МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Кафедра кримінального процесу

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

для підготовки до практичних занять та самостійної роботи
здобувачів першого (бакалаврського) рівня вищої освіти
в галузі знань 12 «Інформаційні технології»
спеціальність: 125 «Кібербезпека та захист інформації»

Одеса
2025

УДК 343.13:007:004.056(094)(073)
Н832

Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»
(*протокол № 4 від «10» лютого 2025 р.*)

Укладачі:

Аркуша Л.І., доктор юридичних наук, професор, завідувач кафедри криміналістики, детективної та оперативно-розшукової діяльності, Голова Комітету з питань юридичної освіти та науки НААУ

ORCID iD: *https://orcid.org/0000-0002-0422-6416*

Дикий О.В., кандидат юридичних наук, доцент, декан Факультету кібербезпеки та інформаційної діяльності, доцент кафедри кримінального процесу

ORCID iD: *https://orcid.org/0000-0001-9659-9350*

Мандриченко Ж.В., кандидат юридичних наук, доцент, доцент кафедри кримінального процесу

ORCID iD: https://orcid.org/0000-0002-9114-3044

Стоянов М.М., кандидат юридичних наук, доцент, доцент кафедри кримінального процесу

ORCID iD: https://orcid.org/0000-0003-4948-3288

Сидорчук В.В., доктор філософії в галузі права, старший викладач кафедри кримінального процесу

ORCID iD: https://orcid.org/*0000-0001-8457-1633*

Рецензенти:

Подобний О.О. – д.ю.н., професор, завідувач кафедри кримінального права, процесу та криміналістики Міжнародного гуманітарного університету;

Цехан Д.М. – д.ю.н, професор, професор кафедри криміналістики, детективної та оперативно-розшукової діяльності Національного університету «Одеська юридична академія».

Н832 **Нормативно-правове забезпечення кібербезпеки** : метод. реком. для підготовки до практ. занять та самост. роботи здобув. першого (бакалаврського) рівня вищ.осв. галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації» [Електронне видання] / уклад.: Аркуша Л.І., Дикий О.В., Мандриченко Ж.В., Стоянов М.М., Сидорчук В.В.; Нац. ун-т «Одеська юрид. академія». Одеса, 2025, 59 с.

Методичні рекомендації призначені для підготовки до практичних занять та самостійної роботи здобувачів першого (бакалаврського) рівня вищої освіти в галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації» з метою закріплення лекційного матеріалу і підготовки до практичних і самостійних занять з дисципліни «Нормативно-правове забезпечення кібербезпеки».

УДК 343.13:007:004.056(094)(073)

ЗМІСТ

ВСТУП 4

КРИТЕРІЇ ОЦІНЮВАННЯ ПІД ЧАС ПОТОЧНОГО КОНТРОЛЮ 9

Тема 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ 13

Тема 2. КІБЕРРИЗИКИ, КІБЕРЗАГРОЗИ ТА КІБЕРАТАКИ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ 15

Тема 3. СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ 17

Тема 4. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІБЕРБЕЗПЕКИ ДЕРЖАВИ. КІБЕРЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 20

Тема 5. ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА УКРАЇНИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ 22

Тема 6. ДЕРЖАВНІ СТАНДАРТИ УКРАЇНИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ 27

Тема 7. НОРМАТИВНІ ДОКУМЕНТИ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ 30

Тема 8. МІЖНАРОДНІ СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ 32

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ І ВМІНЬ 36

РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ 43

ВСТУП

Навчальна дисципліна «Нормативно-правове забезпечення кібербезпеки» призначена для здобувачів, які навчаються за освітньою програмою підготовки бакалаврів з галузі знань 12 «Інформаційні технології» спеціальність 125 «Кібербезпека та захист інформації» в Національному університеті «Одеська юридична академія».

Навчальна дисципліна «Нормативно-правове забезпечення кібербезпеки» присвячена знайомству здобувачів із чинним нормативно-правовим регулюванням, яке покликано забезпечити як у державі в цілому, так і щодо окремих об'єктів критичної інфраструктури чи державних інституцій, безпеку у кіберпросторі. Це на сьогоднішній день, зважаючи на актуальність та рівень розповсюдження інформаційних технологій, є одним із пріоритетних завдань державної політики.

Предмет навчального курсу складають норми права, які у своїй сукупності регулюють питання кібербезпеки.

Метою відповідного курсу є надання уявлення про чинне нормативно-правове забезпечення кібербезпеки, ієрархії нормативно-правових актів, та кола питань, які вони регламентують.

Основними **завдання** курсу є:

- надання загальної характеристики кібернетичної безпеки;
- визначення нормативно-правового регулювання кібербезпеки в Україні;
- окреслення суб'єктів забезпечення кібербезпеки;
- визначення категорії «кіберризик», «кіберзагроза», «кібератака» та «шкідливе програмне забезпечення»;
- систематизація організаційно-правового забезпечення кібербезпеки;
- ознайомлення здобувачів з державними стандартами в галузі кібербезпеки;
- дослідження міжнародних стандартів в галузі кібербезпеки;

- окреслення нормативних документів технічного захисту інформації.

Після закінчення курсу здобувач повинен **знати**:

- основні категорії у сфері забезпечення захисту кібербезпеки;
- визначення та класифікацію кіберзагроз і кібератак;
- загальні положення кібербезпекової політики України;
- систему суб'єктів забезпечення кібербезпеки за чинним законодавством України;
- поняття, ознаки, джерела та види кіберризиків;
- поняття та ознаки кібератаки, можливі типи атак на інформаційні системи;
- поняття, сутність та класифікація кіберзлочинів;
- нормативно правові акти, які складають правову основу забезпечення кібербезпеки України;
- роль інформаційної безпеки та кібербезпеки у системі національної безпеки;
- нормативне регулювання питання охорони персональних даних;
- державне регулювання охорони персональних даних;
- основні Державні Стандарти України в галузі кібербезпеки;
- наявні нормативні документи з технічного захисту інформації;
- міжнародні стандарти в галузі кібербезпеки.

Після закінчення відповідного курсу здобувач повинен **вміти**:

- реалізовувати окремі засоби попередження та боротьби з кібертероризмом;
- використовувати закріплені у нормативно-правових джерелах норми для забезпечення кібербезпеки та боротьби з кіберзагрозами;
- визначати суб'єктів забезпечення кібербезпеки за чинним законодавством України;

- комунікувати з Департаментом кіберполіції Національної поліції України, Національним координаційним центром кібербезпеки, Державною службою спеціального зв'язку та захисту інформації України, Державним центром кіберзахисту та протидії кіберзагрозам;
- визначати кіберризики їх види, джерела та форми;
- класифікувати кібердіяльність як кіберзлочин;
- визначати детермінанти кіберзлочинності, надавати характеристику кіберзлочинності;
- визначати нормативно правові акти, які складають правову основу забезпечення кібербезпеки України;
- обґрунтовувати яким чином закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації сприяють організаційно-правовому забезпеченню кібербезпеки;
- визначати поняття та зміст інформаційної безпеки і кібербезпеки у системі національної безпеки;
- визначати та протидіяти міжнародному інформаційному тероризму та кібертероризму,
- розуміти напрями та забезпечувати безперебійну, захищену роботу критичної інфраструктури;
- сприяти охороні персональних даних та права власності.

