МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки, факультет № 4

ПРОГРАМА

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

125 "Кібербезпека" (Протидія кіберзлочинності; безпека інформаційних та комунікаційних систем)

Харків 2020

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО
Вченою радою
факультету № 4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки факультету № 4 (протокол від 15.09.2020 № 16).

Розробники:
Доцент кафедри інформаційних технологій та кібербезпеки факультету № 4, 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 інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент Тулупов В.В.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Програма вибіркової навчальної дисципліни складена відповідно до освітньої програми першого рівня вищої освіти спеціальності 125 "Кібербезпека" (Протидія кіберзлочинності, безпека інформаційних та комунікаційних систем).

Предметом вивчення навчальної дисципліни є організаційно-технічні аспекти забезпечення безпеки електронних платіжних систем.

Міждисциплінарні зв'язки. Навчальна дисципліна спирається на дисципліни: вища математика; інформаційні технології; алгоритмізація та програмування; операційні системи та комп'ютерні мережі, організація баз даних та знань; теорія інформації та кодування; прикладна криптологія, кібербезпека і формує знання для засвоєння дисциплін: цифрова криміналістика; управління та організація в сфері інформаційної безпеки.

Програма навчальної дисципліни складається з таких тем: «Електронні платіжні системи»; «Регуляторні вимоги до безпеки електронних платіжних систем»; «Протидія злочинам з платіжними інструментами».

1. Мета та завдання навчальної дисципліни

1.1. 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.

1.2. 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.

1.3. Згідно з освітньою програмою 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 стандарту безпеки даних галузі платіжних карток.

вміти: протидіяти злочинам з платіжними інструментами:

- з банкоматом;
- в торгівельно-сервісних підприємствах;
- з платіжною карткою;
- з реквізитами платіжних карток в торгівельно-сервісних підприємствах;
- з платіжними інструментами без присутності картки;
- в системах дистанційного банківського обслуговування.

1.4. Форма підсумкового контролю - залік.

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

1.5. 1.5 Програмні компетентності:

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)	ЗК 1	Здатність до абстрактного, логічного, критичного мислення та встановлення взаємозв'язків між явищами та процесами
Фахові компетентності спеціальності (ФК)	ФК 1	Здатність використовувати актуальні підходи та технології забезпечення кібербезпеки у поєднанні із потрібними програмними інструментами аналізу кіберзагроз

2. Короткий опис змісту навчальної дисципліни

Тема № 1. Електронні платіжні системи

Моделі трансакцій 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.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна:

1. 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 (дата звернення: 26.08.2020).
2. 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: 26.08.2020).
3. 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: 26.08.2020).

4. Про платіжні системи та переказ коштів в Україні: Закон України від 05.04.2001 № 2346-III // База даних «Законодавство України»/Верховна Рада України. URL:https://zakon.rada.gov.ua/laws/show/2346-14 (дата звернення: 26.08.2020).
5. Про цінні папери та фондовий ринок: 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: 26.08.2020).
6. Про електронні довірчі послуги: Закон України: 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: 26.08.2020).
7. 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: 26.08.2020).
8. Зацеркляний М.М., Мельников О.Ф. Основи економічної безпеки: Навчальний посібник. – К.: КНТ, 2009. 337 с.
9. 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. анжай, В.І. Стреляний. Харків, 2013.
10. Протидія злочинам у сфері використання платіжних інструментів. Матеріали тренінгу агентів і інспекторів кіберполіції. / OSCE. Харків, 2016.
11. Online-курс з Blockchain. URL:https://www.youtube.com/playlist?list=PLhZQuknA7yUBt82ow8rEfw_G8tNZjt3qB (дата звернення: 26.08.2020).
12. Математичні основи біткойн-блокчейну. URL: https://habr.com/comp/bitfury/blog/340378/ (дата звернення: 26.08.2020).
13. Бандурка О.М., Глущенко В.В., Глущенко А.С. Гроші і кредит. Підручник. 2-ге вид., доп. і перероб., «Магнолія 2006», 2018, 368 с.
14. 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.
15. Варцаба В.І., Заславська О.І. Сучасне банківництво: теорія і практика: Навч. посібник. Ужгород: Видавництво УжНУ «Говерла», 2018. 364 с.

Допоміжна:

16. ГСТУ 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: 26.08.2020).
17. 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: 26.08.2020).
18. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31 (02.08.1994), ст. 286 (зі змінами та доповненнями на 26.08.2020).
19. Постанова Правління Національного банку України від 26.11.2015 № 829. "Про затвердження нормативно-правових актів з питань інформаційної безпеки".
20. Постанова Правління Національного банку України № 267 від 14 липня 2006 року. "Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці".

Інформаційні ресурси в інтернеті:

21. http://www.bank.gov.ua/
22. http://ema.com.ua/
23. https://www.european-atm-security.eu/
24. https://www.pcisecuritystandards.org/

4. Засоби оцінювання здобувачів вищої освіти

З метою діагностики успішності навчання використовуються:

- поточне письмове опитування на семінарських заняттях по тематиці лекцій, що були прослухані;
- тематичні письмові самостійні роботи у формі рефератів;
- контроль за тестовими завданнями;
- підсумкове тестування з усієї дисципліни – залік (екзамен).

