**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**

**«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

Кафедра права

(назва кафедри, яка забезпечує викладання дисципліни)

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві**

( назва навчальної дисципліни)

рівень вищої освіти перший (бакалаврський)

перший (бакалаврський) / другий (магістерський)

галузь знань 03 Гуманітарні науки

(шифр і назва)

Спеціальність 035 Філологія

(шифр і назва )

освітня програма Прикладна та комп’ютерна лінгвістика

(назви освітньої програми )

вид дисципліни загальна підготовка; вибіркова

(загальна підготовка /спеціальна (фахова) підготовка; обов’язкова/вибіркова)

форма навчання денна

(денна / заочна/дистанційна)

Харків – 2021 рік

**ЛИСТ ЗАТВЕРДЖЕННЯ**

Робоча програма з навчальної дисципліни Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві

Розробники:

Проф., канд.філософ.наук, доцент \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Л.В. Перевалова

(посада, науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(посада, науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри права

(назва кафедри, яка забезпечує викладання дисципліни)

Протокол від « 31 » серпня 2021 року № 1

Завідувач кафедри \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ І.В. Лисенко

(підпис) (ініціали та прізвище)

**ЛИСТ ПОГОДЖЕННЯ**

Шифр та назва освітньої програми Прикладна та комп’ютерна лінгвістика

Кафедра права

(назва кафедри на якій викладається дисципліна)

Гарант ОП Шаронова Н.В. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ПІБ) (Підпис, дата)

Завідувач кафедрою Лисенко І.В. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ПІБ) (Підпис, дата)

**ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  зп | Дата засідання  кафедри-розробника РПНД | Номер протоколу | Підпис завідувача кафедри  (яка викладає) | Підпис завідувача кафедри  (на якій викладається) | Підпис гаранта освітньої програми |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |

**МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ   
ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Метою навчальної дисципліни** Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві є формування у майбутніх фахівців розуміння сутності явища інформаційна безпека, ознайомити з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної безпеки особистості, держави, суспільства.

**Компетентності:**

Загальні компетентності

ЗК-4. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні

**Результати навчання**

Програмні результати навчання за спеціальністю

РН-3. Знати правове забезпечення охорони природного навколишнього середовища, вміти проводити інструментальні виміри числових значень нормованих показників стану навколишнього та виробничого середовища. ▪ РН-4. Здобуття навичок побудови правової позиції з різних питань застосування законодавства та її юридичної аргументації.

Структурно-логічна схема вивчення навчальної дисципліни

|  |  |
| --- | --- |
| Вивчення цієї дисципліни безпосередньо спирається на: | На результати вивчення цієї дисципліни безпосередньо спираються: |
| Правознавство | Правове регулювання створення та розробки Стартап проектів в Україні |
|  | Право інформаційних технологій |

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

(розподіл навчального часу за семестрами та видами навчальних занять)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Семестр | Загальний обсяг | | | За видами аудиторних занять (годин) | | | Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ) | Поточний контроль | Семестровий контроль | |
| Всього (годин) / кредитів ECTS | З них | |
| Аудиторні заняття  (годин) | Самостійна робота  (годин) | Лекції | Лабораторні заняття | Практичні заняття, семінари | Контрольні роботи  (кількість робіт) | Залік | Екзамен |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| **У** | **120/4** | **64** | **56** | **32** |  | **32** |  |  | **+** |  |
|  |  |  |  |  |  |  |  |  |  |  |

Співвідношення кількості годин аудиторних занять до загального обсягу складає \_\_\_\_53\_\_ (%)

(Орієнтовно кількість годин аудиторних занять в одному кредиті ЄКТС для денної форми навчання може становити від 50 до 33 відсотків).

**СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № з/п. | Види навчальних занять (Л, ЛЗ, ПЗ, СР) | Кількість годин | Номер семестру (якщо дисципліна викладається  у декількох семестрах).  Найменування тем та питань кожного заняття.  Завдання на самостійну роботу. | Рекомендована література (базова, допоміжна) |
| 1 | 2 | 3 | 4 | 5 |
| 1  2  3  4  5.  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20    21  22  23  24  25  26  27  28  29  30  31  32  33 | Л  СЗ  СР  Л  СЗ  СР  Л  СЗ  СР  Л  СЗ  СР  Л  СЗ  СР  Л  СЗ  СР  Л  СЗ  СР  Л  СЗ  СР  Л  СЗ  СР  Л  СЗ  СР  Л  СЗ  СР | 2  2  5  2  2  4  2  2  5  4  4  5  4  4  4  2  2  4  4  4  5  4  4  5  4  4  5  2  2  7  2  2  7 | **Тема 1.** **Поняття інформаційної безпеки держави, суспільства та особи**  Інформаційна безпека (поняття і визначення). Інформаційна безпека, її сутність. Інтереси особи, суспільства та держави в інформаційній сфері  ***Поняття інформаційної безпеки держави, суспільства та особи***  Правове забезпечення інформації та інформаційної безпеки. Інформація та види інформації. Інформаційні відносини. Інформаційний суверенітет. Сутність інформаційної безпеки. Види інформаційної безпеки. Інформаційна сфера та інтереси особи, держави та суспільства.  1. Які основні підходи до визначення поняття «інформаційна безпека» Ви знаєте?  2. Назвіть основні ознаки інформаційної безпеки.  3. Назвіть основні визначення поняття «інформаційна безпека».  4. У чому полягають інтереси особи, суспільства та держави в інформаційній сфері?  5. Назвіть об’єкти, суб’єкти та види інформаційної безпеки.  6. Що таке інформація?  7. Що таке джерело інформації?  8. Які є носії інформації?  9. Що розуміють під інформаційними ресурсами? 10. Що таке загроза інформаційній безпеці?    **Тема 2.** **Інформаційна безпека та кібербезпека.**  Кіберпростір: поняття та склад. Проблеми забезпечення інформаційної та кібербезпеки. Стратегії забезпечення національної безпеки держави. Закон України «Про національну безпеку».  ***Проблеми забезпечення інформаційної безпеки та кібербезпеки в Україні***  Кіберпростір та його співвідношення з інформаційною безпекою. Кібербезпека склад та сутність. Стратегія забезпечення національної безпеки. Фундаментальні національні інтереси України.  1. Що таке кіберборотьба?  2. Які основні особливості їй притаманні?  3. Дайте визначення поняття «кібернетична безпека».  4. Назвіть істотні ознаки, які його характеризують. 5. Причини головних проблем забезпечення кібернетичної безпеки.  6. Які стратегії затверджені в Законі України «Про національну безпеку України»?  7. Стратегія воєнної безпеки України.  8. Стратегія кібербезпеки України.  9. Стратегія громадської безпеки та цивільного захисту України.  **Тема 3**. **Загрози для інформаційної безпеки держави, суспільства, людини**  Поняття загроз інформаційній безпеці. Види загроз інформаційній безпеці. Фактори загроз інформаційній безпеці. Джерела загроз інформаційній безпеці**.** Етапи розвитку засобів інформаційних комунікацій    ***Інформаційна безпека та існуючі загрози***  Інформаційна безпека держави та життєво важливі інтереси особистості, суспільства та держави. Об’єкти та суб’єкти інформаційної безпеки. Концепція інформаційної безпеки. Класифікація видів загроз інформаційній безпеці України. Внутрішні та зовнішні джерела загроз інформаційній безпеці. України. Принципи забезпечення інформаційної безпеки. Система забезпечення інформаційної безпеки держави. Основні форми і способи забезпечення інформаційної безпеки держави.  1. Яким чином розрізняються групи загроз інформації?  2. Дайте визначення поняттям «загроза», «небезпека».  3. Визначте види загроз за ймовірністю реалізації.  