Методи викладання і навчання передбачають використання мультимедійного обладнання та проведення окремих практичних занять в спеціалізованих комп'ютерних класах за комп'ютерними робочими місцями для перевірки знань здобувачів та формальної і змістовної підготовки здобувачів до ЄДКІ.

Перелік тем практичних робіт:

Практичне заняття 1	Загальна характеристика кібернетичної безпеки	2 години
Практичне заняття 2	Кіберризики, кіберзагрози та кібератаки. Шкідливе програмне забезпечення	2 години
Практичне заняття 3	Суб'єкти забезпечення кібербезпеки	2 години
Практичне заняття 4	Забезпечення кібербезпеки держави. Кіберзахист критичної інфраструктури	2 години
Практичне заняття 5	Законодавча та нормативно-правова база України в галузі інформаційної та кібербезпеки	4 години
Практичне заняття 6	Державні Стандарти України в галузі інформаційної та кібербезпеки	2 години
Практичне заняття 7	Нормативні документи з технічного захисту інформації	2 години
Практичне заняття 8	Міжнародні стандарти в галузі інформаційної та кібербезпеки	4 години

Перелік тем самостійної роботи:

Самостійна робота 1	Загальна характеристика кібернетичної безпеки	10години
Самостійна робота 2	Кіберризики, кіберзагрози та кібератаки. Шкідливе програмне забезпечення	10 години
Самостійна робота 3	Суб'єкти забезпечення	10 години

	кібербезпеки	
Самостійна робота 4	Забезпечення кібербезпеки держави. Кіберзахист критичної інфраструктури	10 години
Самостійна робота 5	Законодавча та нормативно-правова база України в галузі інформаційної та кібербезпеки	10 години
Самостійна робота 6	Державні Стандарти України в галузі інформаційної та кібербезпеки	10 години
Самостійна робота 7	Нормативні документи з технічного захисту інформації	10 години
Самостійна робота 8	Міжнародні стандарти в галузі інформаційної та кібербезпеки	10 години

Правильність виконаних практичних і самостійних робіт перевіряє викладач.

Основними формами освітнього процесу є лекційні, практичні заняття, консультування та самостійна робота здобувача.

Форми контролю: поточний та підсумковий (іспит)

КРИТЕРІЇ ОЦІНЮВАННЯ ПІД ЧАС ПОТОЧНОГО КОНТРОЛЮ

Таблиця 1. Шкала оцінювання навчальної діяльності теоретичної частини здобувача вищої освіти

Оцінка за шкалою силабусу	**Кількість набраних балів**	**Критерії оцінювання**
		Здобувач вищої освіти
A	90–100	виявив високу теоретичну підготовку, вміння аналізувати літературу, логічно та послідовно викладати фактичний матеріал, робити висновки. У процесі виконання практичної роботи чи аналізу поставлених завдань показує вміння планувати, ставити та інтерпретувати отримані результати відповідно до досягнень науки
B	82–89	виявив високий рівень теоретичних знань програмного матеріалу, вміння послідовно його викласти та застосувати засвоєні знання у процесі постановки і виконання практичної роботи, але допускає несуттєві неточності у відповідях, невеликі помилки у застосуванні теоретичних знань при виконанні практичних завдань
C	74–81	в основному правильно висвітлив питання, але допускає несуттєві помилки у ході розв’язання завдань і показує задовільні знання теоретичного матеріалу
D	64–73	в основному правильно висвітлив питання, але допускає суттєві помилки у ході розв’язання завдань і показує задовільні знання теоретичного матеріалу

E	60–63	правильна, але неповна відповідь, яка свідчить про те, що здобувач вищої освіти вивчав матеріал, але не може логічно та повно висловити свою думку та застосувати його при виконанні практичних завдань

Таблиця 2. Шкала оцінювання навчальної діяльності практичної частини здобувача вищої освіти

Оцінка за шкалою силабусу	**Кількість набраних балів**	**Критерії оцінювання**
		Здобувач вищої освіти
A	90–100	здобувач має набрати більше, або 85% правильних відповідей на тестуванні, за відведений час, який визначається з розрахунку 1 хвилина на 1 запитання, у випадку якщо питома вага питання тестування складає більше 5%, допускається зниження загального % правильних відповідей не менше ніж 82%
B	82–89	здобувач має набрати від 75% до 85% правильних відповідей на тестуванні, за відведений час, який визначається з розрахунку 1 хвилина на 1 запитання, у випадку якщо питома вага питання тестування складає більше 5%, допускається зниження загального % правильних відповідей не менше ніж 72%
C	74–81	здобувач має набрати від 65% до 75% правильних відповідей на тестуванні, за відведений час, який визначається з розрахунку 1 хвилина на 1 запитання, у випадку якщо питома вага питання тестування складає більше 5%, допускається зниження загального % правильних відповідей не менше ніж 62%
D	64–73	здобувач має набрати від 55% до 65% правильних відповідей на тестуванні, за відведений час, який визначається з розрахунку 1 хвилина на 1

		запитання, у випадку якщо питома вага питання тестування складає більше 5%, допускається зниження загального % правильних відповідей не менше ніж 62%
E	60–63	здобувач має набрати від 40% до 55% правильних відповідей на тестуванні, за відведений час, який визначається з розрахунку 1 хвилина на 1 запитання

Тема 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Практичне заняття 1

1. Основні категорії у сфері забезпечення захисту кібербезпеки.
2. «Комп'ютерна інформація», комплексна система захисту інформації. Інформаційна безпека та інформаційна інтервенція.
3. Кіберпростір: визначення, ознаки, юрисдикція.
4. Кібербезпека та кіберзахист: сутність та об'єкти.
5. Кібертероризм: поняття та засоби попередження та боротьби.
6. Кіберзагрози та кібератаки: визначення та класифікації. Кримінальні кіберзагрози.

Методичні рекомендації

Під час вивчення теми здобувачам потрібно звертати увагу на закріплені в законодавстві поняття в сфері забезпечення кібербезпеки. Досліджуючи поняття «комп'ютерна інформація», здобувач має визначитись із засобами, які забезпечують захист відповідної інформації, сприяють інформаційній безпеці та захисту від можливих інформаційних інтервенцій. При дослідженні поняття «кіберпростір» – необхідно звернути увагу на правовідносини, на які він розповсюджується, оскільки вони формують його межу. Категорія «кібербезпека» має нерозривно розглядатись з категорією «кіберзахист», необхідно звернути увагу на їх об'єкти. Під час розгляду поняття «кібертероризму» варто визначитись із засобами, які можуть використовуватись зловмисниками, напрямами їх злочинної діяльності, а також існуючими засобами їх попередження та боротьби. Під час дослідження понять «кіберзагроза» та «кібератака», здобувачі мають звернути увагу на їх класифікації, можливі методи або алгоритми дій зловмисників та можливі кримінальні кіберзагрози, які з огляду на це наявні.

Самостійна робота 1

Здобувачу необхідно надати відповідь на такі питання:

1. Які основні категорії характеризують захист кібербезпеки?

2. Як співвідносяться між собою поняття інформаційна безпека та інформаційна інтервенція?

3. Визначити коло відносин, на які розповсюджується кіберпростір.

4. Які ознаки характеризують поняття кібербезпеки та кіберзахисту?