Питання, або тестові завдання, які виносяться на складання підсумкового контролю (залік, екзамен)

1. Розкрийте зміст етапів комерційної трансакції 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 трансакції?
8. Якими є основні види загроз, що порушують інтереси постачальника, при здійсненні комерційної трансакції?
9. Що відносяться до транзакцій, що здійснюються в середовищі «обличчя до обличчя» (Face-to-face environment)?
10. Що таке MCC 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 трансакційних 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 системі 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. На які питання у контексті системи банківської безпеки дають відповідь нормативні документи України?
27. Яка інформація відповідно до законодавства є об'єктом захисту?
28. Які функції покладені на НБУ щодо захисту інформації в банківській системі України?
29. Яка інформація в банківській системі складає державну таємницю?
30. Яка інформація відноситься до банківської таємниці?
31. Як законодавчо визначено поняття електронних документів?
32. Яким чином передбачено обіг електронних документів в інформаційно-телекомунікаційних системах?
33. Поясніть схематично принцип формування та перевірки електронного підпису.
34. Поясніть суть цифрових сертифікатів.
35. Наведіть та поясніть схему взаємодії суб'єктів правових відносин у сфері послуг електронного підпису.
36. Як законодавством визначені правила захисту інформації в інформаційно-телекомунікаційних системах?
37. Із чого складається система захисту інформації платіжних систем і переказу коштів?
38. Для яких приміщень банку визначені режимні вимоги та правила з технічного захисту інформації?
39. Які вимоги висуваються до приміщень банку, що визначені для захисту інформації.
40. Скільки передбачено рівнів резервування баз даних центра оброблення системи електронних платежів Національного банку (ЦОСЕП)?
41. Що забезпечує система захисту електронних банківських документів в СЕП?
42. Що входить до технологічних засобів безпеки СЕП?
43. Як здійснюється генерація та розподіл ключів електронного підпису в банку, який є учасником СЕП?
44. З чого складаються апаратні і програмні криптографічного захисту СЕП?

45. Яким чином в СЕП здійснюється накладання ЕП електронного банківського документу?
46. Яким чином в СЕП здійснюється перевірка ЕП електронного банківського документу?
47. Яким чином здійснюється шифрування електронних банківських документів в СЕП?
48. Які типи криптографічних ключів і для яких операцій використовуються в СЕП України?
49. Які носії ключової інформації передбачені для учасника СЕП?
50. Які організаційні заходи інформаційної безпеки необхідно здійснити учаснику СЕП?
51. Яким чином здійснюється контроль територіальним управлінням НБУ за виконанням вимог щодо захисту інформації банками учасниками СЕП?
52. Які основні порушення характерні в організації роботи із засобами захисту інформації НБ України?
53. Чи потрібно ліцензування діяльності у сфері криптографічного захисту інформації в банківській системі України?
54. Які основні нормативні документи розроблено в межах PCI SSC?
55. З яких кроків складається система сертифікації платіжних систем на відповідають стандарту PCI DSS?
56. Які організації залучаються до сертифікації платіжних систем на відповідають стандарту PCI DSS?
57. Що виступає в якості об’єктів захисту згідно стандарту PCI DSS?
58. Що відноситься до даних тримача карти і є об’єктом захисту?
59. З чого складається середовище даних тримачів карт?
60. Які вимоги стандарту PCI DSS направлені на створення і підтримку безпечної мережевої інфраструктури платіжної системи?
61. Які вимоги стандарту PCI DSS направлені на захист даних тримача карти в платіжній системі?
62. Які вимоги стандарту PCI DSS направлені на підтримку програми управління вразливостями в платіжній системі?
63. Які вимоги стандарту PCI DSS направлені на впровадження посилених засобів управління доступом в платіжній системі?
64. Які вимоги стандарту PCI DSS направлені на регулярний моніторинг і тестування мережевої інфраструктури в платіжній системі?
65. Як часто згідно стандарту PCI DSS потрібно проводити аналіз налаштувань міжмережевих екранів і маршрутизаторів?
66. Які згідно стандарту PCI DSS необхідно використовувати технології віддаленого адміністративного доступу?
67. Які дані згідно стандарту PCI DSS дозволяється зберігати в платіжній системі?
68. Як часто згідно стандарту PCI DSS потрібно перевіряти програмний код на наявність вразливостей?
69. Як часто згідно стандарту PCI DSS потрібно видалення заблокованих облікових записів?

70. Як часто згідно стандарту PCI DSS потрібна зміна пароля користувача?
71. Якими є вимоги стандарту PCI DSS до політики паролів?
72. Якщо інший термін не визначено законодавством, то згідно стандарту PCI DSS скільки потрібно зберігати дані, які зібрані камерами відеоспостереження?
73. Які події згідно стандарту PCI DSS потрібно протоколювати в платіжній системі?
74. Як часто згідно стандарту PCI DSS слід переглядати журнали протоколювання подій?
75. Як часто згідно стандарту PCI DSS слід аналізувати бездротові мережі з метою ідентифікації всіх використовуваних пристроїв?
76. Етапи злочинів з платіжними інструментами в банкоматах за класифікацією платіжної індустрії.
77. Форми злочинів з платіжними інструментами в банкоматах за класифікацією платіжної індустрії.
78. Види злочинів з платіжними інструментами в банкоматах за класифікацією платіжної індустрії.
79. Класифікація шахрайства в торгівельно-сервісних підприємствах.
80. Класифікація злочинців та різновидів шахрайства в торгівельно-сервісних підприємствах з ціллю компрометації карток.
81. Класифікація злочинців та різновидів шахрайства в торгівельно-сервісних підприємствах з ціллю здійснення шахрайських операцій.
82. Перелік інформації та джерел її отримання 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 та джерела витоку конфіденційної інформації (Data Breaches) про карткові реквізити.
86. Способи протиправного використання карткових реквізитів.
87. Шахрайство держателя платіжної картки.
88. Механізми безпеки ДБО.
89. Загальна схема злочину у ДБО.
90. Ознаки інциденту в системі ДБО.
91. Реагування на злочини з платіжними інструментами в банкоматах.
92. Реагування банків на несанкціоновані платежі.
93. Реагування поліції на несанкціоновані платежі.
94. Реагування на шахрайства держателів платіжних карток.