4. Визначте види загроз за джерелами походження. 5. Визначте види загроз за значенням.  6. Визначте види загроз за структурою та об’єктом впливу.  7. Визначте види загроз за характером реалізації.  8. Які основні підходи до визначення дестабілізуючих факторів ви знаєте?  9. Визначте політичні фактори загроз.  10. Визначте економічні фактори загроз.  11. Визначте організаційно-технічні фактори загроз. 12. Назвіть джерела загроз інформаційній безпеці особи.  13. Назвіть джерела загроз інформаційній безпеці суспільству.  14. Назвіть джерела загроз інформаційній безпеці держави.  15. Які існують етапи розвитку засобів інформаційних комунікацій?  **Тема 4. Принципи, форми та методи забезпечення інформаційної безпеки держави**  Основні принципи забезпечення інформаційної безпеки держави. Основні форми забезпечення інформаційної безпеки держави. Методи забезпечення інформаційної безпеки  ***Основні принципи, форми та методи забезпечення інформаційної безпеки.***  Основні та специфічні принципи інформаційної безпеки. Основні форми забезпечення інформаційної безпеки: інформаційний патронат, інформаційна кооперація, інформаційне протиборство.  1. Поняття забезпечення інформаційної безпеки держави.  2. Основні принципи забезпечення інформаційної безпеки держави.  3. Що таке превентивність?  4. Як можна тлумачити поняття адекватної інформованості?  5. Що таке інформаційний патронат?  6. Що таке інформаційна кооперація?  7. Дати визначення інформаційного протиборства. 8. Способи забезпечення інформаційної безпеки для конкретної особи.  9. Методи забезпечення інформаційної безпеки.  10. Рівні сфери інформаційної безпеки.  11. Які є методи впливу на інформацію?  **Тема 5. Інформаційне протиборство між країнами. Інформаційна війна**  Основні форми інформаційного протиборства. Інформаційна війна та її завдання. Концепція інформаційної війни. Органи інформаційної війни. Основні форми інформаційної війни. Інформаційна зброя.  ***Інформаційна війна як найвищий ступень інформаційного протиборства***  Інформаційне протиборство та його види. Об’єкти впливу інформаційного протиборства. Концепція інформаційного протиборства. Ступені інформаційного протиборства. Інформаційна війна та її особливості. Завдання інформаційної війни. Основні форми та рівні інформаційної війни. Засоби інформаційної війни. Інформаційні переваги у сфері інформаційного протиборства.  1. Дайте визначення поняття «інформаційне протиборство».  2. Назвіть рівні проведення інформаційного протиборства.  3. Назвіть основні ступені інформаційного протиборства.  4. Що відноситься до органів інформаційної війни? 5. Назвіть основні форми інформаційної війни.  6. Що являє собою оперативна безпека?  **Тема 6. Інформаційна зброя в інформаційні війні**  Інформаційна зброя та сфера її застосування. Основні об’єкти застосування інформаційної зброї. Види інформаційної зброї. Особливості застосування інформаційної зброї.  ***Інформаційна зброя та її складові***  Інформаційна зброя воєнного та невоєнного застосування. Засоби ураження комп’ютерних інформаційних систем. Програми з потенційно небезпечними наслідками.  1.Яким чином відрізняється інформаційна зброя від звичайних засобів ураження?  2. Назвіть сферу застосування інформаційної зброї. 3. Назвіть основні об’єкти застосування інформаційної зброї.  4. Що таке комп’ютерні віруси?  5. Які існують види програмних закладок?  6. Назвіть та охарактеризуйте засоби несанкціонованого доступу.  7. Які існують особливості застосування інформаційної зброї?  **Тема 7. Основи теорії інформаційної боротьби**  Зміст теорії інформаційної боротьби. Закони та закономірності інформаційної боротьби. Принципи інформаційної боротьби. Заходи інформаційної боротьби. Способи та форми інформаційної боротьби.    ***Теорія інформаційної боротьби та її сутність***  Поняття теорії інформаційної боротьби та її мета. Фактори впливу: економічний, воєнний та інформаційний. Загальні основи теорії інформаційної боротьби та її структура. Теорія сил та засобів ураження інформації. Теорія захисту інформації. Особливості законів та закономірностей інформаційної боротьби. Заходи інформаційної боротьби: інформаційне забезпечення, інформаційний захист, інформаційна протидія. Способи інформаційної боротьби та їх класифікація.    1. Дати визначення інформаційної боротьби.  2. Яка мета інформаційної боротьби?  3. Які фактори впливають на зміст інформаційної боротьби?  4. Які існують заходи інформаційної боротьби?  5. Охарактеризувати принципи інформаційної боротьби.  6. Дати визначення метода оцінки ефективності інформаційної боротьби.  7. Які існують форми ведення інформаційної боротьби?  8. Які існують способи інформаційної боротьби?  9. Що таке радіоелектронно-вогневий удар? 10.Формула для обчислення числового значення критерію ефективності інформаційної боротьби.    **Тема 8. Основи безпеки інформаційних ресурсів**  Поняття та загальні властивості інформації. Поняття загроз. Загрози безпеки інформації та інформаційних ресурсів. Джерела загроз безпеці інформації. Класифікація вразливостей безпеки. Моделі порушень інформаційних ресурсів  ***Основи безпеки інформаційних технологій***  Інформація та її зміст. Одержувачі інформації. Загрози порушення конфіденційності, цілісностіта  доступності інформації. Загрози безпеки інформації та інформаційних ресурсів. Порушення та їх види.  Джерела загроз безпеки інформації: антропогенні, техногенні та викликані стихійними джерелами. Порушники,цілі та мета їх дій.  1. Що є джерелом та фактором загрози інформації? 2. Які є види загроз комп’ютерної інформації?  3. Які є групи джерел загроз безпеці інформації?  4. Наведіть класифікацію вразливостей безпеці інформації?  5. Які класи (види) загроз розрізняються в інформаційній сфері?  6. Які загрози відносяться до рівня порушення конфіденційності ?  7. Які загрози відносяться до рівня порушення цілісності ?  8. Які існують категорії джерел конфіденційної інформації?  9. Які є моделі порушень інформаційних ресурсів? 10. Яка мета та цілі порушника об’єктів інформаційної діяльності?  11. Наведіть класифікацію порушника за характером дій?  **Тема 9. Забезпечення безпеки інформації та інформаційних ресурсів**  Напрями захисту інформації. Правовий захист. Організаційний захист. Інженерно-технічний захист. Захист інформаційних систем  ***Основні напрями забезпечення безпеки інформації та інформаційних ресурсів.***  Правовий захист: конституційне законодавство, загальні та спеціальні закони, підзаконні акти. Спеціальне законодавство. Страхове забезпечення та його мета. Ліцензія як засіб забезпечення безпеки інформації. Комерційна таємниця. Забезпечення захисту та безпеки інформації на підприємстві. Організаційний захист та його заходи.  Особливості захисту комп’ютерних систем. Служба захисту інформації. Інженерно-технічний захист та його засоби.  1. Які напрями захисту інформації ви знаєте?  2. Сформулюйте поняття права.  3. Яка структура правових актів, які орієнтовані на правовий захист інформації?  4. Дати визначення ліцензії.  5. Що таке комерційна таємниця?  6. Що забезпечує організаційний захист?  7. Назвіть основні організаційні заходи.  8. Функції служби безпеки підприємства (фірми, організації).  9. Завдання служби безпеки підприємства (фірми, організації).  10. Що таке інженерно-технічний захист? Його завдання.  11. Фізичні засоби захисту та їх завдання.  