5. Кібертероризм, які існують засоби попередження та боротьби?

6. Як співвідносяться між собою поняття кіберзагроза та кібератака?

7. Які складові Стратегії забезпечення кримінологічної кібербезпеки, ви б могли запропонувати?

8. Пройдіть тестування, попередньо зареєструвавшись у викладача (здійснює реєстрацію у Moodle), який веде практичні заняття у відповідній групі, за наступною електронною адресою: http://cyber.onua.edu.ua/mod/quiz/view.php?id=4743

або відсканувавши QR-код:

Тема 2. КІБЕРРИЗИКИ, КІБЕРЗАГРОЗИ ТА КІБЕРАТАКИ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Практичне заняття 2

1. Кіберризики: поняття, ознаки, підходи до розуміння.
2. Види кіберризиків. Джерела та форми кіберризиків.
3. Кіберзагроза: поняття та форми реалізації.
4. Джерела кіберзагроз, методи протистояння.
5. Кібератака: поняття, ознаки. Типи атак на інформаційні системи. Шкідливе програмне забезпечення як засіб кібератак.
6. Кіберзлочини: поняття, сутність та класифікація.
7. Кіберзлочинність: сучасний стан та детермінація. Кримінологічна характеристика кіберзлочинців.
8. Протидія кіберзлочинності: вітчизняний та зарубіжний досвід.

Методичні рекомендації

Під час дослідження питання кіберризиків здобувачам потрібно детальніше звернути увагу не тільки на поняття відповідної категорії, але і його ознаки та підходи до розуміння, які наявні в науковій літературі. Також варто дослідити і види кіберризиків, а також їх можливі джерела та наявні форми. Знайомлячись із категорією кіберзагрози здобувачі мають дослідити її поняття, зміст та можливі форми реалізації для подальшого визначення джерел кіберзагроз та наявних методів протидії їм. Розглядаючи поняття кібератаки, здобувач має виділити її ознаки, а також існуючі типи атак на інформаційні системи, визначитись із засобами, які використовують для здійснення кібератаки, в тому числі, і шкідливе програмне забезпечення. Відповідні знання дадуть змогу визначитись із вимогами та змістом до системи виявлення мережевих вторгнень і ознак кібератак. Окрему увагу необхідно приділити тим кібератакам, за вчинення яких передбачена кримінальна відповідальність, та які в загальному формують кіберзлочини.

Що тягне за собою необхідність також дослідити і таке явище як кіберзлочинність, її характеристику та детермінацію. У підсумку, отриманні знання мають сприяти подальшому дослідженню та пропозиціям здобувачів щодо напрямів протидії кіберзлочинності.

Самостійна робота 2

Здобувачу необхідно надати відповідь на такі питання:

1. Вкажіть поняття та підходи до розуміння кіберризиків.

2. Які існують джерела кіберризиків?

3. Дайте визначення поняттю «кіберзагроза», та вкажіть можливі методи протистояння кіберзагрозам.

4. Охарактеризуйте кібератаку, вкажіть типи атак на інформаційні системи.

5. Надайте визначення кіберзлочину. Окресліть сучасний стан та детермінацію кіберзлочинності.

6. Пройдіть тестування, попередньо зареєструвавшись у викладача (здійснює реєстрацію у Moodle), який веде практичні заняття у відповідній групі, за наступною електронною адресою: http://cyber.onua.edu.ua/mod/quiz/view.php?id=3655

або відсканувавши QR-код:

Тема 3. СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Практичне заняття 3

1. Система суб'єктів забезпечення кібербезпеки за чинним законодавством України.
2. Завдання та повноваження Департаменту кіберполіції Національної поліції України.
3. Національний координаційний центр кібербезпеки: основні напрями діяльності та повноваження.
4. Державна служба спеціального зв'язку та захисту інформації України: основні завдання та повноваження.
5. Державний центр кіберзахисту: структура та основні напрями діяльності.

Методичні рекомендації

Під час вивчення теми здобувачам потрібно детальніше звернути увагу на зв'язок суб'єктів забезпечення кібербезпеки із категорією система забезпечення безпеки, оскільки вони забезпечують досягнення поставлених задач і мети забезпечення системи кібербезпеки. Важливим є розуміння наявності «загальних» суб'єктів кібербезпеки, які характеризуються тим, що лише окремі їх повноваження направлені на формування, забезпечення та підтримку функціонування існуючої системи забезпечення кібербезпеки, а також опосередкованістю впливу їх повноважень на існуючу систему забезпечення кібербезпеки або стратегічно-нормативним характером забезпечення ними кібербезпеки. До них відносяться міністерства, центральні органи виконавчої влади, місцеві державні адміністрації, органи місцевого самоврядування, правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності. Що ж стосується «спеціальних» суб'єктів кібербезпеки, то вони характеризуються направленістю абсолютної більшості їх повноважень до

безпосереднього забезпечення кібербезпеки, та в своїй сукупності формують критичну сукупність суб'єктів, що забезпечують тактичну та операційну кібербезпеку. Серед яких, під час підготовки до практичних занять, варто приділити увагу Департаменту кіберполіції Національної поліції України, Національному координаційному центру кібербезпеки, Державній службі спеціального зв'язку та захисту інформації України та Державному центру кіберзахисту (CERT-UA) та іншим. Під час дослідження їх компетенції та місця серед суб'єктів забезпечення кібербезпеки, необхідно користуватись актуальними нормативно-правовими актами, які регулюють їх діяльність та офіційними веб-сайтами зазначених суб'єктів, на яких наявні звіти щодо їх роботи.

Самостійна робота 3

Здобувачу необхідно надати відповідь на такі питання:

1. Зазначте про існуючу систему суб'єктів забезпечення кібербезпеки за чинним законодавством України.

2. Які завдання та повноваження наявні у Департаменту кіберполіції Національної поліції України?

3. Місце Національного координаційного центру кібербезпеки в системі забезпечення кібербезпеки.

4. Охарактеризуйте функції Державної служби спеціального зв'язку та захисту інформації України.

5. Яка структура та основні напрями діяльності Державного центру кіберзахисту?

6. Пройдіть тестування, попередньо зареєструвавшись у викладача (здійснює реєстрацію у Moodle), який веде практичні заняття у відповідній групі, за наступною електронною адресою: http://cyber.onua.edu.ua/mod/quiz/view.php?id=5279

або відсканувавши QR-код: 

Тема 4. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІБЕРБЕЗПЕКИ ДЕРЖАВИ. КІБЕРЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Практичне заняття 4

1. Інформаційна безпека та кібербезпека у системі національної безпеки.
2. Міжнародний інформаційний тероризм та кібертероризм як загроза національній безпеці.
3. Поняття та методи кібервійни. Кіберконфлікт.
4. Критична інфраструктура: поняття та об’єкти.
5. Основні вимоги захисту критичної інфраструктури від кібернетичних загроз.

Методичні рекомендації

Під час вивчення теми здобувачам потрібно детальніше звернути увагу на те, що інформаційна безпека та кібербезпека займають важливе місце у сучасній системі національної безпеки, що пояснюється активним використанням здобутків науково-технічного прогресу в державному управлінні та державній інфраструктурі. У відповідному контексті варто звернути увагу на міжнародний інформаційний тероризм та кібертероризм як загрозу національній безпеці. З огляду на що, здобувачам обов’язково необхідно дослідити існуючі поняття та методи кібервійни, а також зміст поняття кіберконфлікту та його можливі наслідки для критичної інфраструктури держави. Здобувачам необхідно приділити увагу і на визначення та складові (об’єкти) критичної інфраструктури, а також на існуючі законодавчі та доктринальні підходи щодо основних вимог захисту критичної інфраструктури від кібернетичних загроз.

