***МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ***

***ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА***

**Кафедра безпеки інформації та бізнес-комунікацій**

“**ЗАТВЕРДЖУЮ**”

Завідувач кафедри безпеки інформації та бізнес-комунікацій

д.е.н. проф. Хмелярчук

11. 01. 2023 р.

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ СУЧАСНІ ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

|  |  |
| --- | --- |
| **рівень вищої освіти** | другий  *перший (бакалаврський) / другий (магістерський)* |
| **галузь знань** | 05 Соціальні та поведінкові науки  *шифр і назва* |
| **спеціальність**  **освітня програма** | 051 Економіка  «Економіка та безпека інформації» |
| **статус дисципліни** | Обов’язкова  *обов’язкова / вибіркова /* |
| **факультет** | економічний |

2022 – 2023 навчальний рік

Робоча програма нормативної навчальної дисципліни «Сучасні технології інформаційної безпеки» для студентів першого курсу другого (магістерського) рівня вищої освіти зі спеціальності 051 «Економіка», спеціалізація «Економіка та безпека інформації». Львів: Львівський національний університет імені Івана Франка, 2023.

- 20 с.

Розробник: Шевчук Тетяна Віталіївна, доцент кафедри безпеки інформації та бізнес комунікацій, к.е.н., доцент

Робочу програму схвалено на засіданні кафедри безпеки інформації та бізнес комунікацій

Протокол від 11 січня 2023 р. № 6

**Завідувач кафедри безпеки інформації та бізнес комунікацій**

**\_ д. е. н., проф. Хмелярчук М.І.**

11 січня 2023 р.

Шевчук Т.В., 2023 р.

1. **Опис навчальної дисципліни**

|  |  |  |  |
| --- | --- | --- | --- |
| *Найменування показників* | *Галузь знань, напрям підготовки, освітньо- кваліфікаційний рівень* | *Характеристика навчальної дисципліни* | |
| **денна форма**  **навчання** | **заочна форма**  **навчання** |
| **Кількість кредитів** – 4 | **Галузь знань:**  05 **–** соціальні та поведінкові науки | Нормативна | |
|  |
| **Модулів** – 1 | **Спеціальність**: 051 Економіка | **Рік підготовки:** | |
| **Змістових модулів** – 2 | 1-й | -й |
| **Індивідуальне науково-дослідне завдання:** | **Семестр** | |
| **Загальна кількість годин** – 120 | 2-й | -й |
| **Лекції** | |
| **Тижневих годин для денної форми**  **навчання: аудиторних** – 4  **самостійної роботи студента** – 4 | **Освітній ступінь**: бакалавр | 16 год. | год. |
| **Практичні, семінарські** | |
| год. | год. |
| **Лабораторні** | |
| 32 год. | – год. |
| **Самостійна робота** | |
| 72 год. | год. |
| **Індивідуальні завдання:**  год. | |
| **Вид контролю**: залік | |

**Примітка**.

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:

для денної форми навчання – 0,66 для заочної форми навчання –

1. **Мета та завдання навчальної дисципліни**

**Метою** вивчення нормативної навчальної дисципліни ***«Сучасні технології інформаційної безпеки»*** є формування знань щодо сутності інформаційної безпеки як складного багаторівневого явища, що має соціальні, психологічні й технічні виміри; засвоєння студентами сучасних методів захисту інформації (зокрема технічного, інженерного, криптографічного та організаційного); вивчення нормативно-законодавчої бази України щодо захисту інформації; придбання практичних навичок реалізації захисту персональних даних в процесі введення, виведення, передавання, оброблення, накопичення і зберігання; застосування заходів та засобів, спрямованих на технічний захист інформації на об’єктах інформаційної діяльності.

Це дасть змогу підготувати висококваліфікованих і конкурентоспроможних фахівців, які володіють сучасним мисленням, теоретичними знаннями з виявлення і протидії інформаційним загрозам на рівні людини, суспільства та держави; навичками застосування методів та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Основними **завданнями** вивчення дисципліни є: формування у майбутніх фахівців знань про інформаційну безпеку та захист інформації; вивчення принципів забезпечення конфіденційності інформації; виявлення програми з потенційно небезпечними наслідками; дослідження засобів захисту інформації від стороннього втручання, пошкодження чи знищення; виявлення технічних каналів витоку інформації; здобуття практичних навичок із захисту інформаційних і комунікаційних систем.

