**ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**
**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

Кафедра кібербезпеки та програмного забезпечення

# СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

# БЕЗПЕКА БАНКІВСЬКИХ СИСТЕМ

Освітньо-професійна програма «Комп'ютерна інженерія»

першого рівня вищої освіти

за спеціальністю 123 Комп'ютерна інженерія

галузі знань 12 Інформаційні технології

кваліфікація Бакалавр з комп'ютерної інженерії

Розглянуто на засіданні кафедри
Протокол № 13 від 31 березня 2022 р.

м. Кропивницький – 2022

**ЗМІСТ**

## 1. Загальна інформація

| | |
|---|---|
| Назва дисципліни | **Безпека банківських систем** |
| Рік викладання | 2022-2023 навчальний рік |
| Викладач | Лектор – Усік Павло Сергійович, доктор філософії, викладач кафедри кібербезпеки та програмного забезпечення,<br>http://kbpz.kntu.kr.ua/usik-pavlo/<br>https://www.scopus.com/authid/detail.uri?authorId=57215326547<br>https://scholar.google.com.ua/citations?hl=uk&user=jY3Xq0cAAAAJ<br>https://orcid.org/0000-0002-3268-342X |
| Контактний телефон | службовий: (0522)390-449 – робочі дні з $8^{30}$ до $14^{20}$<br>Telegram надано у описі курсу «Безпека банківських систем» на сервері дистанційної освіти ЦНТУ. – URL:<br>http://moodle.kntu.kr.ua/course/view.php?id=1674 |
| E-mail: | У описі курсу «Безпека банківських систем» на сервері дистанційної освіти ЦНТУ. – URL:<br>http://moodle.kntu.kr.ua/course/view.php?id=1674 |
| Консультації | *Очні консультації* відповідно до затвердженого графіку консультацій<br>*Онлайн консультації* засобами електронної пошти, мессенджерів (Facebook-Messenger / Viber / Telegram) у робочі дні |

## 2. Анотація дисципліни

Курс «Безпека банківських систем» призначений для розв'язання теоретичних та практичних завдань з ознайомлення й дослідження особливостей кіберзахисту програмного й апаратного забезпечення в сучасних мережах фінансових установ. Вивчення курсу покликано поставити студента в ситуацію схожу з виробничою, коли потрібно налагодити й підтримувати обчислювальні мережі, а також середовище їх функціонування в рамках підрозділу, банку, підприємства. Лекційні та лабораторні роботи знайомлять студента не тільки із правильними сценаріями розв'язку того або іншого завдання, але й дозволяють побачити основні ознаки й симптоми вразливостей можливого некоректного налагодження політики безпеки, мережевого устаткування й програмного забезпечення в результаті тих або інших розповсюджених помилок.

## 3. Мета і завдання дисципліни

**Метою викладання дисципліни** «Безпека банківських систем» є формування у здобувачів вищої освіти грунтовних теоретичних знань, практичних умінь та навичок в області захисту банківських інформаційних ресурсів, системами й методами визначення захищеності програмних продуктів в автоматизованих банківських системах.

Основними **завданнями** вивчення дисципліни є формування наступних **компетенцій**:

– Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

## 4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій, у поєднанні з лабораторними заняттями.

Формат очний (*Face to face*)

Для заочної форми навчання:

Під час сесії формат очний (*Face to face*), у міжсесійний період – дистанційний (*online*).

## 5. Результати навчання

У результаті вивчення дисципліни студент повинен забезпечити наступні **програмні результати навчання**:

– готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки;

– розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем;

– виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.

## 6. Обсяг дисципліни

| **Ознака дисципліни, вид заняття** | **Кількість годин** | |
|---|---|---|
| | денна форма навчання | заочна форма навчання |
| Рекомендації щодо семестру вивчення | 2022-2023 р. – 8 семестр | |
| Спеціальність | 123 «Комп'ютерна інженерія» | |
| Кількість кредитів / годин | 6/180 | |
| Кількість змістових модулів | 8 семестр – 2 модулі | |
| Нормативна / вибіркова | вибіркова | |
| лекції | 30 | 6 |
| лабораторні | 30 | 6 |
| самостійна робота | 90 | 168 |
| Вид підсумкового контролю | 8 семестр – екзамен – 30. | |

## 7. Пререквізити

Враховуючи послідовність накопичення знань та інформації, дисципліну краще вивчати після вивчення дисципліни «Вступ до кібербезпеки».

## 8. Технічне і програмне забезпечення / обладнання

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Лабораторні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд 501, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету. Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, студенту необхідно мати комп'ютерну техніку (з виходом у Internet) та оргтехніку для комунікації з викладачами, виконання тестових завдань в системі дистанційної освіти.