Самостійна робота 4

Здобувачу необхідно надати відповідь на такі питання:

1. Яке місце посідає інформаційна безпека та кібербезпека у системі національної безпеки?

2. Яким чином міжнародний інформаційний тероризм та кібертероризм становлять загрозу національній безпеці?

3. Надайте поняття кібервійни, які існують їх методи?

4. Надайте поняття критичної інфраструктури та вкажіть об’єкти критичної інфраструктури.

5. Які існують основні вимоги захисту критичної інфраструктури від кібернетичних загроз?

6. Пройдіть тестування, попередньо зареєструвавшись у викладача (здійснює реєстрацію у Moodle), який веде практичні заняття у відповідній групі, за наступною електронною адресою: http://cyber.onua.edu.ua/mod/quiz/view.php?id=3655

або відсканувавши QR-код:

Тема 5. ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА УКРАЇНИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

Практичне заняття 5

1. Нормативно-правові акти, які складають правову основу забезпечення кібербезпеки України, їх структура та види.
2. Нормативно-правові акти, що регламентують загальні питання кібербезпеки. Стратегія кібербезпеки України.
3. Закони України, які дають визначення інформації, її видів та порядку використання.
4. Закони України, що визначають вимоги щодо захисту інформації.
5. Закони України, що регламентують інформацію з обмеженим доступом.
6. Нормативно-правові документи, що встановлюють умови кіберзахисту об’єктів критичної інфраструктури.
7. Кримінальна відповідальність як засіб забезпечення кібербезпеки.

Методичні рекомендації

Під час вивчення теми здобувачам потрібно детальніше звернути увагу на ієрархію нормативно-правових актів, які формують організаційно-правове забезпечення кібербезпеки. Під час дослідження їх змісту необхідно обов’язково визначитись із колом правовідносин у сфері кібербезпеки, на які розповсюджується той чи інший нормативно-правовий акт, та яка його роль у забезпеченні цілісності системи кібербезпеки. Важливу увагу слід приділити Конституції України та законам України: Про національну безпеку, Про засади внутрішньої і зовнішньої політики, Про електронні комунікації. Окремо необхідно зазначити про Стратегію кібербезпеки України, яка визначає місце кібербезпеки в глобальному контексті, виклики та кіберзагрози національного кіберпростору, засади розбудови національної

системи кібербезпеки, пріоритети забезпечення кібербезпеки України стратегічні цілі і завдання, напрями зовнішньополітичної діяльності України у сфері кібербезпеки, механізми реалізації стратегії та забезпечення відкритості, а також оцінює ступінь реалізації Стратегії кібербезпеки України.

Досліджуючи питання пов'язане із законами України, які надають визначення інформації, її видів та порядку використання, здобувачу необхідно дослідити закон України «Про інформацію»  , який регламентує питання щодо визначення інформації, її видів, а також створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Також, досліджуючи відповідне питання, необхідно ознайомитись із Законом України «Про науково-технічну інформацію»  , який визначає основи існуючої державної політики в галузі науково-технічної інформації, а також порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу України. Він регулює правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі.

В свою чергу серед законів України, що визначають вимоги щодо захисту інформації здобувачам варто ознайомитись з наступними: «Про захист інформації в інформаційно-телекомунікаційних системах» 

, «Про основні засади забезпечення кібербезпеки України»  . Які регламентують відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах; а також визначають правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі.

До законів України, що регулюють питання інформації з обмеженим доступом, з якими мають ознайомитись здобувачі, необхідно віднести: «Про державну таємницю»  і «Про захист персональних даних»  . Які в свою чергу регламентують суспільні відносини, пов’язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. А також правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямованих на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

Що ж стосується нормативно-правових документів, що встановлюють умови кіберзахисту об’єктів критичної інфраструктури, то здобувачам потрібно ознайомитись із Постановою КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної

інфраструктури»  , яка визначає організаційно-методологічні, технічні та технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури.

Окремо необхідно приділити увагу кримінальній відповідальності, яка виконує декілька функцій, в площині забезпечення кібербезпеки: превентивну, охорону та відновлюючу. Що забезпечується наявністю як Кримінального кодексу України  , який містить перелік діянь – кримінальних правопорушень (в тому числі і в сфері кібербезпеки), за які наступає кримінальна відповідальність, так і Кримінального процесуального кодексу України  .

Самостійна робота 5

Здобувачу необхідно надати відповідь на такі питання:

1. Які нормативно-правові акти складають правову основу забезпечення кібербезпеки України?
2. Яке місце серед них посідає Конституція України?
3. Які нормативно-правові акти, регламентують загальні питання кібербезпеки?
4. Які ключові положення містить Стратегія кібербезпеки України?

5. Які види інформації наведені в законі України «Про інформацію»?

6. Які вимоги щодо захисту інформації закріплені в законах України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України»?

7. Які нормативно-правові акти регламентують інформацію з обмеженим доступом?

8. Які нормативно-правові акти встановлюють умови кіберзахисту об’єктів критичної інфраструктури?

9. Яку роль відіграє кримінальне законодавство для забезпечення кібербезпеки?

10. Пройдіть тестування, попередньо зареєструвавшись у викладача (здійснює реєстрацію у Moodle), який веде практичні заняття у відповідній групі, за наступною електронною адресою: http://cyber.onua.edu.ua/mod/quiz/view.php?id=3655

або відсканувавши QR-код:

Тема 6. ДЕРЖАВНІ СТАНДАРТИ УКРАЇНИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

Практичне заняття 6

1. Державні стандарти в Україні: поняття, значення та види.
2. Державні стандарти України в галузі інформаційної та/або кібербезпеки.
3. ДСТУ 3396.0-97
4. ДСТУ 3396.1-97
5. ДСТУ 3396.2-97
6. ДСТУ ISO/IEC 15408-1:2023 (ДСТУ ISO/IEC 15408-1:2017)

Методичні рекомендації

Під час вивчення теми здобувачам потрібно детальніше звернути увагу на поняття, сутність та призначення стандартів в Україні, а також на їх види. Окрему категорію яких складають державні стандарти в галузі інформаційної та/або кібербезпеки. Серед яких здобувачі мають ознайомитись із наступними стандартами:

- ДСТУ 3396.0-97  , галузь використання якого становить об’єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ. Вимоги стандарту обов’язкові для підприємств та установ усіх форм власності і підпорядкування, громадян - суб’єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють,

користуються та розпоряджаються інформацією, що підлягає технічному захисту.

- ДСТУ 3396.1-97  , який установлює вимоги до порядку проведення робіт з технічного захисту інформації (ТЗІ). Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян-суб`єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

- ДСТУ 3396.2-97  . Відповідний стандарт установлює терміни та визначення понять у сфері технічного захисту інформації (ТЗІ). Терміни, регламентовані у цьому стандарті, обов’язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації, і рекомендовані для використання у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації. Терміни стандарту є обов’язковими для використання підприємствами та установами усіх форм власності і підпорядкування, громадянами – суб’єктами підприємницької діяльності, міністерствами (відомствами), центральними і місцевими органами державної виконавчої влади, військовими частинами усіх військових формувань, представництвами України за кордоном, які володіють, використовують та розпоряджаються інформацією, що становить державну чи іншу передбачену законом таємницю або є конфіденційною інформацією, яка належить державі.