**Компетентності:**

В результаті вивчення дисципліни студент набуває:

*Загальні компетентності (ЗК):*

|  |
| --- |
| ЗК1. Здійснювати аналіз та узагальнення інформації, що підлягає захисту. |
| ЗК2. Застосовувати технології, методи та засоби захисту інформації з метою  уникнення її пошкодження чи знищення. |

*Спеціальні (фахові) компетентності (СК):*

СК1. Здатність до аналізу та узагальнення інформації щодо захисту від несанкціонованого доступу.

СК2. Вміння організовувати представлення інформації з положень законодавства в галузі захисту інформації.

СК3. Здатність систематизації методів захисту інформації для підвищення рівня безпеки інформації.

СК4. Здатність виконувати адміністрування доступу до комп’ютерних систем з метою призначення невиправданих привілей.

СК5. Вміння проводити програмний захист комп’ютерних систем від вірусів, хакерських атак, комерційного шпигунства.

СК6. Здатність до виконання моніторингу з пошуку каналів витоку інформації.

***Вимоги до знань та вмінь.***

**Студент повинен:**

**знати:** понятійний апарат дисципліни, зокрема «інформаційна безпека»,

«захист інформації», «ідентифікація і аутентифікація», «конфіденційність інформації», «несанкціонований доступ», «комп’ютерні віруси», «цифровий підпис»; правові та організаційні основи забезпечення інформаційної безпеки України; основні види загроз інформаційній безпеці та технічних каналів витоку інформації; методи їх виявлення та блокування; принципи побудови систем захисту інформації; сучасні способи боротьби з несанкціонованим доступом, копіюванням, зміною і збором інформації; основні види вірусів та способи хакерських атак з метою знищення чи пошкодження інформації; основні методи та засоби криптографічного захисту інформації, що циркулює у автоматизованих системах та передається телекомунікаційними каналами та мережами; алгоритми шифрування даних і проведення їх порівняльного аналізу при створенні ефективної системи захисту інформації.

**вміти:**

* розпізнавати методи несанкціонованого доступу до інформації
* планувати й організовувати роботу щодо створення та розвитку системи інформаційної безпеки на підприємстві;
* організовувати роботу щодо виявлення і блокування технічних каналів витоку інформації;
* організовувати ефективний контроль робіт із захисту інформації;
* здійснювати ефективний вибір інформаційних технологій захисту;
* свідомо дотримуватися правил роботи з інформацією з обмеженим доступом та суворо виконувати вимоги до захисту інформації, що діють у системі державного управління України;
* використовувати програмні та апаратні засоби розмежування доступу до інформації в автоматизованих системах;
* застосовувати антивірусні засоби захисту інформації у персональних комп’ютерах;
* застосовувати елементарні методи цифрового шифрування, симетричні системи захисту інформації, криптографічні системи з відкритим ключем.

Програмні результати навчання:

|  |
| --- |
| **ПРН1.** Використовувати спеціальні технічні засоби захисту інформації. |
| **ПРН 2.** Створювати ефективну систему захисту інформації. |
| **ПРН 3.** Працювати у корпоративних інформаційних системах. |
| **ПРН 4.** Систематизувати методи захисту даних і комп’ютерних систем. |

|  |
| --- |
| **ПРН5.** Представляти та подавати інформацію згідно вимог правових та  нормативних актів. |
| **ПРН 6.** Застосовувати основні прийоми та програмні засоби захисту від вірусів та  комерційного шпигунства для підвищення надійності захисту інформації.. |

1. **Програма навчальної дисципліни**

***Змістовий модуль 1. Основи інформаційної безпеки***

**Тема 1. Роль інформації в сучасному інформаційному суспільстві та значення інформаційної безпеки**

Інформаційне суспільство та інформація. Властивості інформації з точки зору її захисту. Інформація як зброя. Інформаційне протиборство та інформаційна війна. Гібридна війна.

