

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра кібербезпеки та DATA-технологій, факультет № 6

РОБОЧА ПРОГРАМА

навчальної дисципліни «Основи кібербезпеки»
обов'язкових компонент
освітньої програми першого рівня вищої освіти

125 Кібербезпека (безпека інформаційних та комунікаційних систем)

Харків 2023

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 (*протокол від 15.08.2023 № 8*)

Розробник:

Доцент кафедри кібербезпеки та DATA-технологій, к.ю.н., професор
Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ к.т.н., доцент;

Павликівський В.І., перший проректор Харківського університету, д.ю.н., професор

1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 3 Загальна кількість годин – 90 Кількість тем – 2	12 Інформаційні технології 125 Кібербезпека бакалавр	Навчальний курс 1 Семестр 1 Вид підсумкового контролю: - екзамен.
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання		заочна форма навчання
Лекції – 24; Лабораторні заняття – 12; Практичні заняття – 12; Самостійна робота – 42; Індивідуальні завдання: Реферати – 1		Лекції – 4; Лабораторні заняття – 2; Практичні заняття – 2; Самостійна робота – 82; Індивідуальні завдання: Реферати – 1

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Основи кібербезпеки» є засвоєння здобувачами вищої освіти правил поведінки з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки.

Міждисциплінарні зв'язки: «Інформаційні технології», «Кібербезпека», «Поліцейська діяльність у кіберсфері».

Завданнями вивчення дисципліни «Основи кібербезпеки» є дослідження принципів та методів безпечної роботи в комп'ютерних системах та мережах, ознайомлення з програмами, призначеними для захисту інформації та її носіїв, засвоєння правил налаштування програмного забезпечення, набуття знань і навичок використання технологій для побудови системи кібербезпеки.

Згідно з освітньою програмою здобувачі вищої освіти повинні:

знати:

- основні положення та терміни, що стосуються кібергігієни на робочому місці;
- заходи кібербезпеки на робочому місці;
- особливості дотримання правил кібербезпеки в системі публічної служби;

вміти:

- визначати заходи кібербезпеки для конкретної ситуації;
- оцінювати загрози та вживати заходів реагування на робочому місці;
- безпечно поводитись у кіберсфері;
- організовувати безпечний доступ до пристроїв і програм;
- критично оцінювати інформацію;

бути ознайомленими

- з основною нормативно-правовою базою у сфері кібербезпеки та інформаційної безпеки.

Програмні компетентності:

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов	
Загальні компетентності (ЗК)	ЗК.2	Знання та розуміння предметної області та розуміння професії
Програмні результати навчання (ПРН)	ПРН.15	використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
	ПРН.30	здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем
	ПРН.53	вирішувати задачі аналізу програмного коду на наявність можливих загроз

3. Програма навчальної дисципліни

Тема № 1. Загальні правила безпечної роботи з пристроями та програмами.

Захист персональних даних. Безпека мобільних пристроїв. Шкідливе програмне забезпечення. Фізична безпека. Убезпечення від неправдивих повідомлень.

Тема № 2. Базові правила убезпечення роботи в комп'ютерній мережі.

Соціальна інженерія. Безпечне користування мережею Інтернет. Безпечне користування електронною поштою. Безпека користування соціальними мережами. Реагування на інциденти безпеки інформації.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами, спеціалізація «безпека інформаційних та комунікаційних систем» (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 № 1							
Тема № 1 Загальні правила безпечної роботи з пристроями та програмами.	44	12	0	12	0	20	Екзамен
Тема № 2 Базові правила забезпечення роботи в комп'ютерній мережі	46	12	0	0	12	22	
Всього за семестр № 1:	90	24	0	12	12	42	

(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 № 1							
Тема № 1 Загальні правила безпечної роботи з пристроями та програмами.	44	2	0	2	0	40	Екзамен
Тема № 2 Базові правила забезпечення роботи в комп'ютерній мережі	46	2	0	0	2	42	
Всього за семестр № 1:	90	4	0	2	2	82	