- ДСТУ ISO/IEC 15408-1:2023 (ДСТУ ISO/IEC 15408-1:2017)

 , визначає критерії історичності та безперервності. Загальні критерії, які використовуються як основа для оцінювання властивостей безпеки ІТ-продуктів і систем. Встановлюючи таку спільну базу критеріїв, що результати оцінки ІТ-безпеки будуть значущими для широкої аудиторії.

Самостійна робота 6

Здобувачу необхідно надати відповідь на такі питання:

1. Що таке державні стандарти України, яка їх роль для забезпечення інформаційної та/або кібербезпеки?
2. На яке коло правовідносин розповсюджується ДСТУ 3396.0-97?
3. Для яких суб’єктів передбачений ДСТУ 3396.1-97?
4. Який загальний зміст ДСТУ 3396.2-97?
5. Що регламентує ДСТУ ISO/IEC 15408-1:2023 (ДСТУ ISO/IEC 15408-1:2017)?
6. Пройдіть тестування, попередньо зареєструвавшись у викладача (здійснює реєстрацію у Moodle), який веде практичні заняття у відповідній групі, за наступною електронною адресою: http://cyber.onua.edu.ua/mod/quiz/view.php?id=3655

або відсканувавши QR-код: 

Тема 7. НОРМАТИВНІ ДОКУМЕНТИ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Практичне заняття 7

1. Нормативні документи з технічного захисту інформації: поняття та види.
2. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».
3. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Методичні рекомендації

Під час вивчення теми здобувачам потрібно детальніше звернути увагу на поняття та види нормативних документів з технічного захисту інформації. Додатково здобувач має знати різницю між нормативно-правовими актами, державними стандартами та нормативними документами з технічного захисту інформації. Серед нормативних документів з технічного захисту інформації здобувачі мають ознайомитись із НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»  та НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»  , що установлюють терміни і визначення понять у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, які є обов'язковими для застосування в усіх видах документації і літератури, що входять до системи технічного захисту

інформації, а також установлюють критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу. Відповідні критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Самостійна робота 7

Здобувачу необхідно надати відповідь на такі питання:

1. Надайте визначення нормативним документам з технічного захисту інформації.
2. Чим відрізняються нормативні документи з технічного захисту інформації від нормативно-правових актів?
3. Який зміст НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»?
4. Який зміст НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»?
5. Пройдіть тестування, попередньо зареєструвавшись у викладача (здійснює реєстрацію у Moodle), який веде практичні заняття у відповідній групі, за наступною електронною адресою: http://cyber.onua.edu.ua/mod/quiz/view.php?id=3655

або відсканувавши QR-код:

Тема 8. МІЖНАРОДНІ СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

Практичне заняття 8

1. Конвенція про кіберзлочинність.
2. Регламенти ЄС в галузі кібербезпеки.
3. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій».
4. Міжнародний стандарт ISO 27001.
5. Міжнародний стандарт ISO 27002.
6. Міжнародний стандарт ISO 27003.
7. Міжнародний стандарт ISO 27005.
8. Міжнародний стандарт ISO/IEC 15408- 2
9. Міжнародний стандарт ISO/IEC 15408-3

Методичні рекомендації

Під час вивчення теми здобувачам потрібно детальніше звернути увагу на питання, що регламентуються Конвенцією про кіберзлочинність , та визначитись з тим наскільки вони є актуальними на сьогоднішній день, зважаючи на тривалий час дії відповідної конвенції, а також на швидкий розвиток інформаційних технологій. Також здобувачі мають визначитись із поняттям та видами регламентів ЄС в галузі кібербезпеки. Також необхідно дослідити Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA)

та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»  . Окрім нього здобувачі мають приділити увагу наступним міжнародним стандартам:

- ISO 27001  , який створений для надання моделі розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою;

- ISO 27002  , який формує звід правил для управління інформаційною безпекою;

- ISO 27003  , який містить вказівки щодо вимог до системи управління інформаційною безпекою і надає рекомендації, можливості та дозволи щодо них. Він не має на меті надавати загальні положення керівництва з усіх аспектів інформаційної безпеки.

- ISO 27005  , який забезпечує рекомендації для менеджменту ризиком інформаційної безпеки в організації, особливо підтримуючи вимоги ISMS згідно з ISO/IEC 27001. Однак він не забезпечує певної методології для управління ризиками інформаційної безпеки. Цей стандарт призначений для визначення в організації підходу до менеджменту

ризиків.

- ISO/IEC 15408- 2  , в якому визначені функціональні компоненти безпеки, що є основою для вимог функціональної безпеки (SFR) або компонентів, виражених в профілі захисту (PP), модулів PP, функціоналі пакету або Security Target (ST). Ці вимоги призначені для досягнення цілей безпеки, як зазначено в PP, PP-модуль, функціональному пакеті або ST. Закріплені в стандарті вимоги описують властивості безпеки, які користувачі можуть виявити шляхом прямої взаємодії з IT або за допомогою реакції IT на подразник.

- ISO/IEC 15408-3  , який містить компоненти гарантії безпеки, що є основою для гарантії безпеки вимогам, виражених в пакеті забезпечення безпеки, профілі захисту (PP), модулі PP, конфігурації PP або цілі безпеки (ST). Закріплені в ньому вимоги встановлюють стандартний спосіб вираження вимог довіри до TOE. Цей стандарт каталогізує набір компонентів довіри, сімейств і класів, а також визначає оцінку критерії для PP, PP-конфігурацій, PP-модулів і ST.

Самостійна робота 8

Здобувачу необхідно надати відповідь на такі питання:

1. Дайте визначення та наведіть приклад регламентів ЄС в галузі кібербезпеки.

2. Яке коло правовідносин регулює регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA)

та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»?

3. Які питання регулює стандарт ISO 27001?

4. Які питання регулює стандарт ISO 27002?

5. Які питання регулює стандарт ISO 27003?

6. Які питання регулює стандарт ISO 27005?

7. Які питання регулює стандарт ISO/IEC 15408- 2?

8. Які питання регулює стандарт ISO/IEC 15408-3?