## 9. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.

Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

**Недопустимість:** запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ, Кодексу академічної доброчесності ЦНТУ.

## 10. Навчально-методична карта дисципліни

### 8 семестр

| **Тиждень, дата, академічні години** | **Тема, основні питання** *(розкривають зміст і є орієнтирами для підготовки до модульного і підсумкового контролю)* | **Форма діяльності (заняття) /формат** | **Матеріали** | **Література, інформаційні ресурси** | **Самостійна робота Завдання, обсяг годин** | **Вага оцінки** | **Термін виконання** |
|---|---|---|---|---|---|---|---|
| Змістовний модуль 1. | | | | | | | |
| Тиж.1 (за розкладом) (2 год.) | **Тема 1. Основні поняття кібербезпеки банківських установ** Суть, мета, завдання інформаційної безпеки банківських установ. Інформаційна безпека автоматизованих систем обробки інформації банку. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Розібрати метод шифрування RSA (4 год.) | 2 бали | Самостійна робота до 2 тижня включно |
| Тиж.1 (за розкладом) (2 год.) | **Тема 2. Банківська таємниця.** Захист банківської таємниці в правовому полі. Злочини передбачені сферою використання комп'ютерів, систем та комп'ютерних мереж. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити захист банківської таємниці в правовому полі (5 год.) | 2 бали | Самостійна робота до 2 тижня включно |
| Тиж.2 (за розкладом) (2 год.) | **Тема 3. Ризики кібербезпеки банківських установ** Загрози інформаційної безпеки банківської установи. Класифікація загроз . Вразливість систем безпеки банківської установи. Класифікація вразливостей. Управління ризиками інформаційної безпеки банків | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити питання керування ризиками (4 год.) | 2 бали | Самостійна робота до 2 тижня включно |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Тиж.1,2 (за розкладом) (6 год.) | **Тема 3. Вивчення системи захисту інформації GnuPG та Kleopatra** | Лабораторна робота / *Face to face* | Методичні рекомендації | [37,38] [47-49 ] | Самостійно опрацювати матеріал: Вивчити принципи та методи роботи з системою захисту даних GnuPG та Kleopatra. Перевірити їх роботу (5 год.) | 7 балів | Самостійна робота до 2 тижня включно |
| Тиж.3 (за розкладом) (2 год.) | **Тема 4. Поняття персональних даних** Поняття конфіденційності персональних даних. Захист персональних даних. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] [27] | Самостійно опрацювати матеріал: Дослідити нормативні документи захисту персональних даних (4 год.) | 2 бали | Самостійна робота до 4 тижня включно |
| Тиж.3 (за розкладом) (2 год.) | **Тема 5. Поняття політики безпеки банківських установ** Політика інформаційної безпеки банку. Реалізація політики інформаційної безпеки банку. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити політику інформаційної безпеки банку (5 год.) | 2 бали | Самостійна робота до 4 тижня включно |
| Тиж.4 (за розкладом) (2 год.) | **Тема 6. Управління інформаційною безпекою банківських установ** Методи захисту інформації. Властивості управління інформаційною безпекою в банку. Впровадження СУІБ в банківських установах. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити властивості управління інформаційною безпекою в банку (4 год.) | 2 бали | Самостійна робота до 4 тижня включно |
| Тиж.3,4 (за розкладом) (6 год.) | **Тема 6. Вивчення системи захисту даних VeraCrypt 1.24.** | Лабораторна робота / *Face to face* | Методичні рекомендації | [37, 38, 50] | Самостійно опрацювати матеріал: Вивчити принципи та методи роботи з системою захисту даних „VeraCrypt 1.24”. Перевірити її роботу. (5 год.) | 7 балів | Самостійна робота до 4 тижня включно |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Тиж.5 (за розкладом) (2 год.) | **Тема 7. Безпека в автоматизованих системах банку** Захист інформації в інформаційних системах. Криптографічний захист інформації. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити питання захисту інформації в автоматизованих системах банку (4 год.) | 2 бали | Самостійна робота до 6 тижня включно |
| Тиж.5 (за розкладом) (2 год.) | **Тема 8. Безпека мережі передачі даних SWIFT** Основні поняття мережі передачі даних SWIFT. SWIFT та інформаційна безпека. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити основні поняття мережі передачі даних SWIFT (5 год.) | 2 бали | Самостійна робота до 5 тижня включно |
| Максимальна кількість балів за змістовим модулем 2 | | | | | | 30 балів | |
| Змістовний модуль 2. | | | | | | | |
| Тиж.6 (за розкладом) (2 год.) | **Тема 9. Безпека даних в мережі банкоматів** Система банкоматів. Поняття безпеки банкоматів. Локальна відеоохоронна система захисту банкоматів. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити поняття безпеки банкоматів (4 год.) | 2 бали | Самостійна робота до 6 тижня включно |
