



МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх
справ

Факультет № 4

Кафедра протидії кіберзлочинності

Факультет № 6

Кафедра кібербезпеки та DATA-технологій


ЗАТВЕРДЖЕНО

На спільному засіданні кафедри
протидії кіберзлочинності факультету № 4
та кафедри кібербезпеки та DATA-
технологій факультету № 6
протокол № 2 від 22.06.2023
Завідувач кафедри
протидії кіберзлочинності факультету № 4
підполковник поліції

Олександр МАНЖАЙ

БЕЗПЕКА ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ (ВК.29)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	кібербезпеки та DATA-технологій факультету № 6 (http://www.univd.edu.ua/uk/dir/2826/kafedra-kiberbezpeky-ta-data-tekhnologiy)
Контактний телефон	+38 057 7398899 (раб.)
E-mail	kiberbezpekaf@gmail.com
ЛЕКТОР (ЛЕКТОРИ)	
	Онищенко Юрій Миколайович, доцент кафедри кібербезпеки та DATA-технологій факультету № 6, к.н.д.у, доцент moj@univd.edu.ua Лекційний потік: факультет № 6, шифр навчальних груп Ф6-Кбдб-21, Ф6-Кбзб-21.
Назва освітньо-професійної програми	Кібербезпека (безпека інформаційних та комунікаційних систем) Cybersecurity (security of information and communication)

	systems)
Рівень вищої освіти	Перший (бакалаврський) (НРК України – 6 рівень та перший цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Статус дисципліни	Вибіркова компонента освітньо-професійної програми, вивчається в 6 семестрі 3 курсу навчання
Мета вивчення дисципліни	<p>Ознайомлення здобувачів вищої освіти зі встановленими законодавством України та міжнародними стандартами вимог щодо забезпечення безпеки електронних платіжних систем та алгоритмами дій з протидії злочинам з платіжними інструментами.</p> <p>Засвоєння здобувачами вищої освіти знань з організаційно-технічних аспектів забезпечення безпеки електронних платіжних систем і вмінь протидіяти злочинам з платіжними інструментами.</p>
Завдання вивчення дисципліни	<p>Сформулювати у здобувачів вищої освіти знання щодо організаційно-технічних аспектів забезпечення безпеки електронних платіжних систем:</p> <ul style="list-style-type: none"> - теоретичних засад запобігання і протидії проявам кіберзлочинності у сфері електронних платіжних систем; - сучасного стану державного управління у сфері запобігання і протидії кіберзлочинам у сфері електронних платіжних систем в Україні та в інших країнах; - шляхів удосконалення запобігання і протидії кіберзлочинності у сфері електронних платіжних систем; - дотримання правил фінансової грамотності та кібергігієни у сфері електронних платіжних систем; - принципів роботи банківських електронних платіжних систем в комерційній діяльності; - складових інфраструктури електронних платіжних систем; - банківської системи України як об'єкта захисту; - вимог стандартів безпеки даних у галузі платіжних карток. <p>Виробити вміння та навички у здобувачів вищої освіти з протидії злочинам з платіжними інструментами:</p> <ul style="list-style-type: none"> - 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.
Обсяг дисципліни в кредитах ECTS/годинах	Кількість кредитів ECTS (загальний обсяг – 150 год.) 3 них (денна/заочна): - аудиторна робота: 74/22 год. - самостійна робота: 76/128 год.
Форми та види проведення навчальних занять	Форма навчання – денна Види навчальних занять: - лекції: 36 год.; - семінарські заняття: 0 год.; - практичні заняття: 38 год.; - лабораторні заняття: 0 год. Форма навчання – заочна Види навчальних занять: - лекції: 8 год.; - семінарські заняття: 0 год.; - практичні заняття: 14 год.; - лабораторні заняття: 0 год.
Самостійна робота	Опрацювання рекомендованої літератури, підготовка тез доповідей до конференцій, самостійне вирішення практичних завдань.
Індивідуальні завдання	Наукові доповіді, реферати
Необхідне обладнання	Мультимедійне обладнання (ноутбук та проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Мова викладання	Українська
Контроль	Поточний та підсумковий контроль Поточний: опитування на практичних заняттях; участь в дискусіях, веб-квестах, обговоренні доповідей, рефератів; підготовка рефератів та доповідей, тестування, виконання самостійних робіт, захист лабораторних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням. Підсумковий контроль: екзамен .
Інтегральна компетентність, загальні компетентності (ЗК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. 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.
Спеціальні компетентності (СК)	<p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>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.</p>
ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ	
Тема № 1. Електронні платіжні системи	
<ol style="list-style-type: none"> 1. Банківські електронні платіжні системи в комерційній діяльності 2. Складові інфраструктури електронних платіжних систем 	
Тема № 2. Регуляторні вимоги до безпеки електронних платіжних систем	
<ol style="list-style-type: none"> 1. Банківська система України як об'єкт захисту 2. Вимоги стандарту безпеки даних галузі платіжних карт 	
Тема № 3. Протидія злочинам з платіжними інструментами	
<ol style="list-style-type: none"> 1. Злочини з платіжними інструментами в банкоматі 2. Компрометація карток при шахрайстві в торгівельно-сервісних підприємствах 3. Шахрайські операції з реквізитами платіжних карток в торгівельно-сервісних підприємствах 4. Злочини з платіжними інструментами без присутності картки 5. Шахрайські операції з платіжною карткою 6. Злочини в системах дистанційного банківського обслуговування 	
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 частотої 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> <p>ПРН 46. Здійснювати аналіз та мінімізацію ризиків Обробки інформації в інформаційно-телекомунікаційних системах.</p>	
Критерії оцінювання результатів навчання	<p>Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю:</p> <ul style="list-style-type: none">- поточний контроль - 50 балів;- підсумковий контроль - 50 балів. <p>Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менш 3 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: самостійне вирішення практичних завдань, підготовку рефератів, тез доповідей на науково-практичні конференції тощо (здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5.</p> <p>Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (екзамені).</p>	
ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS		
Оцінка в	Оцінка за	Оцінка за шкалою ECTS