Базові поняття щодо інформаційної безпеки. Взаємозв’язок інформаційної безпеки, захисту інформації та кібербезпеки.

Міжнародні стандарти в сфері захисту інформації (Світові стандарти із захисту даних в комп'ютерних системах. Державний стандарт України із захисту інформації).

# Тема 2. Інформаційна безпека як складова системи національної безпеки держави

Концептуальні засади забезпечення інформаційної безпеки України (Концепція національної безпеки України, концепція інформаційної безпеки України, доктрина інформаційної безпеки України). Нормативно-правові основи інформаційної безпеки. Аналіз основних положень законодавства в галузі захисту інформації. Державні органи, що забезпечують інформаційну безпеку.

Поняття державної таємниці та її правовий захист. Конфіденційна інформація. Комерційна таємниця та її правовий захист.

Персональні дані та захист приватності: захист персональних даних; співвідношення: конфіденційна інформація, інформація про особу та персональні дані.

Захист авторських прав. Знак охорони авторського права. Види авторських прав в Інтернеті. Чому потрібно захищати авторські права. Приклади порушення авторського права у різних галузях і подіях.

# Тема 3. Загрози інформаційній безпеці

Характеристика загроз безпеки інформації. Класифікація загроз безпеки інформації. Класифікація загроз безпеки за засобами впливу на систему.

Комп'ютерні віруси та їх особливості. Класифікація вірусів. Основні види вірусів і схеми їх функціонування. Шляхи проникнення вірусів у комп'ютер і механізм розподілу вірусних програм. Ознаки появи вірусів.

Джерела загроз безпеці інформаційного суспільства, особистості і держави. Організація каналів витоку інформації: несанкціонований доступ (НСД); канали витоку конфіденційної інформації.

Порушники безпеки; категорії осіб, у числі яких може виявитися порушник; дії порушників безпеки інформації; аналіз спроб зловмисного проникнення в комп'ютерні системи.

# Тема 4. Загрози інформаційній безпеці в інформаційно- комунікаційних мережах

Інформаційна безпека в мережі Інтернет, еволюція загроз інформаційної безпеки, вплив Інтернет на розвиток шкідливих програм. Види шахрайства в мережі Інтернет, шляхи захисту від шахрайства у мережі інтернет.

Сучасні загрози інформаційній безпеці. Кібербезпека в умовах гібридної війни. Кібернетичні загрози, DDoS-атаки, шкідливе програмне забезпечення.

Комп’ютерна злочинність як загроза інформаційній безпеці. Технічні пристрої для здійснення кібершахрайства.

Загрози інформаційній безпеці, які виникають унаслідок користування мобільними пристроями.

# Тема 5. Соціальна інженерія як сучасна загроза інформаційній безпеці

Загальне визначення терміну «соціальна інженерія». Соціальна інженерія як технологія маніпулювання свідомістю.

Історія виникнення соціальної інженерії, основоположники цього поняття.

Заборонені методи маніпулювання людьми.

Основні методи соціальної інженерії, які застосовують зловмисники та методи захисту від них. Основні ознаки атаки за допомогою соціальної інженерії. Захист від загроз, основою яких є соціальна інженерія.

***Змістовий модуль 2. Сучасні методи і технології забезпечення інформаційної безпеки***

**Тема 6. Поняття, сутність і принципи захисту інформації**

Шляхи забезпечення безпеки інформації. Рівні забезпечення безпеки інформації.

Організація системи захисту інформації: політика безпеки інформації, значення політики безпеки інформації для національної безпеки, побудова

системи захисту інформації, законодавче регулювання політик ІБ, комплекс задач, які вирішуються при розробці політики безпеки.

Складові політики інформаційної безпеки. Ідентифікація і аутентифікація користувачів: біометрична ідентифікація й аутентифікація користувача; перваги біометричних методів ідентифікації й аутентифікації користувача в порівнянні з традиційними, приклади; нормативно-правове забезпечення застосування біометричних параметрів при ідентифікації суб'єктів доступу до автоматизованих систем.