4.1.3. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни		Література:
	Тема № 1. Загальні правила безпечної роботи з пристроями та програмами	
	Самостійно дослідити нормативно-правові акти, як регламентують правила кібербезпеки в державних органах	1-27, Інтернет

	Дослідити схеми вчинення кіберправопорушень та запропонувати власні методи протидії ним	1-27, Інтернет
	Підготувати реферат про досвід забезпечення кібербезпеки в одній із зарубіжних країн	1-27, Інтернет
	Тема № 2. Базові правила убезпечення роботи в комп'ютерній мережі	
	Встановити одну з ОС з підвищеним рівнем безпеки	1-27, Інтернет
	Вивчити термінологію, яка застосовується у середовищі фахівців у сфері кібербезпеки	1-27, Інтернет
	Заповнити таблицю «зручності» застосування різних сервісів для забезпечення безпеки інформації в мережі	1-27, Інтернет
	Вивчити методи убезпечення роботи в мережі	1-27, Інтернет

5. Індивідуальні завдання

5.1.1. Теми рефератів

1. Правове забезпечення у сфері інформаційної безпеки та кібербезпеки.
2. Порівняльний аналіз антивірусного програмного забезпечення.
3. Аналіз систем безпеки операційних систем.
4. Мандатна політика безпеки.
5. Дискреційна політика безпеки.
6. Безпека електронних платіжних систем.
7. Системи виявлення вторгнень.
8. Сканери вразливостей.
9. Послуги безпеки різних платформ електронної пошти.
10. Конфіденційність систем обміну електронними повідомленнями

5.1.2. Теми курсових робіт

1. Управління інцидентами інформаційної безпеки.
2. Безпека комунікацій.
3. Політика використання криптографічних ключів.
4. Забезпечення безпеки автентифікаційними даними користувачів та системи управління ними.
5. Обмеження доступу до інформації та процедури забезпечення безпечного підключення.
6. Зміст політики використання криптографічних засобів.
7. Політики резервного копіювання інформації.
8. Використання засобів штучного інтелекту для убезпечення в кіберсфері.
9. Кібергігієна дітей.
10. Роль кіберполіції у виконанні стратегії кібербезпеки України.
11. Правила кібергігієни на об'єктах критичної інфраструктури.
12. Кібербезпека в мережі Інтернет речей (IoT) та проблеми захисту підключених пристроїв.

5.1.3. Теми наукових робіт

1. Політики, процедури та заходи безпеки обміну інформацією.
2. Заходи захисту електронного обміну повідомленнями.

3. Зміст процедур ідентифікації, збирання, отримання і зберігання інформації, яку можна використовувати як електронні докази.
4. Аналіз загроз та вразливостей критичної кіберінфраструктури.
5. Розробка та вдосконалення методів виявлення та запобігання кібератакам.
6. Роль соціальної інженерії в кіберзлочинності та механізми її протидії.
7. Кібербезпека в інтернет-офісах та хмарних сервісах.
8. Розвиток інструментів для аналізу кіберзагроз та прогнозування їхнього розвитку.
9. Аналіз механізмів кібершпигунства та розробка заходів протидії.
10. Кібергігієна щодо мобільних застосунків та мобільних пристроїв.

6. Методи навчання

Лекції із застосуванням мультимедійного проектора; семінарські заняття: моделювання ситуативних задач, дебати, тренінги, рольові та ігрові заняття, розв'язання задач тощо.