9. Пройдіть тестування, попередньо зареєструвавшись у викладача (здійснює реєстрацію у Moodle), який веде практичні заняття у відповідній групі, за наступною електронною адресою: http://cyber.onua.edu.ua/mod/quiz/view.php?id=3655

або відсканувавши QR-код:

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ І ВМІНЬ

1. В яких випадках можливе збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди?
2. В яких випадках персональні дані не належать до конфіденційної інформації про особу, відповідно до Закону України «Про захист персональних даних»?
3. Визначіть коло відносин, на які розповсюджується кіберпростір.
4. Вкажіть поняття та підходи до розуміння кіберризиків.
5. Схарактеризувати сучасний стан та детермінацію кіберзлочинності.
6. Дайте визначення персональних даних.
7. Дайте визначення поняттю «кіберзагроза», та вкажіть можливі методи протистояння кіберзагрозам.
8. Дайте визначення поняттю «кіберзагроза».
9. Дайте визначення поняттю «кіберпростір».
10. Дайте визначення поняттю «кібертероризм».
11. Дайте визначення поняттю «комп'ютерна інформація».
12. Дайте визначення та наведіть приклади регламентів ЄС в галузі кібербезпеки.
13. Дайте загальну характеристику Стратегії кібербезпеки України.
14. Для яких суб'єктів передбачений ДСТУ 3396.1-97?
15. З кого складається Національна система науково-технічної інформації?
16. З чого складаються Інформаційні ресурси національної системи науково-технічної інформації?
17. З яких джерел складається нормативно-правове регулювання кібербезпеки в Україні?
18. З якою метою законодавець формує ДСТУ у сфері кібербезпеки?

19. За яких умов міжнародний нормативно-правовий акт є легальним на території України?

20. Зазначте існуючу систему суб'єктів забезпечення кібербезпеки за чинним законодавством України.

21. Яким суб'єктом забезпечується кіберзахист об'єкта критичної інфраструктури відповідно до Постанови КМУ «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури»?

22. Які існують засоби попередження кібертероризму та боротьби з ним?

23. Місце Національного координаційного центру кібербезпеки в системі забезпечення кібербезпеки.

24. На яке коло правовідносин розповсюджується ДСТУ 3396.0-97?

25. На які види, за режимом доступу, поділяється науково-технічна інформація?

26. На які види поділяється інформація за порядком доступу?

27. На які правовідносини розповсюджується дія Закону України «Про інформацію»?

28. Надайте визначення кіберзлочину.

29. Надайте визначення нормативним документам з технічного захисту інформації.

30. Надайте поняття кібервійни, які існують їх методи?

31. Надайте поняття кіберконфлікту.

32. Надайте поняття критичної інфраструктури та вкажіть об'єкти критичної інфраструктури.

33. Схарактеризувати кібератаку, вкажіть типи атак на інформаційні системи.

34. Схарактеризувати функції Державної служби спеціального зв'язку та захисту інформації України.

35. Який суб'єкт відповідно до Закону України «Про інформацію» є суб'єктом інформаційних відносин?

36. Хто є суб’єктами відносин, пов’язаних з персональними даними?

37. Хто є суб’єктом забезпечення кібербезпеки в розрізі Закону України «Про основні засади забезпечення кібербезпеки України»?

38. Чи є обов’язковими для виконання ДСТУ у сфері кібербезпеки, які втратили чинність?

39. Чи є обов’язковими для виконання ДСТУ у сфері кібербезпеки?

40. Чим відрізняються нормативні документи з технічного захисту інформації від нормативно-правових актів?

41. Що використовують державні органи для збереження резервних копій своїх інформаційних ресурсів та їх оперативного відновлення, в контексті Постанови КМУ «Про затвердження загальних вимог до кіберзахисту об’єктів критичної інфраструктури»?

42. Що відповідно до Закону України «Про інформацію» є об’єктом інформаційних відносин?

43. Що є об’єктом відносин у сфері науково-технічної інформації?

44. Що є об’єктом кібербезпеки та кіберзахисту в розрізі Закону України «Про основні засади забезпечення кібербезпеки України»?

45. Що є підставою виникнення прав на науково-технічну інформацію?

46. Що Законом України «Про основні засади забезпечення кібербезпеки України» відноситься до об’єктів критичної інфраструктури?

47. Що регламентує ДСТУ ISO/IEC 15408-1:2023 (ДСТУ ISO/IEC 15408-1:2017)?

48. Що таке державні стандарти України, яка їх роль для забезпечення інформаційної та/або кібербезпеки?

49. Як співвідносяться між собою поняття інформаційна безпека та інформаційна інтервенція?

50. Як співвідносяться між собою поняття кіберзагроза та кібератака?

51. Як співвідносяться поняття кібервійни та кіберконфлікту?

52. Яка роль відповідного нормативно-правового забезпечення для формування кібербезпеки України?

53. Яка роль шкідливого програмного забезпечення під час кібератак?

54. Яка система суб'єктів забезпечення кібербезпеки на міжнародному рівні?

55. Яка структура та основні напрями діяльності Державного центру кіберзахисту та протидії кіберзагрозам?

56. Яке коло правовідносин регулює регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»?

57. Яке місце інформаційної безпеки та кібербезпеки у системі національної безпеки?

58. Яке місце серед нормативно-правових актів, що регламентують питання кібербезпеки посідає Конституція України?

59. Яке поняття і ознаки кіберпростору?

60. Який граничний строк, протягом якого діє рішення про віднесення інформації до державної таємниці, передбачений для різних ступенів секретності інформації?

61. Який загальний зміст ДСТУ 3396.2-97?

62. Який зміст НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»?

63. Який зміст НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»?

64. Яким чином державою здійснюється охорона персональних даних, як відбувається державне регулювання охорони персональних даних?

65. Яким чином забезпечується кіберзахист об’єкта критичної інфраструктури, відповідно до Постанови КМУ «Про затвердження загальних вимог до кіберзахисту об’єктів критичної інфраструктури»?

66. Яким чином міжнародний інформаційний тероризм та кібертероризм становлять загрозу національній безпеці?

67. Яким чином реалізується комплексна система захисту інформації?

68. Яких основних суб’єктів національної системи кібербезпеки виділяє Закон України «Про основні засади забезпечення кібербезпеки України»?

69. Які види інформації з обмеженим доступом виділяє Закон України «Про інформацію»?

70. Які види інформації за змістом виділяє Закон України «Про інформацію»?

71. Які види інформації наведені в законі України «Про інформацію»?

72. Які вимоги щодо захисту інформації закріплені в законах України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України»?

73. Які відомості не можуть бути віднесені до інформації з обмеженим доступом?

74. Які дії Закон України «Про інформацію» не дозволяє вчиняти з конфіденційною інформацією про особу без її згоди?

75. Які з законів України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, регулюють питання забезпечення кібербезпеки України?

76. Які завдання та повноваження наявні у Департаменту кіберполіції Національної поліції України?

77. Які існують джерела кіберризиків?

78. Які існують національні нормативно-правові акти щодо забезпечення кібербезпеки та боротьби з кіберзагрозами.

79. Які існують основні вимоги захисту критичної інфраструктури від кібернетичних загроз?

80. Які існують суб'єкти забезпечення кібербезпеки у банківській сфері?

81. Які ключові положення містить Стратегія кібербезпеки України?

82. Які кримінальні правопорушення, пов'язані з кібербезпекою наявні у Кримінальному кодексі України?

83. Які міжнародні договори, згода на обов'язковість яких надана Верховною Радою України сприяють організаційно-правовому забезпеченню кібербезпеки?

84. Які міжнародні нормативно-правові акти, які регламентують недоторканість персональних даних?

85. Які міжнародні правові акти ратифіковані Україною щодо забезпечення кібербезпеки та боротьби з кіберзагрозами?

86. Які можуть існувати джерела кіберзагроз?

87. Які нормативно-правові акти встановлюють умови кіберзахисту об'єктів критичної інфраструктури?

88. Які нормативно-правові акти регламентують інформацію з обмеженим доступом?