Засоби захисту даних від комп'ютерних вірусів та їх особливості.

Виявлення вірусів і шкідливих програм та їх усунення.

Захист даних від несанкціонованого доступу (НСД). Технічні засоби заходи захисту даних від їх витоку.

# Тема 7. Забезпечення інформаційної безпеки підприємницької діяльності

Сутність та місце інформаційної безпеки у системі економічної безпеки підприємства: структура процесу організації інформаційної безпеки суб’єкта підприємництва; загрози безпеці підприємницької діяльності; інформаційна безпека підприємства; організація безпеки в роботі з персоналом підприємства; промислове шпигунство в підприємницькій діяльності.

Безпека Інтернет-банкінгу в Україні: небезпеки, які можуть підстерігати користувачів онлайн банкінгу, заходи для забезпечення безпечного користування інтернет-банкінгом, системи безпеки Інтернет-банкінгу, що використовуються найбільшими українськими банками.

Інформаційна безпека ведення електронного бізнесу.

Загрози інформаційній безпеці, які виникають унаслідок користування мобільними пристроями.

# Тема 8. Основи криптографічного захисту інформації

Основні положення та визначення. Криптографічні методи захисту інформації. Сучасні криптосистеми та їх особливості. Класичні техніки шифрування. Симетричні та асиметричні алгоритми шифрування інформації. Цифрові підписи. Адміністрування ключами.

1. **Структура навчальної дисципліни**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Назва змістових модулів і тем | |  | Кількість годин | | | | | | | | | | |
|  | Денна форма | | | | | | Заочна  форма | | | | |
| Всього | Лекції | Практичні | | Лабораторні | Індивідуальні | Самостійна робота | Лекції | Практичні | Лабораторні | Індивідуальні | Самостійна робота |
| **Змістовий модуль 1. Основи інформаційної безпеки** | | | | | | | | | | | | | |
| Тема 1. Роль інформації в  сучасному інформаційному суспільстві та значення  інформаційної безпеки | | 14 | 2 | |  | 4 | - | 8 | - | - | - | - | - |
| Тема 2. Інформаційна безпека  як складова системи  національної безпеки держави | | 14 | 2 | |  | 4 | - | 8 | - | - | - | - | - |
| Тема 3. Загрози  інформаційній безпеці | | 14 | 2 | |  | 4 | - | 8 | - | - | - | - | - |
| Тема 4. Загрози  інформаційній безпеці в інформаційно-комунікаційних мережах | | 14 | 2 | |  | 4 | - | 8 | - | - | - | - | - |
| Тема 5. Соціальна інженерія  як сучасна загроза інформаційній безпеці | | 14 | 2 | |  | 4 |  | 8 |  |  |  |  |  |
| Разом за змістовим модулем 1 | | 70 | 10 | |  | 20 |  | 40 |  |  |  |  |  |
| **Змістовий модуль 2. Сучасні методи і технології забезпечення інформаційної безпеки** | | | | | | | | | | | | | |
| Тема 6. Поняття, сутність і  принципи захисту інформації | | 16 | 2 | |  | 4 |  | 10 |  |  |  |  |  |
| Тема 7. Забезпечення  інформаційної безпеки підприємницької діяльності | | 16 | 2 | |  | 4 | - | 10 | - | - | - | - | - |
| Тема 8. Основи криптографічного захисту  інформації | | 17 | 2 | |  | 4 | - | 11 | - | - | - | - | - |
| Разом за змістовим модулем 2 | | 49 | 6 | |  | 12 | - | 31 | - | - | - | - | - |
| Усього: | | 119 | 16 | |  | 32 |  | 71 | - | - | - | - | - |
| Підсумковий контроль:  залік | |  | 1 | | | | | |  | | |  | |
| Разом: | Годин |  | 120 | | | | | |  | | |  | |
| Кредитів |  | 4 | | | | | |  | | |  | |

