



Силабус освітнього компонента Програма навчальної дисципліни



Безпека банківських систем

Шифр та назва спеціальності

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Національна безпека у сфері кіберзахисту

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна, Вибіркова

Семестр

6

Мова викладання

Українська

Викладачі, розробники



ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем», «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів.

[Детальніше про викладача на сайті кафедри](#)



КОРОЛЬ Ольга Григорівна

olha.korol@khpi.edu.ua

кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з яких 14 навчальних посібників, 48 статей у закордонних виданнях та фахових виданнях України, 8 патентів на корисну модель, 9 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави», «Інформаційна безпека держави»,

«Комплексний тренінг «Безпека веб-застосунків», у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Безпека банківських систем" є вибірковою навчальною дисципліною. У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки (ІБ) держави в банківському секторі (БнС). Ключову роль при побудові систем безпеки банківських інформаційних ресурсів (БІР) як складових національних інформаційних ресурсів держави, відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення ІБ держави на усіх рівнях.

Мета та цілі дисципліни

Оволодіння студентами комплексом знань в області захисту банківських інформаційних ресурсів, системами й методами визначення захищеності програмних продуктів в автоматизованих банківських системах, набуття на основі цих знань практичних навичок і теоретичних знань, необхідних для творчого підходу в питанні сучасного та в майбутньому оперативного захисту контуру бізнес-процесів в організаціях банківського сектору. Формування професійної компетентності майбутніх фахівців з кібербезпеки, достатньої для роботи на посаді адміністратора інформаційної безпеки банку та необхідної для розвитку кар'єри.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ-7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ФК-1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

ФК-2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ФК-4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки.

ФК-8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

ФК-9. Здатність використовувати знання щодо безпекової складової зовнішньої політики України та інших держав.

ФК-10. Здатність засвоювати основні теоретичні поняття та набуття практичних навичок дослідження, підготовки документів та їх використання в управлінській діяльності.

ФК-11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.

ФК-13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку.

ФК-14. Здатність здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки, готувати пропозиції щодо підвищення її ефективності.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

ПРН-7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.

ПРН-8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

ПРН-10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ПРН-12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.

ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.

ПРН-17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.

ПРН-21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку, здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки та готувати пропозиції щодо підвищення її ефективності.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 24 год., лабораторні роботи – 24 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Основи криптографічного захисту, Менеджмент інформаційної безпеки.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Структура внутрішньої платіжної системи комерційного банку. Послуги та механізми безпеки.

Основні складові інформаційної безпеки держави. Нормативні документи. Основні принципи і механізми забезпечення ІБ в ОБС України. Основні функції АБС. Структурна схема СУІБ НСМЕП.

Тема 2. Правове забезпечення банківської безпеки.

Рекомендації міжнародних стандартів. Постанова НБУ від 28.09.2017 № 95. Групові та часткові показники ІБ. Концепція побудови синергетичної моделі загроз. Стандарт СОУ Н НБУ 65.1 СУІБ 1.0: 2010. Система управління інформаційною безпекою.

Тема 3. Доступ до банківської інформації.

Основні банківські інформаційні ресурси. Політики довіри. Концепція інфраструктури безпеки. Мета і сервіси інфраструктури безпеки. Механізми автентифікації.

Тема 4. Ризики у банківській діяльності.

Класифікація кібератак на АБС. Статистика цільових атак 2020-2021. Синергетична модель загроз безпеці БІР. Удосконалена модель зловмисника.

Тема 5. Сертифікати відкритих ключів. Система PGP.

Основні механізми технології відкритих ключів та PGP в автоматизованих банківських системах. Протоколи сертифікації.

Тема 6. Оцінка ризиків у банківській діяльності.

Аудит інформаційної безпеки. Методики оцінки ризиків.

Тема 7. Безпека мікропроцесорних карток.

Внутрішньоплатіжна система комерційного банку. Стандарти пластикових карток. Механізми забезпечення безпеки валідності. Смарт-карти. Контактні та безконтактні смарт-карти. Операційні системи смарт-карт.

3D Secure.

Тема 8. Системи електронного обміну даними.