балах	національною шкалою	Оцінка	Пояснення
97-100	Відмінно ("зараховано")	А	„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")	В	„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		С	„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 носять 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
<p>Перелік питань, що виносяться на підсумковий контроль</p> <ol style="list-style-type: none"> 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 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. 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.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. 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.
2. 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).
3. 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.
4. Протидія злочинам у сфері використання платіжних інструментів. Матеріали тренінгу агентів і інспекторів кіберполіції. / OSCE. Харків, 2016.
5. Бандурка О.М., Глущенко В.В., Глущенко А.С. Гроші і кредит. Підручник. 2-ге вид., доп. і перероб., «Магнолія 2006», 2018, 368 с.
6. 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 ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. 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.
2. Міщенко С. Вдосконалення системи роздрібних безготівкових платежів / С. Міщенко// Вісник КНЕУ ім. Т.Г. Шевченка. Серія: Економіка. – 2014. – № 5. – С. 22–27.
3. Коваль Н. Особливості функціонування платіжних систем України на сучасному етапі їх розвитку. 2012. URL: <http://www.economy.nauka.com.ua/?op=1&z=1441>.
4. Шелудько С.А. Міжнародні стандарти банківської справи: навчальний посібник. — К.: Видавничий дім «Кондор», 2020. — 260 с.

Нормативно-правові акти:

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#Text> (дата звернення: 20.06.2023).

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: 20.06.2023).
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: 20.06.2023).
4. 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).
5. 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).
6. 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).
7. 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).
8. 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).
9. 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).
10. 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).
11. 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).
12. 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).
13. 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).

14. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85: від 10.11.2015. К.: Національна поліція України, 2015. 9 с.
15. 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).
16. 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).
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: 20.06.2023).
18. 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).
19. 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:

1. <http://www.bank.gov.ua/>
2. <http://ema.com.ua/>
3. <https://www.european-atm-security.eu/>
4. <https://cyberpolice.gov.ua/>
5. https://bank.gov.ua/admin_uploads/article/Tipovij_opis_PS_rezident.pdf
6. <https://novapay.ua/bezpeka/>