною 5-бальною шкалою. Відомість результатів оформлюється за системою ECTS.

Оцінка «відмінно» виставляється, якщо під час проведення контролю було виявлено:

1. Наявність у студента всебічних, повних, глибоких інтегрованих знань програмового матеріалу, вміння вільно виконувати завдання запропонованого варіанту.
2. Вміння студента в письмовій та усній формі чітко, вичерпно і правильно викласти відповіді на питання запропонованого варіанту.
3. Глибоке розуміння студентом взаємозв'язку головних понять і положень предмета, розуміння значення цих положень і понять для майбутньої професії.
4. Високий рівень підготовленості студента з питань курсу до подальшої роботи над вдосконаленням рівня своєї професійної кваліфікації.

У відповідях студентів не має бути значних помилок. Відмінно виконана робота демонструє наявність у студента творчих здібностей.

Оцінка «добре» виставляється, коли студент письмово відповів на всі запитання, засвоїв всю навчальну програму курсу. У відповідях, які оцінені на «добре», можлива не більш як одна незначна помилка або виявлено декілька неточностей. Студент спроможний з допомогою літератури ліквідувати всі недоліки у відповідях.

Оцінка «задовільно» виставляється, коли студент дав відповіді на питання всіх завдань, але при цьому можуть проявитися певні прогалини у засвоєнні програми курсу. У відповідях, які оцінені на «задовільно», можуть зустрітися не більше як одна груба помилка або декілька значних та істотних неточностей.

Оцінка «незадовільно» виставляється за роботу, яка засвідчує про наявність у студента великих та суттєвих прогалин у знаннях основного матеріалу курсу, а у наявних його письмових відповідях є як принципові, так і грубі помилки. Студенти, які не представили письмові відповіді на модульних контрольних роботах, вважаються такими, що одержали оцінку «незадовільно».

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль з дисципліни здійснюється у формі іспиту. Іспит проводиться в усній формі шляхом співбесіди. Підсумкова оцінка визначається наступними критеріями:

Оцінки «відмінно» (А) заслуговує студент, який виявив всебічне і глибоке знання програмового матеріалу, вміння вільно виконувати завдання, передбачені програмою, засвоїв основну і ознайомився з додатковою літературою, розуміє взаємозв'язок головних понять дисципліни та їх значення для майбутньої професії.

Оцінки «дуже добре» (В) заслуговує студент, що виявив повне знання програмового матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу, рекомендовану програмою, виявив систематичний характер знань з дисципліни і здатний до їх самостійного поповнення, але під час відповіді допустив незначні неточності.

Оцінки «добре» (C) заслуговує студент, що виявив повне знання програмового матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу, рекомендовану програмою, виявив систематичний характер знань з дисципліни і здатний до їх самостійного поповнення, але під час відповіді допустив неточності і помилки.

Оцінки «задовільно» (D) заслуговує студент, що виявив знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, оцінка «задовільно» виставляється студентам, що допустили помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення.

Оцінки «достатньо» (E) заслуговує студент, що виявив знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, оцінка «достатньо» виставляється студентам, що допустили грубі помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення за допомогою викладача.

Оцінка «незадовільно» (FX) виставляється студенту, який виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань. Студенти, які не з'явилися на екзамен без поважних причин, вважаються такими, що одержали незадовільну оцінку.

Оцінка «неприйнятно» (F) виставляється студенту, не виконав повністю план навчальної дисципліни, виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань, не виявив знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією.

За бажанням студента результуюча підсумкова оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль. Переведення результатів, отриманих за 100-бальною шкалою оцінювання в національну 4-х бальну та шкалу за системою ECTS здійснюється за наступною схемою:

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		Екзамен та диференційований залік	Залік
90 – 100	**A**	відмінно	Зараховано
82-89	**B**	добре	
74-81	**C**		

64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	Не зараховано

Результати підсумкового контролю знань вносяться до відомості обліку успішності.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1

Тема 1. Головні тенденції застосування інформаційних технологій у правопорушеннях: (відео-шоу, облікові записи у соцмережах, спеціально створені сайти, працевлаштування, skype, viber). Стадії правопорушень та відповідні технології на цих стадіях

Тема 2. Основні оператори мови запитів Google для пошуку інформації. Перелік утиліт для пошуку в мережі інформації про комп'ютер, стани каналів зв'язку, маршрут руху пакетів, доменні імена та IP-адреси.