1. **Теми семінарських занять (немає)**
2. **Теми практичних занять (немає)**
3. **Теми лабораторних занять**

|  |  |  |
| --- | --- | --- |
| **№**  **теми** | **Назва теми** | **Кількість**  **годин** |
| Тема 1. | Роль інформації в сучасному інформаційному  суспільстві та значення інформаційної безпеки. | 4 |
| Тема 2. | Інформаційна безпека як складова системи національної  безпеки держави. | 4 |
| Тема 3. | Загрози інформаційній безпеці. | 4 |
| Тема 4. | Загрози інформаційній безпеці в інформаційно-  комунікаційних мережах. | 4 |
| Тема 5. | Соціальна інженерія як сучасна загроза інформаційній  безпеці. | 4 |
| Тема 6. | Поняття, сутність і принципи захисту інформації. | 4 |
| Тема 7. | Забезпечення інформаційної безпеки підприємницької  діяльності. | 4 |
| Тема 8. | Основи криптографічного захисту інформації. | 4 |
|  | ***Разом*** | ***32*** |

1. **Самостійна робота**

|  |  |  |
| --- | --- | --- |
| **№**  **теми** | **Назва теми** | **Кількість**  **годин** |
| Тема 1. | Інформаційне протиборство, інформаційні війни,  гібридна війна. | 8 |
| Тема 2. | Інформаційна безпека у контексті забезпечення національної безпеки України, пріоритетні напрямки  державної політики в інформаційній сфері. | 8 |
| Тема 3. | Оцінювання наслідків реалізації загроз у сфері  інформаційної безпеки для життєдіяльності окремої особистості, груп людей, організацій та держави. | 8 |
| Тема 4. | Види шахрайства в мережі Інтернет. Шахрайство з  електронною поштою. Спамінг. | 8 |
| Тема 5. | Використання маніпулятивних прийомів впливу на  індивідуальну та масову свідомість | 8 |
| Тема 6. | Захист приватності в повсякденному житті та  професійній діяльності. | 10 |
| Тема 7. | Загрози безпеки підприємницької діяльності. | 10 |

|  |  |  |
| --- | --- | --- |
| Тема 8. | Криптографічні методи захисту інформації. Сучасні  криптосистеми та їх особливості. Класичні техніки. шифрування | 11 |
|  | ***Разом*** | ***71*** |

Для активізації студентів до самоосвіти та самовиховання важливим завданням викладача є навчання методиці самостійного дослідження та опанування матеріалу. Головною метою самостійної роботи є закріплення, розширення та поглиблення набутих у процесі аудиторної роботи знань, вмінь та навичок, а також самостійне вивчення та засвоєння нового матеріалу під керівництвом викладача, але без його безпосередньої участі. Самостійна робота студентів з дисципліни «Сучасні технології інформаційної безпеки» включає: – опрацювання теоретичних основ прослуханого лекційного матеріалу; – вивчення окремих тем, що передбачені для самостійного опрацювання; – вирішення та письмове оформлення задач і ситуаційних вправ; – виконання індивідуальних завдань; – підготовка до семінарських (практичних) занять; – підготовка до контрольних робіт; – виконання домашніх завдань. Викладач на самостійне опрацювання студентам виносить ті питання з тем програми курсу, що не розглядалися на лекціях. Зміст таких питань та перелік необхідної літератури викладач визначає в індивідуальному порядку та повідомляє студентам на лекціях.

1. **Індивідуальні завдання (немає)**
2. **Методи навчання**

*Лекції:* Передбачають систематичний і послідовний виклад навчального матеріалу, а також інтерактивні форми участі студентів в обговоренні дискусійних питань. Види лекційних занять: оглядова лекція, проблемна лекція.