12. Які апаратні засоби захисту інформації Ви знаєте?  13. Що таке криптографія?  14. Назвіть переваги цифрового шифрування.  **Тема 10. Захист інформаційних систем**  Джерела конфіденційної інформації. Інформаційна система як об’єкт захисту. Рівні захисту інформаційних систем. Основні принципи захисту інформаційних систем.  ***Захист інформаційних систем***  Джерела інформації. Люди як джерела інформації. Інформаційна система, її структура. Інформаційні ресурси та їх властивості. Рівні захисту інформації: локальний, мережевий, на рівні користувачів. Корпоративні інформаційні системи (КІС).  1. Які існують категорії джерел конфіденційної інформації?  2. Які складові має інформаційна система?  3. Розкрийте поняття «цілісність».  4. Розкрийте поняття «доступність».  5. Розкрийте поняття конфіденційності інформації. 6. Назвіть основні напрями забезпечення безпеки інформації.  7. Розкрийте зміст моделі системи захисту інформації.  8. Якими показниками може бути оцінено якість розподілу доступу?  9. Назвіть основні принципи та рівні захисту інформаційних систем.  10. Розкрийте поняття інформаційно-комунікаційної системи.  11. Назвіть рівні інформаційно-комунікаційних мереж.  12. Сутність випадкового методу доступу до ресурсів системи.  13. Основні завдання захисту інформації в мережі? 14. Різновиди побудови комп’ютерних мереж?  15. Що повинні включати угоди обміну програмним забезпеченням?  16.Назвіть заходи управління обробкою й зберіганням інформації.  **Тема 11. Інформаційна безпека України**  Інформаційна безпека та її місце в національній безпеки України. Основні реальні та потенційні загрози інформаційній безпеці України. Стан та перспективи розвитку інформаційної безпеки. Система та політика забезпечення інформаційної безпеки.  ***Забезпечення інформаційної безпеки України***  Національна безпека та її структура. Принципи забезпечення національної безпеки. Загрози інформаційної безпеки: зовнішні та внутрішні загрози. Сутність інформаційної безпеки. Мета та завдання забезпечення інформаційної безпеки України.  1. Що розуміється під «інформаційною безпекою України»?  2. Яке її місце в системі національної безпеки України?  3. Основні напрями політики інформаційної безпеки України?  4. Найважливіші завдання у сфері інформаційної безпеки?  5. В яких сферах проявляються реальні та потенційні загрози безпеці України?  6. Охарактеризуйте загрози інформаційній безпеці України у воєнній сфері.  7. Охарактеризуйте загрози інформаційній безпеці України в економічній сфері.  8. Охарактеризуйте загрози інформаційній безпеці України в екологічній сфері.  9. Які завдання реалізації інформаційної політики з питань євроінтеграції?  10. Яким чином розрізняються групи загроз інформації?  11. Дайте визначення поняттям «загроза», «небезпека».  12. Визначте види загроз за ймовірністю реалізації. 13. Визначте види загроз за джерелами походження. 14. Визначте види загроз за значенням.  15. Визначте види загроз за структурою та об’єктом впливу.  16. Визначте види загроз за характером реалізації.  17. Які основні підходи до визначення дестабілізуючих факторів ви знаєте?  18. Визначте політичні фактори загроз.  19. Визначте економічні фактори загроз.  20. Визначте організаційно-технічні фактори загроз. 21. Назвіть джерела загроз інформаційній безпеці особи.  22. Назвіть джерела загроз інформаційній безпеці суспільству.  23. Назвіть джерела загроз інформаційній безпеці держави.  24. Які існують етапи розвитку засобів інформаційних комунікацій? | 1-7, 8, 10  2, 4, 8 – 11, 20  1-6, 8 -11, 13  2-7, 8 – 11  4,7, 13  2-7, 13  2-7, 8-11  4-6, 9-11, 13, 18,20  4-6, 9-11, 13, 18,20  4-6, 9-11, 13, 17 - 20  1-7, 9 - 13. |
| Разом (годин) | | 120 |  |  |

