

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
Кафедра кібербезпеки та DATA-технологій, факультет № 6

РОБОЧА ПРОГРАМА

навчальної дисципліни "Безпека електронних платіжних систем"
вибіркових компонент
освітньої програми першого рівня вищої освіти

Кібербезпека
(безпека інформаційних та комунікаційних систем)

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО

Вченою радою
факультету № 6
Протокол від 25.08.2023 № 7

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 (протокол від 15.08.2023 № 8).

Розробники:

Доцент кафедри кібербезпеки та DATA-технологій факультету № 6, кандидат наук з державного управління, доцент Онищенко Ю.М.

Рецензенти:

завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, доктор технічних наук, професор Петров К.Е.

доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент Світличний В.А.

1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – <u>5</u> Загальна кількість годин – <u>150</u> Кількість тем – <u>3</u>	12 Інформаційні технології 125 Кібербезпека (Безпека інформаційних та комунікаційних систем) бакалавр	Навчальний курс <u>3</u> Семестри <u>6</u> Види підсумкового контролю: - <u>екзамен</u> .
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання Лекції – <u>36 год</u> ; Практичні заняття – <u>38 год</u> ; Самостійна робота – <u>76 год</u> ; Індивідуальні завдання: Реферати (тощо) – <u>1</u>	заочна форма навчання Лекції – <u>8 год</u> ; Практичні заняття – <u>14 год</u> ; Самостійна робота – <u>128 год</u> ; Індивідуальні завдання: Реферати (тощо) – <u>1</u>	

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни "Безпека електронних платіжних систем" є формування знань з організаційно-технічних аспектів забезпечення безпеки електронних платіжних систем і вмінь протидіяти злочинам з платіжними інструментами.

Основними завданнями вивчення дисципліни "Безпека електронних платіжних систем" є:

- ознайомлення із організаційно-технічними аспектами забезпечення безпеки електронних платіжних систем;
- формування вмінь протидіяти злочинам з платіжними інструментами.

Міждисциплінарні зв'язки. Навчальна дисципліна спирається на дисципліни: інформаційні та комунікаційні технології, алгоритмізація та програмування, електроніка та схемотехніка, операційні системи та комп'ютерні мережі, теорія інформації та кодування, теорія інформації та кодування, кібербезпеки, організація баз даних та знань, управління та організація систем захисту інформації, правові засади захисту інформації, методи та засоби технічного захисту інформації і формує знання для засвоєння дисциплін: цифрова криміналістика; управління та організація систем захисту інформації.

Очікувані результати навчання: у результаті вивчення навчальної дисципліни здобувачі вищої освіти повинні:

знати: організаційно-технічні аспекти забезпечення безпеки електронних платіжних систем:

- принципи роботи банківських електронних платіжних систем в комерційній діяльності;
- складові інфраструктури електронних платіжних систем;
- банківську систему України як об'єкт захисту;
- вимоги стандартів безпеки даних у галузі платіжних карток.

вміти: протидіяти злочинам з платіжними інструментами:

- з банкоматом;
- в торгівельно-сервісних підприємствах;
- з платіжною картою;
- з реквізитами платіжних карток в торгівельно-сервісних

підприємствах;

- з платіжними інструментами без присутності картки;
- в системах дистанційного банківського обслуговування.

На вивчення навчальної дисципліни відводиться 150 годин/5 кредитів ECTS.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність самостійно досліджувати і розроблювати комплексні системи забезпечення кібербезпеки викладати і здійснювати аналітичну діяльність в області кібербезпеки	
Загальні компетентності (ЗК)	КЗ 1	Здатність застосовувати знання у практичних ситуаціях.
	КЗ 2.	Знання та розуміння предметної області та розуміння професії.
	КЗ 4.	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
	КЗ 5.	Здатність до пошуку, оброблення та аналізу інформації.
Фахові компетентності спеціальності (ФК)	КФ 3.	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	КФ 9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
	КФ 10.	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
	КФ 12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
Програмні результати навчання (ПРН)	<p>ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.</p> <p>ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.</p> <p>ПРН 5. Адаптуватися в умовах частоті зміни технологій професійної діяльності, прогнозувати кінцевий результат.</p> <p>ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.</p> <p>ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.</p> <p>ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.</p> <p>ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.</p> <p>ПРН 19. Застосовувати теорії та методи захисту щодо забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.</p> <p>ПРН 43. Застосовувати національні та міжнародні регулюючі акти у сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.</p>	

3. Програма навчальної дисципліни

Тема № 1. Електронні платіжні системи

Моделі транзакцій в традиційній та електронній комерції. Складові інфраструктури електронних платіжних систем. Функціонування та обслуговування платіжних карток. Платіжні системи криптографічних валют.