| Тиж.6 (за розкладом) (6 год.) | **Тема 9. Дослідження захисту інформації у спрощених EDI-системах** Пошук уразливостей за допомогою Metasploit | Лабораторна робота / *Face to face* | Методичні рекомендації | [35-38] | Самостійно опрацювати матеріал: Будь-якою мовою програмування розробити спрощену систему захищеного обміну банківською інформацією з використанням Microsoft CryptoAPI. (5 год.) | 6 балів | Самостійна робота до 6 тижня включно |
| Тиж.7 (за розкладом) (2 год.) | **Тема 10. Безпека даних в мобільних пристроях** Кібербезпека мобільних та дистанційних телекомунікацій. Загрози втрати інформації з мобільних пристроїв. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити загрози втрати інформації з мобільних пристроїв (4 год.) | 2 бал | Самостійна робота до 8 тижня включно |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Тиж.7 (за розкладом) (2 год.) | **Тема 11. Положення про заходи із забезпечення інформаційної безпеки в банківській системі України** Вимоги до кібербезпеки в банківській системі. Вимоги до банків, та до впровадження СУІБ. Вимоги до криптографічного захисту інформації в інформаційних системах Національного банку. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити положення про заходи із забезпечення інформаційної безпеки в банківській системі України (5 год.) | 1 бал | Самостійна робота до 8 тижня включно |
| Тиж.8 (за розкладом) (2 год.) | **Тема 12. Захист інформації в приміщеннях банків, у яких обробляються електронні документи** Загальні положення. Вимоги до приміщень з обмеженим доступом. Вимоги до комутаційних кімнат. Вимоги до серверних приміщень і приміщень електронних архівів. Вимоги до екранованих приміщень. Вимоги до систем заземлення банків та систем захисту від пошкодження блискавкою. Вимоги до систем електроживлення банків. Рекомендації щодо побудови структурованих і локальних мереж. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити вимоги до приміщень з обмеженим доступом, до комутаційних кімнат, до серверних приміщень і приміщень електронних архівів, до екранованих приміщень, до систем заземлення банків та систем захисту від пошкодження блискавкою, до систем електроживлення банків (4 год.) | 2 бал | Самостійна робота до 8 тижня включно |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Тиж.7,8 (за розкладом) (6 год.) | **Тема 12. Розробка системи «Банкоматик»** | Лабораторна робота / *Face to face* | Методичні рекомендації | [35-38] | Самостійно опрацювати матеріал: Будь-якою мовою програмування розробити спрощену систему емуляції роботи банкоматів «Банкоматик» з використанням Microsoft CryptoAPI. (5 год.) | 6 балів | Самостійна робота до 8 тижня включно |
| Тиж.9 (за розкладом) (2 год.) | **Тема 13. Western Union. Вимоги до захисту інформації при переказі коштів через систему Western Union** Вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів. Кібербезпека при здійсненні переказів грошових коштів з використанням ЗКЗІ. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити вимоги до забезпечення захисту інформації при здійсненні переказів грошових коштів (4 год.) | 2 бал | Самостійна робота до 10 тижня включно |
| Тиж.9 (за розкладом) (2 год.) | **Тема 14. Інформаційна злочинність** Основні поняття інформаційної злочинності. Кіберзлочинність в Україні. Боротьба із інформаційною злочинністю. | Лекція / *Face to face* | Презентація | [1] [16-19] [21-25] | Самостійно опрацювати матеріал: Дослідити поняття інформаційної злочинності (5 год.) | 2 бал | Самостійна робота до 10 тижня включно |
| Тиж.10 (за розкладом) (2 год.) | **Тема 15. Нормативно-правові акти з питань безпеки в банківській сфері** Положення про захист інформації електронних банківських документів з використанням засобів захисту інформації Національного банку України. | Лекція / *Face to face* | Презентація | [1-5] [16-19] [21-25] [33] | Самостійно опрацювати матеріал: Дослідити нормативно-правові акти з питань безпеки в банківській сфері (4 год.) | 1 бал | Самостійна робота до 10 тижня включно |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Тиж.9,10 (за розкладом) (6 год.) | **Тема 15. Вивчення захисту повідомлень в протоколі SET** | Лабораторна робота / *Face to face* | Методичні рекомендації | [35-38] | Самостійно опрацювати матеріал: Будь-якою мовою програмування розробити просту систему захисту повідомлень з використанням процедур захисту, які використовуються в протоколі SET. (5 год.) | 6 балів | Самостійна робота до 10 тижня включно |
| Максимальна кількість балів за змістовим модулем 4 | | | | | | 30 балів | |
| Максимальна кількість балів за екзамен | | | | | | 40 балів | |