**САМОСТІЙНА РОБОТА**

|  |  |  |
| --- | --- | --- |
| №  з/п | Назва видів самостійної роботи | Кількість годин |
| 1 | Опрацьовування лекційного матеріалу | 8 |
| 2 | Підготовка до практичних (лабораторних) занять | 16 |
| 3 | Самостійне вивчення тем та питань, які не викладаються  на лекційних заняттях | 32 |
| 4 | Виконання індивідуального завдання: |  |
| 5 | Інші види самостійної роботи |  |
|  | Разом | 56 |

**ІНДИВІДУАЛЬНІ ЗАВДАННЯ**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 (вид індивідуального завдання)

|  |  |  |
| --- | --- | --- |
| №  з/п | Назва індивідуального завдання  та (або) його розділів | Терміни виконання  (на якому тижні) |
|  |  |  |

**МЕТОДИ НАВЧАННЯ**

Під час проведення занять з навчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві» використовуються такі методи навчання як: інноваційні методи з використанням мультимедійних презентацій, співбесіда, пояснення, ділова гра, вирішення конкретних правових ситуацій.

**МЕТОДИ КОНТРОЛЮ**

Система оцінювання сформованих компетенцій у студентів враховує види занять, які згідно з робочою програмою навчальної дисципліни передбачають лекції, семінарські заняття та самостійну роботу. Оцінювання сформованих компетенцій у студентів здійснюється за накопичувальною 100-бальною системою.

Контрольні заходи включають такі етапи оцінювання:

1. Поточний контроль, що здійснюється під час лекцій шляхом перевірки конспектів (максимальна сума – 15 балів).
2. Поточний контроль під час практичних занять здійснюється за допомогою перевірки виконаних завдань, реферату за обраною темою (максимальна сума – 15 балів).
3. Контроль самостійної роботи здійснюється шляхом перевірки тестових завдань, практичних задач і оцінюється сумою набраних балів (максимальна сума – 15 балів).
4. Підсумковий контроль, що здійснюється у формі заліку, відповідно до графіку навчального процесу (максимальна сума – 25 балів).

**РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)**

Таблиця 1. – Розподіл балів для оцінювання успішності студента для заліку

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Перевірка конспектів | Індивідуальні  завдання | КР (КП) | РГЗ | Поточний контроль | Тощо | Залік | Сума |
| 15 | 15 | …. | … | 15 | …. | 55 | 100 |

Таблиця 2. – Розподіл балів для оцінювання успішності студента для іспиту

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Контрольні роботи | Лабораторні роботи | КР (КП) | РГЗ | Індивідуальні завдання | Тощо | Іспит | Сума |
| ….. | ….. | …. | … | …. | …. | ….. | 100 |

Таблиця 3 – Шкала оцінювання знань та умінь: національна та ЕСТS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Рейтингова**  **Оцінка, бали** | **Оцінка ЕСТS та її визначення** | **Національна оцінка** | **Критерії оцінювання** | | |
| **позитивні** | | **негативні** |
| **1** | **2** | **3** | **4** | | **5** |
| 90-100 | А | Відмінно | - **Глибоке знання** навчального матеріалу, що містяться в **основних і додаткових літературних джерелах;**  - **вміння аналізувати** явища, які вивчаються, в їхньому взаємозв’язку і розвитку;  - **вміння** проводити **теоретичні розрахунки**;  - **відповіді** на запитання **чіткі**, **лаконічні, логічно послідовні;**  **- вміння вирішувати складні практичні задачі.** | | Відповіді на запитання можуть містити **незначні неточності** |
| 82-89 | В | Добре | - **Глибокий рівень знань** в обсязі **обов’язкового матеріалу**, - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**;  - вміння вирішувати **складні практичні задачі.** | | Відповіді на запитання містять **певні неточності;** |
| 75-81 | С | Добре | - **Міцні знання** матеріалу, що вивчається, та його **практичного застосування;**  **-** вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**;  - вміння вирішувати **практичні задачі.** | | **-** невміння використовувати теоретичні знання для вирішення **складних практичних задач.** |
| 64-74 | Д | Задовільно | - Знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**;  - вміння вирішувати прості **практичні задачі**. | Невміння давати **аргументовані відповіді** на запитання;  - невміння **аналізувати** викладений матеріал і **виконувати розрахунки;**  - невміння вирішувати **складні практичні задачі.** | |
| 60-63 | Е | Задовільно | - Знання **основних фундаментальних положень**  - вміння вирішувати найпростіші **практичні задачі**. | Незнання **окремих (непринципових) питань** з матеріалу модуля;  - невміння **послідовно і аргументовано** висловлювати думку;  - невміння застосовувати теоретичні положення при розв’язанні **практичних задач** | |
| 35-59 | FХ  (потрібне додаткове вивчення) | Незадовільно | **Додаткове вивчення** матеріалу може бути виконане **в терміни, що передбачені навчальним планом**. | Незнання **основних фундаментальних положень** навчального матеріалу модуля;  - **істотні помилки** у відповідях на запитання;  - невміння розв’язувати **прості практичні задачі.** | |
| 1-34 | F  (потрібне повторне вивчення) | Незадовільно | - | - Повна **відсутність знань** значної частини навчального матеріалу модуля;  - **істотні помилки** у відповідях на запитання;  -незнання основних фундаментальних положень;  - невміння орієнтуватися під час розв’язання **простих практичних задач** | |

**НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ   
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Конспект лекцій, плани практичних занять, завдання для самостійної роботи, питання, задачі, завдання для поточного та підсум­кового контролю знань і вмінь студентів, завдання до комплексної контрольної роботи та інші методичні матеріали, які є в наявності.