*Практичні заняття*: Відвідування та активна участь студентів у роботі практичних занять є обов’язковою умовою успішного складання курсу. Пропонуються наступні *методи навчання:*

* метод практичного засвоєння курсу з допомогою складання тестових завдань, вирішення задач та ситуацій з метою набування умінь і практичних навичок (практичні заняття);
* метод модульного контролю з допомогою періодичного складання модулів за тематикою лекційних та практичних занять;
* метод самостійного засвоєння студентами навчального матеріалу у вигляді складання тестів, вирішення задач та ситуацій, написання рефератів на підставі самостійно опрацьованої базової літератури та додаткових джерел інформації (в т.ч. законодавчих актів) з метою конкретизації й поглиблення базових знань, необхідних умінь та практичних навичок (самостійна робота);
* методи усного та письмового контролю (практичні заняття та самостійна робота);
* кейс-метод;
* семінар-дискусія, семінар-розгорнута бесіда;
* бліц опитування;
* дискусія з елементами аналізу;
* презентація-обговорення;
* вирішення ситуаційних завдань.

1. **Методи контролю**

До методів поточного контролю засвоєння знань студентами упродовж семестру належать:

* *результати виконання лабораторних робіт, завдань поточного контролю;*
* *відповіді на практичних заняттях,* систематичність та активність роботи на практичних заняттях;
* *усна презентація як різновид індивідуального науково-дослідного завдання*;
* виконання *модульних (контрольних) завдань* за матеріалами кожного змістовного модуля;
* *підсумкова контрольна робота наприкінці семестру* за матеріалами усіх змістовних модулів.

Підсумкове оцінювання знань студентів здійснюється за поточним та проміжним контролем знань протягом семестру. З метою перевірки якості підготовки, знань, умінь студента з дисципліни використовуються такі засоби оцінювання:

1. для *поточного контролю*:
   * стандартизовані тести;
   * поточне опитування;
   * наскрізні проекти; командні проекти;
   * аналітичні звіти, реферати, есе;
   * розрахункові та розрахунково-графічні роботи;
   * презентації результатів виконаних завдань та досліджень;
   * студентські презентації та виступи на наукових заходах;
   * розрахункові роботи;
   * завдання на тренажерах, реальних об’єктах, тощо;
   * інші види індивідуальних та групових завдань.
2. для *проміжного контролю* – проведення модульного контролю, що включають тестування, теоретичні питання.

Розподіл балів які може накопичувати студент при вивченні дисципліни

«Сучасні технології інформаційної безпеки», наведено в таблиці 1.

Таблиця 1

|  |  |  |
| --- | --- | --- |
| Форми контролю | Максимальна кількість балів | |
| Денна форма навчання | Заочна  (дистанційна) форма навчання |
| Поточний контроль: |  |  |
| Розрахункова робота | 20 балів |  |
| Тестування | 2 х 10 балів = 20 балів |  |
| Тези та виступ на науковій конференції | до 20 балів |  |
| Презентація та захист індивідуальних (дослідницько-аналітичних) робіт | 20 балів |  |
| Модульна контрольна робота | 20 балів |  |
| Всього за результатами поточного контролю: | 100 |  |
|  |  |  |
| Всього | 100 |  |

Форма **підсумкового контролю** за навчальною дисципліною «Сучасні технології інформаційної безпеки» – **залік**.

У кінцевому підсумку студент може набрати **100 балів.**

1. **Розподіл балів, які отримують студенти**

Оцінювання знань студента здійснюється за 100-бальною шкалою. Максимальна кількість балів при оцінюванні знань студентів з даної дисципліни, яка завершується заліком, становить за поточну успішність 100 балів. При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань студентів за різними системами:

**Шкала оцінювання: національна та ECTS**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Оцінка в балах*** | ***Оцінка ECTS*** | ***За національною шкалою*** | |
| ***Екзаменаційна оцінка, оцінка з***  ***диференційованого заліку*** | ***Залік*** |
| 90 – 100 | А | *Відмінно* | *Зараховано* |
| 81-89 | В | *Добре* |
| 71-80 | С |
| 61-70 | D | *Задовільно* |
| 51-60 | Е |
| 0-50 | FX | *Незадовільно з можливістю повторного складання* | *Не зараховано з можливістю повторного*  *складання* |

1. **Рекомендована література**

**Базова;**

1. Остроухов В. В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М. Інформаційна безпека. Підручник під ред. В. В. Остроухова. К.: Видавництво Ліра-К., 2021. 412 с.
2. Гур’єв В.І., Мехед Д.Б., Ткач Ю.М., Фірсова І.В. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека». Ніжин: ФОП Лук’яненко В.В. ТПК

«Орхідея», 2018. 166 с. : іл.