89. Які нормативно-правові акти складають правову основу забезпечення кібербезпеки України?

90. Які нормативно-правові акти регламентують загальні питання кібербезпеки?

91. Які ознаки у поняття кіберризиків?

92. Які ознаки характеризують поняття кібербезпеки та кіберзахисту?

93. Які основні завдання стоять перед урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA?

94. Які основні категорії характеризують захист кібербезпеки?

95. Які питання регулює Закон України «Про науково-технічну інформацію»?

96. Які питання регулює стандарт ISO 27001?

97. Які питання регулює стандарт ISO 27002?

98. Які питання регулює стандарт ISO 27003?

99. Які питання регулює стандарт ISO 27005?

100. Які питання регулює стандарт ISO/IEC 15408- 2?

101. Які питання регулює стандарт ISO/IEC 15408-3?

102. Які правовідносини регулює Закон України «Про державну таємницю»?

103. Які правовідносини регулює Закон України «Про захист персональних даних»?

104. Які правовідносини регулює Закон України «Про основні засади забезпечення кібербезпеки України»?

105. Які правопорушення пов'язані з порушенням авторських та суміжних прав закріплені в Конвенції про кіберзлочинність?

106. Які правопорушення пов'язані зі змістом закріплені в Конвенції про кіберзлочинність?

107. Які правопорушення проти конфіденційності закріплені в Конвенції про кіберзлочинність?

108. Які правопорушення, пов'язані з комп'ютерами закріплені в Конвенції про кіберзлочинність?

109. Які ступені секретності інформації передбачає Закон України «Про державну таємницю»?

110. Яку інформація про фізичну особу Закон України «Про інформацію» відносить до конфіденційної?

111. Яку роль відіграє кримінальне законодавство для забезпечення кібербезпеки?

РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ

Нормативно-правові акти

1. Біла книга. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. Матеріал для обговорення (Policy Paper). URL: parlament.org.ua/2017/12/au_White-book-oncybersecurity-draft_5
2. ДСТУ 3396.0-97 «Захист інформації. Технічний захист інформації. Порядок проведення робіт. Основні положення»
3. ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення»
4. ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт»
5. ДСТУ ISO/IEC 27000:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник»
6. ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»
7. ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки»
8. ДСТУ ISO/IEC 27003:2018 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою»
9. ДСТУ ISO/IEC 27005:2011 «Інформаційні технології. Методи захисту. Менеджмент ризику інформаційної безпеки»
10. ДСТУ ISO/IEC 15408-1:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель»
11. ДСТУ ISO/IEC 15408-2:2022 «Інформаційні технології. Методи захисту.Критерії оцінювання. Частина 2. Функціональні вимоги»
12. ДСТУ ISO/IEC 15408-3:2022 «Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 3. Вимоги до гарантії безпеки»

13. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

14. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»

15. Загальні рекомендації Державного центру кіберзахисту та протидії кіберзагрозам Держспецзв'язку для підвищення рівня захисту інформаційних ресурсів та систем і для запобігання кіберінцидентам в установах, на підприємствах і в організаціях. URL: https://www.kmu.gov.ua/news/250099405

16. Конвенція про кіберзлочинність від 23 листопада 2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_575

17. Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 року, № 1009-р. URL: http://zakon2.rada.gov.ua/laws/show/1009-2017-р

18. Кримінальний кодекс України від 05 квітня 2000 року, № 2341III. URL: https://zakon.rada.gov.ua/laws/show/234114#n89

19. Кримінальний процесуальний кодекс України від 13 квітня 2012 року, № 4651VI. URL: https://zakon.rada.gov.ua/laws/show/465117#Text

20. Лист НБУ від 03 грудня 2018 року, №56-0007/64280. URL: https://news.dtkt.ua/debet-kredit/portal-news/52126

21. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Затверджене Постановою Правління Національного банку України 28 вересня 2017 року, № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17

22. Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій : Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року. URL: https://zakon.rada.gov.ua/laws/show/984_024-19#Text

23. Про банки і банківську діяльність: Закон України від 7 грудня 2000 року, № 2121-III. URL: https://zakon.rada.gov.ua/laws/show/2121-14

24. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 07 листопада 2018 року, № 2155-VIII. Відомості Верховної Ради України (ВВР). 2006. № 30

25. Про державну таємницю : Закон України від 21 січня 1994 року, № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

26. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29 грудня 2016 року. *Рада національної безпеки і оборони України*. URL: https://zakon.rada.gov.ua/laws/show/32/2017

27. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 року, № 518. Офіційний вісник України від 02.07.2019. 2019. № 50. С. 53. Стаття 1697, код акту 94896/2019

28. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету міністрів України від 29 березня 2006 року, № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF

29. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року, № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

30. Про захист персональних даних : Закон України від 01 червня 2010 року, № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

31. Про звернення громадян: Закон України від 02 жовтня 1996 року, № 393/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/393/96-вр#Text

32. Про інформацію: Закон України від 02 жовтня 1992 року, № 2657-XII / Верховна рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12

33. Про науково-технічну інформацію: Закон України від 25 червня 1993 року, № 3322-XII. URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text

34. Про Національний банк України: Закон України від 20 травня 1999 року № 679-XIV URL: https://zakon.rada.gov.ua/laws/show/679-14

35. Про Національний координаційний центр кібербезпеки: положення затверджене Указом Президента України від 7 червня 2016 року № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

36. Про національну безпеку України : Закон України від 21 червня 2018 року, № 2469-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2163-19/print1509543369819103

37. 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

38. Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32»: Рішення РНБО від 10 липня 2017 року. *Рада національної безпеки і оборони України*. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17#Text

39. Про рішення Ради національної безпеки і оборони від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року, № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12

40. Проект Концепції інформаційної безпеки України. URL: http://www.osce.org/uk/fom/175056?download=true

41. Статут Організації Об'єднаних Націй і Статут Міжнародного Суду ООН від 26 червня 1945 року. URL: http://zakon4.rada.gov.ua/laws/show/995_010

42. Стосовно заходів щодо високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі: Директива (ЄС)

2016/1148 від 6 липня 2016 року. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

43. Стратегія кібербезпеки України: Указ Президента України від 15 березня 2016 року, № 96/2016. *Президент України*. URL: https://www.president.gov.ua/documents/962016-19836

44. Стратегія кібербезпеки України: Указ Президента України від 14 травня 2021 року, № 447/2021. *Президент України*. URL: https://www.president.gov.ua/documents/4472021-40013

45. Угода про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27 червня 2014 року. *Офіційний вісник України* від 26.09.2014. № 75. Том 1. С. 83. Ст. 2125

46. Цивільний кодекс України: Кодекс України від 16 січня 2003 року, № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Tex

Основні джерела

1. Бараненко Р.В., Задорожна А.Ю. Аналіз методів протидії кібератакам. *Юридичний бюлетень*. 2018. № 6. С. 148–161

2. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека”. *Правова інформатика*. 2014. № 2 (42). С. 54-62

3. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ : НАУ, 2013. 432 с.

4. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. *Інформаційна безпека*: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 р., м. Київ. Київ : Наук.-вид. центр НА СБ України, 2013. 416 с.