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

1. Як називається параметр, який можуть підмінити зловмисники під час телефонування, для того щоб особа вважала, що спілкується з довіреним номером?
2. Які заходи слід вжити для убезпечення мобільного пристрою від несанкціонованого фізичного доступу?
3. На Ваш телефон надійшло повідомлення з телефону начальника про прохання надіслати службовий документ на пошту pp_minko_pp@mail.ru. Яких заходів Ви будете вживати?
4. Від невідомого контакта Вам на телефон надійшло повідомлення про те, що в районі Вашого проживання протягом тижня буде вимкнено електроенергію на пів доби. Також було залишено посилання, де можна переглянути графік відключень. При переході за посиланням у телефоні з'явилося попередження про встановлення якоїсь програми (apk) на телефон. Якими будуть Ваші дії?
5. Інструменти ведення пропаганди.
6. Що таке фейк?
7. Ознаки фейків?
8. Способи протидії неправдивим повідомленням.
9. Що належить до персональних даних про особу?
10. Який з видів інформації не належить до інформації з обмеженим доступом?
11. Що таке «інформація про фізичну особу (персональні дані)» відповідно до Закону України «Про інформацію»?
12. Якого головного правила слід дотримуватись для безпечного користування електронною поштою?
13. Загрози під час користування поштовою скринькою.
14. Ви отримуєте листа від представника Адміністрації Президента України. Який з нижченаведених пунктів найбільше викликав би у Вас довіру?

15. Чому листи, які містять у собі пароль для відкриття файлу в застосунку, викликають велику підозру?
16. Ризики використання неліцензованого програмного забезпечення.
17. Що таке вірус-вимагач?
18. Що є ознакою, що Ваш комп'ютер, імовірно, інфіковано вірусом?
19. Чому НЕ рекомендовано вставляти невідомі флеш-носії в комп'ютер своєї установи?
20. Що означає атака «людина посередині»?
21. Що НЕ є загрозою при крадіжці мобільного пристрою?
22. Що таке соціальна інженерія?
23. Що таке фішинг?
24. Ознаки фішингового листа.
25. Ваш друг попросив Вас у месенджері перекинути йому на карту 1000 грн. Ваші дії?
26. Вам потрібно встановити додаток на Ваш комп'ютер. У пошуковій системі Ви побачили декілька посилань, що пропонували завантаження такого додатку. Звідки Ви його будете завантажувати?
27. Користуючись мережею Інтернет з дому, Ви раптово побачили, що спроба дістатись пошукової системи викликала в браузері повідомлення про підозрілий недовірений сертифікат. Що Ви зробите?
28. Чому користування соціальними мережами безкоштовне для користувачів?
29. Які паролі є надійними?
30. Хто відповідає за конфіденційність інформації в соціальних мережах?

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи оцінювання результатів навчання включають в себе поточний та підсумковий контроль.

Засобами оцінювання результатів навчання можуть бути екзамени (комплексні екзамени); тести; наскрізні проекти; командні проекти; аналітичні звіти, реферати, есе; розрахункові та розрахунково-графічні роботи; презентації результатів виконаних завдань та досліджень; завдання на лабораторному обладнанні, тренажерах, реальних об'єктах тощо; інші види індивідуальних та групових завдань.

Поточний контроль. До форм поточного контролю належить оцінювання:

- рівня знань під час семінарських, практичних, лабораторних занять;
- якості виконання самостійної роботи.

Поточний контроль здійснюється під час проведення семінарських, практичних та лабораторних занять і має на меті перевірку набутих здобувачем вищої освіти (далі – здобувач) знань, умінь та інших компетентностей 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 роботу виставляються в журналі 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 (семінарські, практичні, лабораторні тощо); самостійна робота (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 формі, передбаченій в робочою програмою 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**.

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

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).