Тема 3. Сервіси для ідентифікації , збір інформації доменного імені та хостингу. Аналіз повних заголовків електронного листа та його розшифровка.

Тема 4. Сервіси для встановлення відомостей про одержувача електронного листа (дата і час прочитання повідомлення, IP-адресу, з якої повідомлення було прочитано). Мультимедійні засоби спілкування.

Тема 5. Способи ідентифікації співрозмовників Skype, Viber, Jabber і т.д. Технології забезпечення анонімності та безпечної передачі інформації у мережі.

Тема 6. Порядок роботи TOR мережі. Принцип роботи I2P мережі.

Тема 7. Шифрування інформації. Засоби стеганографічних перетворень. Спеціальне програмне забезпечення для приховування інформації. WinHex. Приховування інформації з використанням альтернативних потоків.

Тема 8. Хмарні сховища.

Модуль 2

Тема 9. Протокол передачі даних FTP.□Комп'ютерна мережа Peer-to-Peer (P2P).

Тема 10. Інтернет орієнтовані платіжні системи. Платіжні системи банківських карт.

Тема 11. Платіжні системи електронних гаманців. Платіжні системи посередників.

Тема 12. Огляд стандартних засобів комп'ютерної техніки. Перелік запитань для експертного дослідження.

Тема 13. Дослідження даних операційної системи з метою виявлення доказової інформації. Сервіси для аналізу зображень, завантажених з мережних ресурсів.
Тема 14. Огляд мобільних засобів комп'ютерної техніки з функцією телефону. Програмне забезпечення для мобільного пристрою.
Тема 15. Взаємодія правоохоронних органів на національному рівні. Міжнародна взаємодія з використанням інформаційних технологій.
Тема 16. Структура Генерального секретаріату Інтерполу. Проекти, в рамках яких Україна взаємодіє з Генеральним секретаріатом Інтерполу.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Усього	у тому числі				
		лекції	практичні	лабораторні	індивідуальна робота	самостійна робота
Модуль 1						
Тема 1. Головні тенденції застосування інформаційних технологій у правопорушеннях: (відео-шоу, облікові записи у соцмережах, спеціально створені сайти, працевлаштування, skype, viber). Стадії правопорушень та відповідні технології на цих стадіях	8	2	2	-		4
Тема 2. Основні оператори мови запитів Google для пошуку інформації. Перелік утиліт для пошуку в мережі інформації про комп'ютер, стани каналів зв'язку, маршрут руху пакетів, доменні імена та IP-адреси.	8	2	2	-		4
Тема 3. Сервіси для ідентифікації , збір інформації доменного імені та хостингу. Аналіз повних заголовків електронного листа та його розшифровка.	7	1	2	-		4
Тема 4. Сервіси для встановлення відомостей про одержувача електронного листа (дата і час прочитання повідомлення, IP-адресу, з якої повідомлення було прочитано). Мультимедійні засоби спілкування.	6	1	1	-		4
Тема 5. Способи ідентифікації співрозмовників Skype, Viber, Jabber і т.д.	6	1	1	-		4

Технології забезпечення анонімності та безпечної передачі інформації у мережі.						
Тема 6. Порядок роботи TOR мережі. Принцип роботи I2P мережі.	6	1	1	-		4
Тема 7. Шифрування інформації. Засоби стеганографічних перетворень. Спеціальне програмне забезпечення для приховування інформації. WinHex. Приховування інформації з використанням альтернативних потоків.	7	1	2			4
Тема 8. Хмарні сховища.	6	1	1			4
Разом за модулем 1	**54**	**10**	**12**			**32**
Модуль 2						
Тема 9. Протокол передачі даних FTP.Комп'ютерна мережа Peer-to-Peer (P2P).	10	1	2			4
Тема 10. Інтернет орієнтовані платіжні системи. Платіжні системи банківських карт.	12	1	2			4
Тема 11. Платіжні системи електронних гаманців. Платіжні системи посередників.	10	1	1			4
Тема 12. Огляд стандартних засобів комп'ютерної техніки. Перелік запитань для експертного дослідження.	12	1	1			4
Тема 13. Дослідження даних операційної системи з метою виявлення доказової інформації. Сервіси для аналізу зображень, завантажених з мережних ресурсів.	6	1	1			4
Тема 14. Огляд мобільних засобів комп'ютерної техніки з функцією телефону. Програмне забезпечення для мобільного пристрою.	10	1	2			4
Тема 15. Взаємодія правоохоронних органів на національному рівні. Міжнародна взаємодія з використанням інформаційних технологій.	6	1	1			4
Тема 16. Структура Генерального секретаріату Інтерполу. Проекти, в рамках яких Україна взаємодіє з Генеральним секретаріатом Інтерполу.	10	1	2			3
Разом за модулем 2	**51**	**8**	**12**			**31**
Усього годин	**105**	**18**	**24**			**63**