Тема № 2. Регуляторні вимоги до безпеки електронних платіжних систем

Організаційно-технічні аспекти системи захисту інформації в банківській галузі України. Вимоги стандарту безпеки даних галузі платіжних карт (Payment Card Industry Security Standard).

Тема № 3. Протидія злочинам з платіжними інструментами

Злочини з платіжними інструментами в банкоматі. Злочини з платіжними інструментами без присутності картки (card-not-present, CNP). Протиправне використання карткових реквізитів (шахрайські операції). Реагування на злочини з платіжними інструментами в банкоматах. Реагування на несанкціоновані платежі. Реагування на шахрайства держателів платіжних карток.

4. Структура навчальної дисципліни
4.1.1. Розподіл часу навчальної дисципліни за темами
(денна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 6							
Тема №1. Електронні платіжні системи	46	12		10		24	екзамен
Тема №2. Регуляторні вимоги до безпеки електронних платіжних систем	48	12		10		26	
Тема №3. Протидія злочинам з платіжними інструментами	56	12		18		26	
Всього за семестр № 6	150	36		38		76	

4.1.2. Розподіл часу навчальної дисципліни за темами
(заочна форма навчання)

Номер та назва навчальної теми		Кількість годин відведених на вивчення навчальної дисципліни						Вид контролю
		Всього	з них:					
			Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
	Семестр № 6							
Тема № 1. Електронні платіжні системи		48	2		4		42	екзамен
Тема № 2. Регуляторні вимоги до безпеки електронних платіжних систем		48	2		4		42	
Тема № 3. Протидія злочинам з платіжними інструментами		54	4		6		44	
Всього за семестр № 6		150	8		14		128	

4.1.3. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни		Література
Тема № 1. Електронні платіжні системи		
Опрацювати текст лекції № 1 та літературу до теми, створивши стислий конспект в електронному виді. Закінчити виконання практичних занять. Створити мультимедійну презентацію за темою. Підготувати розгорнуті змістовні відповіді на контрольні запитання до теми.		1, 4, 5, 8-19, 23, 24, 28, інформаційні ресурси в Інтернеті

Перелік питань до тем навчальної дисципліни		Література
Тема № 2. Регуляторні вимоги до безпеки електронних платіжних систем		
Опрацювати текст лекції № 2 та літературу до теми, створивши стислий конспект в електронному виді. Закінчити виконання практичних занять. Створити мультимедійну презентацію за темою. Підготувати розгорнуті змістовні відповіді на контрольні запитання до теми.		2, 4, 5, 8-19, 23, 24, 28-32, інформаційні ресурси в Інтернеті
Тема № 3. Протидія злочинам з платіжними інструментами		
Опрацювати текст лекції № 3 та літературу до теми, створивши стислий конспект в електронному виді. Закінчити виконання практичних занять. Створити мультимедійну презентацію за темою. Підготувати розгорнуті змістовні відповіді на контрольні запитання до теми.		3, 5-10, 20-22, 25-29, 31, 32, інформаційні ресурси в Інтернеті

5. Індивідуальні завдання

5.1.1. Теми рефератів

1. Порівняння стандартів індустрії платіжних карт PCI Security Standards.
2. Тенденції інцидентів інформаційної безпеки в платіжних системах.
3. Функціонування сучасних криптографічних валют.

6. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких здобувачі вищої освіти повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять та опрацювання літератури до теми, виконання завдань практичних занять.

Індивідуальна робота передбачає написання рефератів.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

Контроль проводиться по тестових завданнях на підсумковому контролі – заліку.

