ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА БАНКІВСЬКИХ СИСТЕМ

першого рівня вищої освіти

м. Кропивницький

1. Загальна інформація

Назва дисципліни	**Безпека банківських систем**
Викладач	Усік Павло Сергійович, доктор філософії, старший викладач кафедри кібербезпеки та програмного забезпечення, http://kbpz.kntu.kr.ua/usik-pavlo/ https://www.scopus.com/authid/detail.uri?authorId=57215326547 https://scholar.google.com.ua/citations?hl=uk&user=jY3Xq0cAAAAJ https://orcid.org/0000-0002-3268-342X
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20} Telegram надано у описі курсу «Безпека банківських систем» на сервері дистанційної освіти ЦНТУ. – URL: https://moodle.kntu.kr.ua/course/view.php?id=1013
E-mail:	mr.usik@ukr.net
Консультації	*Очні консультації* відповідно до затвердженого графіку консультацій *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 ґрунтовних 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 здатності застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності.

4. Результати навчання

У результаті вивчення дисципліни здобувач вищої освіти буде вміти:

– діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

– розробляти моделі загроз та порушника;

– вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

– реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

– здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;

– здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

5. Обсяг дисципліни

Ознака дисципліни	
Кількість кредитів / годин	4/120
Нормативна / вибіркова	вибіркова
Вид підсумкового контролю	залік

6. 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.

7. Програма навчальної дисципліни

Тема 1. Основні поняття кібербезпеки банківських установ
Суть, мета, завдання інформаційної безпеки банківських установ.
Інформаційна безпека автоматизованих систем обробки інформації банку.
Тема 2. Банківська таємниця та захист персональних даних.
Захист банківської таємниці в правовому полі.
Поняття конфіденційності персональних даних.
Тема 3. Нормативно-правові акти з питань безпеки в банківській сфері
Положення про захист інформації електронних банківських документів з використанням засобів захисту інформації Національного банку України
Тема 4. Загрози кібербезпеці банківських інформаційних систем
Загрози інформаційної безпеки банківської установи. Класифікація загроз.
Тема 5. Ризики кібербезпеки банківських установ
Вразливість систем безпеки банківської установи. Класифікація вразливостей.
Управління ризиками інформаційної безпеки банків
Тема 6. Поняття політики безпеки банківських установ
Політика інформаційної безпеки банку.
Реалізація політики інформаційної безпеки банку.
Тема 7. Технічний захист інформації в банківських системах. Захист платіжної інфраструктури та банкоматів.
Апаратні та програмні засоби захисту.
Мережевий та системний захист.
Тема 8. Криптографічний захист інформації в банківських системах
Шифрування, електронний цифровий підпис, управління ключами.
Тема 9. Захист платіжних систем і електронних банківських сервісів
Основні загрози платіжним системам і е-банкінгу. Аутентифікація та авторизація користувачів.
Тема 10. Моніторинг, аудит та реагування на інциденти кібербезпеки
Журнали подій, SIEM, SOC, план реагування на інциденти.

8. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

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

Форма підсумкового контролю: залік.

Поточний контроль передбачає оцінювання кожної лабораторної роботи. Основними критеріями є правильність виконання завдання, якість захисту роботи та дотримання встановлених термінів. У процесі оцінювання враховується рівень розуміння теоретичного матеріалу та сформованість практичних навичок.

Підсумковий контроль здійснюється у формі заліку, який оцінює ступінь засвоєння теоретичних положень дисципліни та здатність студента застосовувати отримані знання на практиці. Однак, в процесі вивчення дисципліни передбачено виконання комплексу робіт під час лекційних та лабораторних занять, а також індивідуальних завдань. У зв'язку з цим здобувачам вищої освіти може бути виставлена оцінка понад 60 балів без обов'язкового виконання підсумкової залікової роботи.

9. Рекомендована література

Базова

1. Усік П.С., Буравченко К. О. Безпека банківських систем. Навчальний посібник – Кропивницький: ЦНТУ, 2022. – 194 с.
2. Усік П.С., Смірнова Т.В., Буравченко К. О., Смірнов О.А., Улічев О.С., Смірнов С. А., «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту» Кібербезпека: освіта, наука, техніка. Том 1 № 29. С. 704-716. 2025. Режим доступу: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/930
3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (1994);
4. Закон України "Про захист персональних даних" (2010)
5. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)
6. Закон України "Про національну безпеку (2018)
7. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
8. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229;
9. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;
10. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
11. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
12. 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.
13. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
14. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.
15. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

16. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.
17. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2009.-276с.
18. А.М. Гребенюк, Л.В. Рибальченко. Основи управління інформаційною безпекою: навч. Посіб. Дніпро: Дніпроп. держ. ун т внутріш. справ, 2020. – 144 с.
19. 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.
20. 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.
21. 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

22. 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»)
23. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. –К.: "МК-Прес", 2005. – 432 с.
24. 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.
25. 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.
26. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
27. Зубок М. І. Безпека банківської діяльності: навч. посібник / Зубок . І. — К. : КНЕУ, 2002. — 190 с.
28. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник.-К. ДУІКТ, 2010. - 316 с.
29. Лужецький В.А. Захист персональних даних. Навчальний посібник./ Лужецький В.А., Войтович О.П., Дудатьєв А.В – Вінниця: ВНТУ, 2009. – 487 с.
30. Лужецький В.А., Войтович О.П., Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-СУМ-Вінниця, 2009. – 240 с.
31. 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.
32. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки : К.: ДУІКТ, 2008. – 186 с.
33. 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.
34. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О. К. Юдін. — К. : НАУ, 2011. — 640 с.
35. 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

36. 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.
37. 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

38. Курс «Безпека банківських систем» на сервері дистанційної освіта ЦНТУ. – URL: https://moodle.kntu.kr.ua/course/view.php?id=1013
39. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/
40. Онлайн-курси Coursera. – URL: https://www.coursera.org
41. Академія Cisco. – URL: https://www.netacad.com
42. Он-лайн ресурс з інформаційних технологій. – URL:https://habr.com
43. Он-лайн ресурс з інформаційних технологій. – URL:https://dou.ua/
44. Пошукова система. – URL:https://www.google.com/
45. Он-лайн ресурс перегляду відеоуроків.– URL:https://www.youtube.com
46. GnuPG для Linux.– URL: https://gnupg.org/download/index.html
47. Kleopatra для Linux .– URL: https://kde.org/applications/en/utilities/org.kde.kleopatra
48. Kleopatra для Windows.– URL: https://www.gpg4win.org/download.html
49. Довідкова система для „VeraCrypt”.– URL: https://www.veracrypt.fr/en/Home.html
50. VisualStudio.– URL: https://visualstudio.microsoft.com/ru/free-developer-offers/