6.3. Теми практичних занять

№	Назва теми	Кількість годин
1	Основні оператори мови запитів Google для пошуку інформації	2
2	Перелік утиліт для пошуку в мережі інформації про комп'ютер, стани каналів зв'язку, маршрут руху пакетів, доменні імена та IP-адреси	2
3	Сервіси для ідентифікації та збір інформації доменного імені та хостингу	2
4	Схема маршрут руху листа від відправника до одержувача. Сервіси встановлення відомостей про одержувача електронного листа (дата і час прочитання повідомлення, IP-адресу, з якої повідомлення було прочитано).	2
5	Способи ідентифікації співрозмовників Skype, Viber, Jabber і т.д.	2
6	Шифрування інформації. Засоби стеганографічних перетворень. Спеціальне програмне забезпечення для приховування інформації.	2
7	WinHex. Можливості програми та її застосування. Приховування інформації з використанням альтернативних потоків.	2
8	Інтернет орієнтовані платіжні системи. Ідентифікувати банк-емітент карти.	2
9	Складання запитів до різних служб згідно поданих додатків	2
10	Огляд стандартних засобів комп'ютерної техніки. Перелік запитань для експертного дослідження.	2
11	Дослідження даних операційної системи з метою виявлення доказової інформації.	2
12	Сервіси для аналізу зображень, завантажених з мережних ресурсів	2
	Разом	**24**

6.4. Самостійна робота

№	Назва роботи	Кількість годин
1	Проробка лекційного матеріалу.	20
2	Підготовка до практичних занять, обробка та	30

	оформлення результатів	
3	Проробка питань програми, які не викладались на лекціях	5
4	Виконання домашніх завдань	8
	Разом	**63**

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби: мультимедійний проектор
Обладнання: персональні комп'ютери, мобільні телефони, доступ в Інтернет.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41.
2. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03.08.2017
3. Про національну безпеку України : Закон України від 21.06.2018 № 2496-VIII // База даних «Законодавство України» / Верховна Рада України.
4. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : АртЕк, 2018. 422 с.
5. Українська кіберполіція: протистояти найнебезпечнішим хакерам світу // Українська правда : сайт. 20.10.2019.
6. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5–6.
7. Про затвердження Положення про Департамент кіберполіції Національної поліції України : Наказ Нац. поліції України від 10.11.2015 № 85
8. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Рішення Ради нац. безпеки і оборони України від 01.05.2014 № 449/2014. *Урядовий кур'єр*. 2014. № 81.
9.Бандурка О. М., Литвинов О. М. Протидія злочинності та профілактика злочинів : монографія. Харків : ХНУВС, 2011. 308 с.
10.Про протидію торгівлі людьми : Закон України від 20.09.2011 № 3739-VI // База даних «Законодавство України» / Верховна Рада України.
11.Підготовка працівників структурних підрозділів Національної поліції України у частині забезпечення та захисту прав дітей. Частина 1. : навч.-метод. посіб. / за заг. ред. Т. В. Журавель, Л. В. Зуб, О. В. Ковальова, Ю. В. Пилипас. Київ : ФОП Буря О. Д., 2019. 515 с.

Додаток 2

Результати перегляду

робочої програми навчальної дисципліни

Робоча програма перезатверджена на 20____/ 20____н.р. без змін; зі змінами (Додаток____).

потрібне підкреслити)

протокол №____від «____»_____20____р. Завідувач кафедри _____

(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20____/ 20____н.р. без змін; зі змінами (Додаток____).

(потрібне підкреслити)

протокол №____від «____»_____20____р. Завідувач кафедри _____

(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20____/ 20____н.р. без змін; зі змінами (Додаток____).

(потрібне підкреслити)

протокол №____від «____»_____20____р. Завідувач кафедри _____

(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20____/ 20____н.р. без змін; зі змінами (Додаток____).

(потрібне підкреслити)

протокол №____від «____»_____20____р. Завідувач кафедри _____

(підпис) (Прізвище ініціали)