## 11. Система оцінювання та вимоги

**Види контролю:** поточний, підсумковий.

**Методи контролю:** спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

**Форма підсумкового контролю:** 8 семестр – екзамен.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Безпека банківських систем» здійснюється згідно з кредитною трансферно-накопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи, виконання лабораторних робіт), для оцінювання якої призначається 60 балів, та екзамену, максимальна оцінка за який складає 40 балів.

### Розподіл балів, які отримують студенти при вивченні дисципліни «Безпека банківських систем»

**8 семестр**

| Поточний контроль та самостійна робота | | | | | | | | | | | | | | | | | | | Екзамен | Сума |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Змістовий модуль 1 | | | | | | | | | | Змістовий модуль 2 | | | | | | | | | | |
| Т1 | Т2 | Т3 | | Т4 | Т5 | Т6 | | Т7 | Т8 | Т9 | | Т10 | Т11 | Т12 | | Т13 | Т14 | Т15 | | |
| Л1 | Л2 | Л3 | ЛР1 | Л4 | Л5 | Л6 | ЛР2 | Л7 | Л8 | Л9 | ЛР3 | Л10 | Л11 | Л12 | ЛР4 | Л13 | Л14 | Л15 | ЛР5 | |
| 2 | 2 | 2 | 7 | 2 | 2 | 2 | 7 | 2 | 2 | 2 | 6 | 2 | 1 | 2 | 6 | 2 | 2 | 1 | 6 | |
| 30 | | | | | | | | | | 30 | | | | | | | | | 40 | 100 |

Примітка: Т1, Т2,…,Т14 – тема, Л – теоретичні (лекційні) заняття, ЛР – лабораторні заняття

**Шкала оцінювання: національна та ЄКТС**

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену</td><td>для заліку</td></tr>
<tr><td>90-100</td><td>A</td><td>відмінно</td><td rowspan="5">задовільно</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>1-34</td><td>F</td><td>незадовільно з обов’язковим повторним вивченням дисципліни</td><td>не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

*Критерії оцінювання.* Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, лабораторні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті:

**оцінку «відмінно» (90-100 балів, А)** – заслуговує студент, який:

– всебічно, систематично і глибоко володіє навчально-програмовим матеріалом;

– вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;

– засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;

– засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває;

– вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію;

– самостійно визначає окремі цілі власної навчальної діяльності, виявив творчі здібності і використовує їх при вивченні навчально-програмового матеріалу, проявив нахил до наукової роботи.

**оцінку « добре» (82-89 балів, В)** – заслуговує студент, який:

– повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;

– має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування проблем професійного спрямування;

– під час відповіді допустив деякі неточності, які самостійно виправляє, добирає переконливі аргументи на підтвердження вивченого матеріалу;

**оцінку «добре» (74-81 бал, С)** – заслуговує студент, який:

– в загальному роботу виконав, але відповідає на екзамені з певною кількістю помилок;

– вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;

– опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

**оцінку «задовільно» (64-73 бали, D)** – заслуговує студент, який:

– знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;

– виконує завдання, але при рішенні допускає значну кількість помилок;

– ознайомлений з основною літературою, яка рекомендована програмою;

– допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення.

**оцінку «задовільно» (60-63 бали, E)** – заслуговує студент, який:

– володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

**оцінка «незадовільно» (35-59 балів, FX)** – виставляється студенту, який:

– виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

**оцінку «незадовільно» (35 балів, F)** – виставляється студенту, який:

– володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;

– допускає грубі помилки при виконанні завдань, передбачених програмою;

– не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

**При виставленні оцінки враховуються результати навчальної роботи студента протягом семестру**

Критерії оцінки заліку:

– «зараховано» – студент має стійкі знання про основні поняття дисципліни, може сформулювати взаємозв'язки між поняттями.

– «незараховано» – студент має значні пропуски в знаннях, не може сформулювати взаємозв'язку між поняттями, що вивчаються в курсі, не має уявлення про більшість основних понять дисципліни, що вивчається.