Переваги впровадження СУІБ. Цілі та результат впровадження ISO27001. Опис критичних бізнес-процесів та програмно-технічних комплексів, які забезпечують їх функціонування. Структура мережі банку. Принципи забезпечення безперервності роботи. Методологія оцінювання ризиків. Впровадження та функціонування СУІБ.

Тема 9. Технологія захисту міжбанківських платежів. Платіжна система First Virtual: безпека без шифрування.

EDI-системи. Система EDIFACT. Безпека EDI-систем. Платіжна система First Virtual: безпека без шифрування.

Тема 10. Актуальні проблеми інформаційної та кібербезпеки в банківській сфері.

Правове підґрунтя. Використання хмарних технологій. Методи поширення шкодиносів. Атаки на банкомати. Шкідносні семпли. Крадjenня через ATM Switch.

Тема 11. Цифрові валюти. криптовалюти.

Організація транзакції BITCOIN. Поняття про BLOCKCHAIN. Майнінг основні етапи. Моделі та механізми отримання конценцусу. Основи протоколів смарт-контрактів.

Тема 12. Захищені протоколи.

Протокол SSL в АБС. Протокол Alert. Протокол SET. Технологія OAEP.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Вивчення системи захисту інформації GnuPG та Kleopatra.

Тема 2. Вивчення системи захисту даних VeraCrypt 1.24.

Тема 3. Вивчення системи захисту даних КриптоБанк 5.0.

Тема 4. Дослідження захисту інформації у спрощених EDI-системах.

Тема 5. Розробка системи "Банкоматик".

Тема 6. Вивчення захисту повідомлень в протоколі SET.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 31.12.2023. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
3. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 6 травня 2015 року № 287/2015. Дата оновлення: 16.09.2020. URL: <https://zakon.rada.gov.ua/laws/show/287/2015#Text>
4. Про національну безпеку: Закон України від 21.06.2018 № 2469-VIII. Дата оновлення: 31.03.2023. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
5. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" № 96/2016. Дата оновлення: 28.08.2021. URL: <https://zakon.rada.gov.ua/laws/show/96/2016#Text>
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229. Дата оновлення: 04.05.2008. URL: <https://zakon.rada.gov.ua/laws/show/1229/99#Text>
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: <https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf>
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: <https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf>
9. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22. https://tzi.ua/assets/files/1.1_003_99.pdf
10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806). <https://tzi.com.ua/downloads/2.5-004-99.pdf>
11. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 наказ Адміністрації Держспецв'язку від 28.12.2012 № 806). <https://tzi.com.ua/downloads/1.1-002-99.pdf>
12. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. <https://tzi.com.ua/downloads/1.1-005-07.pdf>
13. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, наказ ДСТСЗІ СБУ від 04.12.2000 № 53 (Зміна № 1 наказ Адміністрації Держспецв'язку від 28.12.2012 № 806). <https://tzi.com.ua/downloads/1.4-001-2000.pdf>
14. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с. <https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnologii-zakhystu.pdf>
15. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсєєв, О.В. Мілов, С.Е. Остапов, О.В. Северінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.

<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBG006AnvjQHU1SdBl3xCaUju>.

Додаткова література

16. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL:

<https://www.iso.org/ru/contents/data/standard/08/28/82875.html>

17. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL:

<https://www.iso.org/ru/contents/data/standard/08/05/80585.html>

18. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL:

<https://www.iso.org/ru/contents/data/standard/08/05/80585.html>.

19. Кравченко П. Блокчейн і децентралізовані системи. Ч. 1 – Харків: ПРОМАРТ, 2019. – 452 с.

<https://repository.kpi.kharkov.ua/server/api/core/bitstreams/0e26ed5b-990d-4271-85f8-573434a7722f/content>

20. Кравченко П. Блокчейн і децентралізовані системи. Ч. 3 – Харків: ПРОМАРТ, 2020. – 306 с.

21. Євсєєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПТОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсєєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020. – 241 с.

<http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf>.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 20% семестрової оцінки;
- іспит: 40% семестрової оцінки.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: <http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/>

Погодження

Силабус погоджено

28.08.2024



Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП
Андрій ТКАЧОВ