Контрольні питання

1. Розкрийте зміст етапів комерційної транзакції типового бізнес-процесу.
2. Зобразити та пояснити взаємодію учасників комерційної діяльності.
3. Охарактеризуйте види електронної комерції.
4. Зобразити та пояснити структуру типової електронної платіжної системи.
5. Якою є загальна схема Internet-banking?
6. Які задачі захисту інформації вирішуються в системах електронного бізнесу?
7. Якими є основні види загроз, що порушують інтереси споживача, при здійсненні комерційної транзакції?
8. Якими є основні види загроз, що порушують інтереси постачальника, при здійсненні комерційної транзакції?
9. Що відносяться до транзакцій, що здійснюються в середовищі «обличчя до обличчя» (Face-to-face environment)?
10. Що таке МСС торговця?
11. Якою є процедура авторизації за платіжною карткою?

12. Якою є процедура клірингу та розрахунків за здійсненою операцією?
13. Якою є процедура претензійних платежів?
14. Що входить до транзакційних даних?
15. Із чого складаються реквізити платіжної картки?
16. Як класифікуються носії електронних платіжних засобів?
17. Які є механізми автентифікації клієнта в ДБО?
18. Які є інформаційні потоки в системі мобільних платежів?
19. Які є інформаційні потоки мобільних переказів, платежів і розрахунків системи мобільних грошей?
20. Які існують бізнес-моделі організації системи мобільних платежів?
21. Які існують інтернет-орієнтовані платіжні системи (internet-based payment services) дематеріалізованих грошей?
22. З чого складається банківська система України?
23. Якими є основні банківські операції?
24. Які платіжні засоби використовуються в банківській системі України?
25. Яким чином здійснюються електронні міжбанківські розрахунки?
26. Яка інформація відповідно до законодавства є об'єктом захисту?
27. Які функції покладені на НБУ щодо захисту інформації в банківській системі України?
28. Яка інформація в банківській системі складає державну таємницю?
29. Яка інформація відноситься до банківської таємниці?
30. Як законодавчо визначено поняття електронних документів?
31. Яким чином передбачено обіг електронних документів в інформаційно-телекомунікаційних системах?
32. Поясніть схематично принцип формування та перевірки електронного підпису.
33. Поясніть суть цифрових сертифікатів.
34. Наведіть та поясніть схему взаємодії суб'єктів правових відносин у сфері послуг електронного підпису.
35. Як законодавством визначені правила захисту інформації в інформаційно-телекомунікаційних системах?
36. Із чого складається система захисту інформації платіжних систем і переказу коштів?
37. Для яких приміщень банку визначені режимні вимоги та правила з технічного захисту інформації?
38. Які вимоги висуваються до приміщень банку, що визначені для захисту інформації.
39. Скільки передбачено рівнів резервування баз даних центра оброблення системи електронних платежів Національного банку (ЦОСЕП)?
40. Що забезпечує система захисту електронних банківських документів в СЕП?
41. Що входить до технологічних засобів безпеки СЕП?
42. Як здійснюється генерація та розподіл ключів електронного підпису в банку, який є учасником СЕП?
43. З чого складаються апаратні і програмні елементи криптографічного захисту СЕП?
44. Яким чином в СЕП здійснюється накладання ЕП електронного банківського документу?
45. Яким чином в СЕП здійснюється перевірка ЕП електронного банківського документу?