## 12. Рекомендована література

### Базова


1. Усік П.С., Буравченко К. О. Безпека банківських систем. Навчальний посібник – Кропивницький: ЦНТУ, 2022. – 194 с.
2. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994);
3. Закон України “Про захист персональних даних” (2010)
4. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)
5. Закон України “Про національну безпеку (2018)
6. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
7. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229;
8. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;

9. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
10. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
11. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.
12. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.
14. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
15. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.
16. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2009.-276с.
17. А.М. Гребенюк, Л.В. Рибальченко. Основи управління інформаційною безпекою: навч. Посіб. Дніпро: Дніпроп. держ. ун т внутріш. справ, 2020. – 144 с.
18. Головань СМ., Васюков І.В., Давиденко А.М., Хорошко В.О., Щербак Л.М. Основи організації електронного документообігу: У 2 т./ – К.: ДУІКТ, 2008. – Т. 1. – 230 с., Т. 2. – 233 с.
19. Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М. Конфіденційне діловодство. Практикум: Навч. Посіб. – Луганськ: СНУ ім. В.Даля, 2010. – 180 с.
20. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об'єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.

**Допоміжна**

21. Усік П.С., Смірнова Т.В., Бурмак Ю.А., Улічев О.С., Доренський О.П., «Стійка функція шифрування удосконаленого модуля криптографічного захисту інформації в інформаційно-комунікаційних системах» Кібербезпека: освіта, наука, техніка. № 1(13). С. 183-201. 2021. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/346 (Фахове видання. Категорія «Б»)
22. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2005. – 432 с.
23. Бондаренко М. Ф. Визначення та обґрунтування суті політики інформаційної безпеки / М. Ф. Бондаренко, О. В. Потій, Ю. І. Горбенко та ін.// Радиотехника. – 2003. – № 134. – С. 9-25.
24. Домарєв В. В. Обґрунтування основних функцій системи управління інформаційною безпекою / В. В. Домарєв, Д. В. Домарєв, С. Б Гордієнко. // Вісник Державного університету інформаційно-комунікаційних технологій. – 2012. – Т. 10, № 2. – С. 102-104.
25. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
26. Зубок М. І. Безпека банківської діяльності: навч. посібник / Зубок . І. — К. : КНЕУ, 2002. — 190 с.
27. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник.-К. ДУІКТ, 2010. - 316 с.
28. Лужецький В.А. Захист персональних даних. Навчальний посібник./ Лужецький В.А., Войтович О.П., Дудатьєв А.В – Вінниця: ВНТУ, 2009. – 487 с.
29. Лужецький В.А., Войтович О.П., Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-СУМ-Вінниця, 2009. – 240 с.

30. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації / За ред. проф. В.О.Хорошка – К.: Видавництво НАУ, 2002. – 208с.
31. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки : К.: ДУІКТ, 2008. – 186 с.
32. Юдін О. К. Захист інформації в мережах передачі даних: підруч. / Г. Ф. Конахович, О. Г. Корченко, О. К. Юдін. — К.: Вид-во ТОВ НВП «ШТЕРСЕРВІС», 2009. — 714 с.
33. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О. К. Юдін. — К. : НАУ, 2011. — 640 с.
34. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ ―НВП‖ІНТЕРСЕРВІС‖, 2009. – 716 с.

**Методичне забезпечення**

35. П. С. Усік, С. П. Євсеєв, К. О. Буравченко Безпека банківських систем / Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання за спеціальністю «Кібербезпека» – Кропивницький: ЦНТУ – 2022. – 39 с.
36. П. С. Усік, С. П. Євсеєв, К. О. Буравченко Безпека банківських систем / Методичні вказівки до виконання лабораторних робіт для студентів заочної форми навчання за спеціальністю «Кібербезпека» – Кропивницький: ЦНТУ – 2022. – 39 с.

**Інформаційні ресурси**

37. Курс «Безпека банківських систем» на сервері дистанційної освіта ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=1674
38. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/
39. Онлайн-курси Coursera. – URL: https://www.coursera.org
40. Академія Cisco. – URL: https://www.netacad.com
41. Он-лайн ресурс з інформаційних технологій. – URL:https://habr.com
42. Он-лайн ресурс з інформаційних технологій. – URL:https://dou.ua/
43. Пошукова система. – URL:https://www.google.com/
44. Он-лайн ресурс перегляду відеоуроків.– URL:https://www.youtube.com
45. GnuPG для Linux.– URL: https://gnupg.org/download/index.html
46. Kleopatra для Linux .– URL: https://kde.org/applications/en/utilities/org.kde.kleopatra
47. Kleopatra для Windows.– URL: https://www.gpg4win.org/download.html
48. Довідкова система для „VeraCrypt”.– URL: https://www.veracrypt.fr/en/Home.html