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

Базова література

|  |  |
| --- | --- |
| 1 | Конституція України // Відомості ВРУ, 1996, №30, ст..141, [Електронний ресурс]. Режим доступу:  <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> |
| 2 | Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України− від 7.09.2005 року № 2824-ІV. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_575#Text> |
| 3 | Про інформацію: Закон України // Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> |
| 4 | Про національну безпеку України: Закон України// Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> |
| 5 | Про захист інформації в інформаційно-телекомунікаційних системах: Закон України// Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> |
| 6 | Про доступ до публічної інформації: Закон України // Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> |
| 7 | Про Державну службу спеціального зв’язку та захисту інформації України: Закон України// Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/3475-15#Text> |
| 8 | Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І. Забезпечення інформаційної безпеки держави: навч. посіб. Львів: Видавництво Львівської політехніки, 2017. 204 с. |
| 9 | Інформаційна безпека держави: підручник: в 2 т. Т. 1. / В.М. Петрик та ін.; за заг. ред. В.В. Остроухова. Київ: ДНУ «Книжкова палата України», 2016. 264 с. |
| 10 | Лісовська Ю. П. Інформаційна безпека України: навч. посіб. Київ: Кондор, 2018. 172 с. |
| 11 | Лизанчук В. Інформаційна безпека України: теорія і практика. Львів. Вид-во ЛНУ ім. Івана Франка. 2017. 728 с. |
| 12 | Мехед Д., Ткач Ю., Базилевич В., Гур’єв В., Усов Я. Аналіз вразливостей корпоративних інформаційних систем. Захист інформації. 2018. № 1. С. 61 – 66. |
| 13 | Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім “Києво-Могилянська академія”, 2015. – 497 с. |
| 14 | * Інформаційна безпека / За ред. Ю. Я. Бобала та І. В. Горбатого. Львів: Вид-во Львівської політехніки. 2019. 580 с. |

Допоміжна література

|  |  |
| --- | --- |
| 15 | Харитонов Є.О., Давидова І.В.Інформаційна безпека: проблеми приватного права. Навчально-методичний посібник. Вид-во Фенікс, 2020. 194 с. |
| 16 | Петрик В., Присяжнюк М. Інформаційна безпека держави. Підручник у 2-х томах. Київ. Вид-во «Книжкова палата України». 2016. 264 с. |
| 17 | Нашинець-Наумова А.Ю. Інформаційна безпека суб’єктів господарювання: проблеми теорії та практики правозастосування: Монографія. Видав. Дім «Гельветика». 2017. 386 с. |
| 18 | Могильний С.Б. Інформаційна безпека при роботі в Інтернеті: навч.-метод. посібник / за ред. О. В. Лісового та ін. – К., 2018. – 105 с. |
| 19 | Корпоративна безпека: практичний посібник. Консалтингова компанія Сідкон. 2018. 276 с. |
| 20 | Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Вид-во SIDCON. 2021. 372 с. |

**ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ**

1. Верховна Рада України. Офіційний веб-портал парламенту України. [Електронний ресурс]. Режим доступу: <https://www.rada.gov.ua/>

2. Президент України. Офіційне інтернет-представництво. Президента України. [Електронний ресурс]. Режим доступу: <https://www.president.gov.ua/>

3. Кабінет Міністрів України. Урядовий портал. Єдиний веб-портал виконавчий органів України. [Електронний ресурс]. Режим доступу: <https://www.kmu.gov.ua/>

4. Національний технічний університет «Харківський політехнічний інститут». Кафедра права. [Електронний ресурс]. Режим доступу: <http://web.kpi.kharkov.ua/pravo/uk/>