46. Яким чином здійснюється шифрування електронних банківських документів в СЕП?
47. Які типи криптографічних ключів і для яких операцій використовуються в СЕП України?
48. Які носії ключової інформації передбачені для учасника СЕП?
49. Які організаційні заходи інформаційної безпеки необхідно здійснити учаснику СЕП?
50. Яким чином здійснюється контроль територіальним управлінням НБУ за виконанням вимог щодо захисту інформації банками учасниками СЕП?
51. Які основні порушення характерні в організації роботи із засобами захисту інформації НБ України?
52. Чи потрібно ліцензування діяльності у сфері криптографічного захисту інформації в банківській системі України?
53. Які основні нормативні документи розроблено в межах PCI SSC?
54. З яких кроків складається система сертифікації платіжних систем?
55. Які організації залучаються до сертифікації платіжних систем?
56. Що виступає в якості об'єктів захисту згідно стандарту PCI DSS?
57. Що відноситься до даних тримача карти і є об'єктом захисту?
58. З чого складається середовище даних тримачів карт?
59. Які вимоги стандарту PCI DSS направлені на створення і підтримку безпечної мережної інфраструктури платіжної системи?
60. Які вимоги стандарту PCI DSS направлені на захист даних тримача карти в платіжній системі?
61. Які вимоги стандарту PCI DSS направлені на підтримку програми управління вразливостями в платіжній системі?
62. Які вимоги стандарту PCI DSS направлені на впровадження посилених засобів управління доступом в платіжній системі?
63. Які вимоги стандарту PCI DSS направлені на регулярний моніторинг і тестування мережної інфраструктури в платіжній системі?
64. Як часто згідно стандарту PCI DSS потрібно проводити аналіз налаштувань міжмережних екранів і маршрутизаторів?
65. Які згідно стандарту PCI DSS необхідно використовувати технології віддаленого адміністративного доступу?
66. Які дані згідно стандарту PCI DSS дозволяється зберігати в платіжній системі?
67. Як часто згідно стандарту PCI DSS потрібно перевіряти програмний код на наявність вразливостей?
68. Як часто згідно стандарту PCI DSS потрібно видалення заблокованих облікових записів?
69. Як часто згідно стандарту PCI DSS потрібна зміна пароля користувача?
70. Якими є вимоги стандарту PCI DSS до політики паролів?
71. Якщо інший термін не визначено законодавством, то згідно стандарту PCI DSS скільки потрібно зберігати дані, які зібрані камерами відеоспостереження?
72. Які події згідно стандарту PCI DSS потрібно протоколювати в платіжній системі?
73. Як часто згідно стандарту PCI DSS слід переглядати журнали протоколювання подій?
74. Як часто згідно стандарту PCI DSS слід аналізувати бездротові мережі з метою ідентифікації всіх використовуваних пристроїв?

75. Етапи злочинів з платіжними інструментами в банкоматах за класифікацією платіжної індустрії.
76. Форми злочинів з платіжними інструментами в банкоматах за класифікацією платіжної індустрії.
77. Види злочинів з платіжними інструментами в банкоматах за класифікацією платіжної індустрії.
78. Класифікація шахрайства в торгівельно-сервісних підприємствах.
79. Класифікація злочинців та різновидів шахрайства в торгівельно-сервісних підприємствах з ціллю компрометації карток.
80. Класифікація злочинців та різновидів шахрайства в торгівельно-сервісних підприємствах з ціллю здійснення шахрайських операцій.
81. Перелік інформації для розслідування шахрайства в торгівельно-сервісних підприємствах.
82. Перелік джерел отримання інформації для розслідування шахрайства в торгівельно-сервісних підприємствах.
83. Злочини з платіжними інструментами без присутності картки (card-not-present, CNP).
84. Технології поширення шкідливих програм з метою викрадення конфіденційної інформації щодо банківських реквізитів (карткових реквізитів та облікових даних систем Інтернет-банкінгу).
85. Причини витоку конфіденційної інформації (Data Breaches) про карткові реквізити.
86. Джерела витоку конфіденційної інформації (Data Breaches) про карткові реквізити.
87. Способи протиправного використання карткових реквізитів.
88. Шахрайство держателя платіжної картки.
89. Механізми безпеки ДБО.
90. Загальна схема злочину у ДБО.
91. Ознаки інциденту в системі ДБО.
92. Реагування на злочини з платіжними інструментами в банкоматах.
93. Реагування банків на несанкціоновані платежі.
94. Реагування поліції на несанкціоновані платежі.
95. Реагування на шахрайства держателів платіжних карток.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних і лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти (далі – здобувач) з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

$$\begin{array}{l} \text{Загальна кількість} \\ \text{балів (перед} \\ \text{підсумковим} \\ \text{контролем)} \end{array} = \left(\begin{array}{l} \text{Результат} \\ \text{навчальних} \\ \text{занять} \\ \text{за семестр} \end{array} + \begin{array}{l} \text{Результат} \\ \text{самостійної} \\ \text{роботи за} \\ \text{семестр} \end{array} \right) / 2 \quad *10$$

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструється в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображаються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. **Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50**.