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

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.

$$\text{Підсумкові бали навчальної дисципліни} = \frac{\text{Підсумкові бали за поточний семестр} + \text{Підсумкові бали за попередній семестр}}{2}$$

У цьому розділі також повинні бути розроблені чіткі критерії оцінювання здобувачів вищої освіти під час поточного контролю (*робота на семінарських, практичних, лабораторних та інших аудиторних заняттях, самостійна робота, виконання індивідуальних творчих завдань*) та підсумкового контролю. Кафедра визначає вимоги до здобувачів стосовно засвоєння змісту навчальної дисципліни, а саме: кількість оцінок, яку він повинен отримати під час аудиторної роботи, самостійної роботи. Наприклад:

Робота під час навчальних занять	Самостійна робота	Підсумковий контроль
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, виконати практичне завдання тощо	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 засвоєний цілком, потрібні практичні навички роботи з освоєним матеріалом сформовані, усі 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 засвоєний цілком, потрібні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання, виконані, якість виконання жодного з них не оцінена мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією-двома значними 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 засвоєний частково, але прогалини не носять істотний характер, потрібні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконана, деякі з виконаних завдань містять помилки, робота з трьома значними помилками
65-69			
60-64		E	«Достатньо» – теоретичний зміст курсу засвоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконана або якість виконання деяких з них оцінена числом балів, близьким до мінімального, робота, що задовольняє мінімуму критеріїв оцінки
40-59	Незадовільно («не зараховано»)	FX	«Умовно незадовільно» – теоретичний зміст курсу засвоєний частково, потрібні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконана, 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 освоєний, потрібні практичні навички роботи несформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значного підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

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

Основна

1. Oles N. How to Catch a Phish: A Practical Guide to Detecting Phishing Emails. Apress Berkeley, CA, 2023. 147 p. DOI: <https://doi.org/10.1007/978-1-4842-9361-4>.
2. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: наук.-практ. посіб. Київ: К.І.С., 2021. 160 с. URL: <https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69>.
3. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с.
4. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>

5. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О. В. Манжай, В. В. Носов. К. : ВАІТЕ, 2021. 106 с.

6. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М.Барановський, В.В.Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. Київ: ВАІТЕ, 2021. 262 с.

Допоміжна

7. Манжай О. В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня. 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 65-67.

8. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня. 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 72-73.

9. Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. In: Gruschka N. (eds) Secure IT Systems. NordSec 2018. *Lecture Notes in Computer Science*. 2020. Vol. 11252. Springer, Cham. (DOI: 10.1007/978-3-030-03638-6_18).

10. Pfleeger S. L., Sasse M. A., Furnham A. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*. 2014. Vol. 11. Iss. 4. pp. 489-510. (DOI: 10.1515/jhsem-2014-0035).

11. Review of cyber hygiene practices (December 2016). European Union Agency For Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport, p. 4.

12. Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*. 2020. Vol. 128 (DOI: 10.1016/j.dss.2019.113160).

13. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.

14. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

15. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11 березня 2021 року, введено в дію Указом Президента України від 19 березня 2021 року № 106/2021. URL: <https://zakon.rada.gov.ua/laws/show/106/2021#Text>.

16. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 10.05.2023).

17. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL:

<https://zakon.rada.gov.ua/laws/show/447/2021#Text> (дата звернення: 10.05.2023).

18. Про захист персональних даних: закон України від 01.06.2010; [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 49 (09.07.2010), стор. 199, стаття 1604.

19. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06; [із змінами і доповненнями]. *Офіційний вісник України*. 2006. № 13 (12.04.2006), стор. 164, стаття 878.

20. Про доступ до публічної інформації: закон України від 13.01.2011; [із змінами і доповненнями]. *Офіційний вісник України*. 2011. № 10 (18.02.2011), стор. 29, стаття 446.

21. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. *Баланс*. 2014, № 19, С. 5. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n11.

22. Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.

23. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *Офіційний вісник Європейського Союзу*. 04.05.2016. L 119. С. 1. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

24. 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>.

25. Про електронні комунікації: Закон України від 16.12.2020 : [із змінами і доповненнями]. *Офіційний вісник України*. 2021. № 6 (21.01.2021). Ст. 306.

Інформаційні ресурси в Інтернеті

26. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

27. Ви вмієте розпізнавати фішинг? URL: <https://phishingquiz.withgoogle.com/?hl=uk>.