1. Голобородько А.Ю., Гусєва О.Ю., Легомінова С.В. Цифрова економіка: підруч., Київ: Видавництво ДУТ, 2020. 400 с.
2. Поліщук В.В.Програмні технології захисту інформації: конспект лекцій для студентів за напрямом підготовки 6.050103 «Програмна інженерія» факультету інформаційних технологій УжНУ. Ужгород: 2018. 80 с.
3. Войціховський, А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісник Харківського національного університету імені В.Н. Каразіна. Сер.: Право. 2020. Вип. 29. С. 281-288.
4. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико–правові та організаційні аспекти. НАПрН України, НДІІП, НАН України, Нац. б–ка України ім. В. І. Вернадського. Київ, 2015. 388 с.
5. Макаренко Є. А., Рижиков М. М., Ожеван М. А. Міжнародна інформаційна безпека: сучасні виклики та загрози. К. : Центр вільної преси, 2006. - 916 с.
6. Петрик В.М. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: навчальний посібник. К. : Росава, 2006. 208 с.
7. Інформаційна безпека (соціально-правові аспекти): Підручник / Остроухов В. В., Петрик Б. М., Прнсяжнюк М. М. та ін. ; за заг - ред. Є. Д. Скулиша. К. : КНТ, 2010. 776 с.
8. Зубок М.І. Інформаційна безпека в підприємницькій діяльності. К.: ГНОЗІС, 2015 216 с.
9. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека. Навчальний посібник. Харків: Вид. ХНЕУ, 2000. 352 с.

**Допоміжна**

1. Четверик Г. Г. Напрямки реалізації державної політики у сфері кібернетичної безпеки / Г. Г. Четверик // Вісник Дніпропетровського університету. 2012. Вип 22. C. 240-245.
2. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. Вид. 2- доп. і перероб. К.: Текст, 2008. 400 с.
3. Ліпкан В. А. Національна безпека України: [навчальний посібник] / В. А. Ліпкан. [2-ге вид.]. К. : КНТ, 2009. 576 с.
4. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : [навчальний посібник] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. К. : КНТ, 2006. 280 с.

**14. Інформаційні ресурси**

1. Законодавство України. Офіційний портал Верховної Ради. URL:www/ <http:///www.rada.gov.ua>
2. Проект Концепція інформаційної безпеки України [Електронний ресурс]. URL: <http://www.osce.org/uk/fom/175056?download=true>
3. Стратегія кібербезпеки України від 15.03.2016 р. [Електронний ресурс]. URL: <http://zakon3.rada.gov.ua/laws/show/96/2016>
4. Діордіца І. В. Поняття та зміст кіберзлочинності. URL: [http://goal-](http://goal-/) int.org/ponyattya-ta-zmist-kiberzlochinnosti/
5. Діордіца І. В. Сучасний кібертероризм: аспекти правового регулювання. URL: <http://goal-int.org/suchasnij-kiberterorizm-aspekti-> pravovogo-regulyuvannya/
6. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення. URL: <http://goal-int.org/sistema-zabezpechennya-kiberbezpeki-> sutnist-ta-priznachennya/
7. Діордіца І. В. Поняття та зміст кіберзагроз на сучасному етапі. URL: <http://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-> suchasnomu-etapi/
8. Діордіца І. В. Кібертероризм як елемент дестабілізації системи стратегічних комунікацій. URL: [http://goal-int.org/kiberterorizm-yak-elementi- destabilizacii-sistemi-strategichnix-komunikacij/](http://goal-int.org/kiberterorizm-yak-elementi-destabilizacii-sistemi-strategichnix-komunikacij/)
9. Діордіца І. В. Поняття та зміст кібершпигунства. URL: [http://goal-](http://goal-/) int.org/ponyattya-ta-zmist-kibershpigunstva/