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

$$\begin{array}{l} \text{Підсумкові} \\ \text{бали} \\ \text{навчальної} \\ \text{дисципліни} \end{array} = \begin{array}{l} \text{Загальна кількість} \\ \text{балів (перед} \\ \text{підсумковим} \\ \text{контролем)} \end{array} + \begin{array}{l} \text{Кількість балів} \\ \text{за підсумковим} \\ \text{контролем} \end{array}$$

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне

складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\begin{array}{l} \text{Підсумкові} \\ \text{бали} \\ \text{навчальної} \\ \text{дисципліни} \end{array} = \begin{array}{l} \text{Підсумкові} \\ \text{бали за} \\ \text{поточний} \\ \text{семестр} \end{array} + \begin{array}{l} \text{Підсумкові} \\ \text{бали за} \\ \text{попередній} \\ \text{семестр} \end{array} / 2$$

Незадовільні оцінки виставляються тільки в відомостях обліку успішності. Здобувачам вищої освіти, які отримали не більше як дві незадовільні оцінки (нижче ніж 60 балів) з навчальної дисципліни, можуть бути встановлені різні строки ліквідації академічної заборгованості, але не пізніше як за день до фактичного початку навчальних занять у наступному семестрі.

Робота під час навчальних занять	Самостійна та індивідуальна робота	Підсумковий контроль
Отримати не менше 3 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, виконати практичне завдання.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97-100	Відмінно ("зараховано")	A	"Відмінно" – теоретичний зміст курсу освоєний цілком , необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85 – 89	Добре ("зараховано")	B	"Дуже добре" – теоретичний зміст курсу освоєний цілком , необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані , якість виконання більшості з них оцінено числом балів, близьким до максимального , робота з двома – трьома незначними помилками.
80-84			
75 – 79		C	"Добре" – теоретичний зміст курсу освоєний цілком , практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані , якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками , робота з декількома незначними помилками, або з однією – двома значними помилками.
70 – 74	Задовільно ("зараховано")	D	"Задовільно" – теоретичний зміст курсу освоєний не повністю , але прогалини не несуть істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано , деякі з виконаних завдань, містять помилки , робота з трьома значними помилками.
65-69			
60 – 64		E	"Достатньо" – теоретичний зміст курсу освоєний частково , деякі практичні навички роботи не сформовані , частина передбачених програмою навчання навчальних завдань не виконані , або якість виконання деяких з них оцінено числом балів, близьким до мінімального , робота, що задовольняє мінімуму критеріїв оцінки.
40–59	Незадовільно ("не зараховано")	FX	"Умовно незадовільно" – теоретичний зміст курсу освоєний частково , необхідні практичні навички роботи не сформовані , більшість передбачених програм навчання, навчальних завдань не виконано , або якість їхнього виконання оцінено числом балів, близьким до мінімального ; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
21-40			
1–20		F	"Безумовно незадовільно" – теоретичний зміст курсу не освоєно , необхідні практичні навички роботи не сформовані , всі виконані навчальні завдання містять грубі помилки , додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

10.Рекомендована література (основна, додаткова), інформаційні ресурси в Інтернеті

Основна:

1. Лекція на тему № 1 «Електронні платіжні системи».
2. Лекція на тему № 2 «Регуляторні вимоги до безпеки електронних платіжних систем».
3. Лекція на тему № 3 «Протидія злочинам з платіжними інструментами».
4. Корченко А.О. Банківська безпека / А.О. Корченко, Л.М. Скачек, В.О. Хорошко; за загальним ред. д.т.н. проф. В.О. Хорошка. – К: ПВП “Задруга”, 2014. – 185 с.
5. Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures. Version 3.2, April 2016. URL:https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1480496667980 (дата звернення: 20.06.2023).
6. Методика розкриття злочинів, вчинених у сфері функціонування платіжних карток та електронних розрахунків. / МВС України, Харків. нац. ун-т внутр. справ; О.І. Безпалова, Д.Т. Карпізін, В.В. Носов, О.В. Манжай, В.І. Стреляний. Харків, 2013.
7. Протидія злочинам у сфері використання платіжних інструментів. Матеріали тренінгу агентів і інспекторів кіберполіції. / OSCE. Харків, 2016.
8. Бандурка О.М., Глущенко В.В., Глущенко А.С. Гроші і кредит. Підручник. 2-ге вид., доп. і перероб., «Магнолія 2006», 2018, 368 с.
9. Центральний банк і грошово-кредитна політика. Підруч. / Г.В. Сілакова, О.А. Гнатенко, Г.І. Лановська, Н.І. Климаш, [та ін.] за заг. ред. Т.А. Говорушко. – Львів «Магнолія 2006», 2018. – 296 с.

Додаткова:

10. Іщук Г. Забезпечення безпеки даних карткових платіжних систем при проведенні платіжних операцій / Г. Іщук, А. Пелешенко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – № 2. – С. 106–111. URL: http://nbuv.gov.ua/UJRN/Nzundiz_2014_2_20.
11. Міщенко С. Вдосконалення системи роздрібних безготівкових платежів / С. Міщенко// Вісник КНЕУ ім. Т.Г. Шевченка. Серія: Економіка. – 2014. – № 5. – С. 22–27.
12. Коваль Н. Особливості функціонування платіжних систем України на сучасному етапі їх розвитку. 2012. URL: <http://www.economy.nauka.com.ua/?op=1&z=1441>.
13. Шелудько С.А. Міжнародні стандарти банківської справи: навчальний посібник. — К.: Видавничий дім «Кондор», 2020. — 260 с.

Нормативно-правові акти:

14. Про банки і банківську діяльність: Закон України від 07.12.2000 № 2121-III // База даних «Законодавство України»/Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2121-14#Text> (дата звернення: 20.06.2023).
15. Про валюту і валютні операції: Закон України від 21.06.2018 № 2473-VIII // База даних «Законодавство України»/Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2473-19> (дата звернення: 20.06.2023).
16. Про Національний банк України: Закон України від 20.05.1999 № 679-XIV // База даних «Законодавство України»/Верховна Рада України. URL:

- <https://zakon.rada.gov.ua/laws/show/679-14> (дата звернення: 20.06.2023).
17. Про платіжні послуги: Закон України від 30.06.2021 № 1591-IX // База даних «Законодавство України»/Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1591-20> (дата звернення: 20.06.2023).
 18. Про ринки капіталу та організовані товарні ринки: Закон України від 23.02.2006 № 3480-IV // База даних «Законодавство України»/Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/3480-15> (дата звернення: 20.06.2023).
 19. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII // База даних «Законодавство України»/Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (дата звернення: 20.06.2023).
 20. Про кіберзлочинність: конвенція Ради Європи від 07.09.2005 ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 20.06.2023).
 21. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016. URL: <http://zakon.rada.gov.ua/laws/show/96/2016> (дата звернення: 20.06.2023).
 22. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021. — URL: <https://www.president.gov.ua/documents/4472021-40013> (дата звернення: 20.06.2023).
 23. Про захист інформації в інформаційно-комунікаційних системах. Закон України: від 05.07.1994, № 1170-VII. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення: 20.06.2023).
 24. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text> (дата звернення: 20.06.2023).
 25. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 20.06.2023).
 26. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 20.06.2023).
 27. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85: від 10.11.2015. К.: Національна поліція України, 2015. 9 с.
 28. Постанова Правління Національного банку України Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України від 12.08.2022 № 178. URL: <https://zakon.rada.gov.ua/laws/show/v0178500-22#Text> (дата звернення: 20.06.2023).
 29. ДСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD). Видання офіційне. Київ. Національний банк України. 2010. URL:

- <http://s-byte.com/useful/27002.pdf> (дата звернення: 20.06.2023).
30. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України // База даних «Законодавство України» /ВР України. URL: <http://zakon3.rada.gov.ua/laws/show/v0365500-11> (дата звернення: 20.06.2023).
 31. Постанова Правління Національного банку України від 14.04.2023 № 49 «Про затвердження Положення про використання засобів криптографічного захисту інформації Національного банку України» // База даних «Законодавство України»/Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/v0049500-23#Text> (дата звернення: 20.06.2023).
 32. Постанова Правління Національного банку України № 267 від 14 липня 2006 року. "Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці" // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/z0935-06#Text> (дата звернення: 20.06.2023).

Інформаційні ресурси в Інтернеті:

33. <http://www.bank.gov.ua/>
34. <http://ema.com.ua/>
35. <https://www.european-atm-security.eu/>
36. <https://cyberpolice.gov.ua/>
37. https://bank.gov.ua/admin_uploads/article/Tipovij_opis_PS_rezident.pdf
38. <https://novapay.ua/bezpeka/>