5. Войціховський, А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник*

Харківського національного університету імені В. Н. Каразіна. Серія «Право», 2020. № 29. С. 281-288. https://doi.org/10.26565/2075-1834-2020-29-38

6. Гавловський В.Д. Захист інформації шляхом посилення ефективності протидії кібератакам. *Інформація і право*. № 2(30)/2019. С. 105-110

7. Гавловський В.Д. Кримінологічний аналіз злочинів, учинених з використанням соціальних мереж. *Інформація і право*. 2017. № 3(22). С. 101-107

8. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118-129

9. Гнусов Ю.В., Кійков В.М. Сучасні тенденції розвитку DDoS-атак. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.

10. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник. Одеса: ОНАЗ ім. О. С. Попова, 2019. 320 с.

11. Дикий О.В., Сидорчук В.В. Поняття OSINT та суміжні категорії. *Юридичний науковий електронний журнал.* 2024, № 9. С.332-336. DOI: https://doi.org/10.32782/2524-0374/2024-9/78

12. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О.М. Суходолі. Київ: НІСД, 2020. 28 с.

13. Діордіца І.В. Інформаційні інтервенції як загроза кібернетичній безпеці. *Науковий вісник Херсонського державного університету*. Серія Юридичні науки. 2015. Випуск 6. Том 2. С. 50-56. URL: https://www.socosvita.kiev.ua/sites/default/files/Diord_1_2015.pdf

14. Діордіца І.В. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України. *Підприємництво, господарство і право*. 2017. № 10. С. 206-211

15. Дубов Д.В. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. К. : НІСД, 2018. 84 с.

16. Еделєва М.А. Забезпечення інформаційної безпеки в контексті реалізації державної інформаційної політики. *Вісник Маріупольського державного університету. Серія «Історія. Політологія».* 2017. Вип. 19. С. 133–141

17. Живко З. Б., Рудий Т. В., Сеник В. В., Родченко С. С. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи. *Соціально-правові студії* : науково-аналітичний журнал / гол. ред. О. Балинська. Львів : ЛьвДУВС, 2020. Вип. 3 (9). С. 18–25

18. Зачек О. І., Дмитрик Ю. І. Застосування профайлінгу для протидії кіберзлочинності. *Соціально-правові студії* : науково-аналітичний журнал / гол. ред. О. Балинська. Львів : ЛьвДУВС, 2020. Вип. 4 (10). С. 94–100

19. Іванюта С.П. Пріоритетні напрями законодавчого та організаційного забезпечення паспортизації об’єктів критичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2018-07/1_Ivaniuta-9af75.pdf

20. Інформаційна безпека та кібрбезпека держави: навчальний посібник/ [Н.М. Титова, Н.М. Рідей, В.П. Настрадін, М.М. П рисяжнюк, С.М. Мамченко, С.В. Артюх, Р.О. Яворська]; за заг. ред.. М.М. Присяжнюка. Київ6 Видавництво Ліра-К, 2024. 224 с.

21. Кобко Є. В. Інформаційна безпека в системі національної безпеки: сучасність і перспективи. *NATIONAL LAW JOURNAL: TEORY AND PRACTICE.* 2019. MARTIE. С. 46-50. URL: http://www.jurnaluljuridic.in.ua/archive/2019/2/part_2/11.pdf

22. Ковальчук А.Ю. Гавловський В.Д. Кіберзлочини як загроза державній безпеці: кримінологічні та організаційні особливості обліку. *Інформація і право.* 2023. № 4 (47). С. 187-196

23. Козак Н.С. Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів : дис. … канд. юрид. наук : 12.00.09. Ірпінь, 2011. 229 с.

24. Козюра В.Д., Хорошко В.О. Як протистояти реальним кіберзагрозам об'єктам критичної інфраструктури України. *Кібербезпека в Україні*: правові та організаційні питання : матеріали Всеукр. наук.- практ. конф., м. Одеса, 17 листопада 2017 р. Одеса : ОДУВС, 2017. С. 79–80

25. Кравцова М.О. Кіберзлочинність : кримінологічна характеристика та запобігання органами внутрішніх справ : автореф дис. на здобуття наук. ступеня к.ю.н. : 12.00.08. Харків, 2016. 19 с.

26. Леонов Б.Д., Шостак Р.М., Серьогін В.С. Розвиток методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури (на прикладі США). *Інформація і право*. № 3(34)/2020. С. 88-95

27. Лесько Н.В., Кіра С.О. Кібербезпека як частина національної безпеки України в умовах війни. *Юридичний науковий електронний журнал.* 2023. № 5. С. 224-226. URL: http://lsej.org.ua/5_2023/55.pdf

28. Ліпкан В. А. Національна і міжнародна безпека у визначеннях та поняттях / В. А. Ліпкан, О. С. Ліпкан. – 2-ге вид., доп. і перероб. – К.: Текст, 2008. 400 с.

29. Ліпкан В.А. Інкорпорація інформаційного законодавства України: [монографія] / В.А. Ліпкан, К.П. Череповський / за заг. ред. В.А. Ліпкана. – К.: ФОП О.С. Ліпкан, 2014. 408 с.

30. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : [навчальний посібник] / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К.: КНТ, 2006. 280 с.

31. Лук’янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України. Сер.: Державне управління*. 2016. № 3. С. 131-137

32. Павлов І. М., Толюпа С. В., Ніщенко В. І. Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем. *Сучасний захист інформації*. 2014. № 4. С. 44–52

33. Піцик Ю. Напрями протидії кіберзлочинам проти власності. *National law journal: theory and practice*. 2018. iunie. С. 52-54

34. Рижов І.М. Базові концепти антитерористичної безпеки: монографія. Київ: Нац. акад. СБУ, 2016. 327 с.

35. Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору. *Україна: події, факти, коментарі*. 2017. № 19. С. 42–48

36. Світличний В.А. Дослідження атак на відмову в обслуговуванні інформаційно-телекомунікаційних систем. *Кібербезпека в Україні*: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. Одеса : ОДУВС, 2018. С. 88–89

37. Світличний В.А., Петров К.Е. Від ідентифікації комп’ютера до ідентифікації користувача у мережі Інтернет. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.

38. Серьогін В.С., Леонов Б.Д. Окремі проблеми криміналістичного забезпечення розслідування злочинів, пов’язаних з неправомірним дистанційним доступом до комп’ютерної інформації. *Інформація і право*. 2017. № 2(21). С. 108-115

39. Таран О.В., Гавловський В.Д. Організована кіберзлочинність в Україні: проблеми формування офіційної статистики та її аналізу. *Інформація і право*. № 4(39)/2021. С. 193-201

40. Тарасюк А.В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. 2020, № 2, Ч.2. С. 119-124

41. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134

42. Ткачук Т.Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. *Jurnalul juridic national: teorie şi practică*. 2017. № 6. С. 42–46

43. Толюпа С. В., Штаненко С. С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. *Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут*. 2018. Вип. № 3. С. 56–66

44. Торяник В.В., Чмирь А.Ю. Актуальність проблеми атаки на відмову в обслуговуванні. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнар. наук.- практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.

45. Трофименко О.Г., Логінова Н.І., Манаков С.Ю., Янковський О.Г. Кіберризики в освітньому секторі. *Сучасна спеціальна техніка.* 2022, №2. С. 111-117

46. Фролова О.М. Роль ООН в системі міжнародної інформаційної безпеки URL: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140

47. Хахановський В.Г., Гавловський В.Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право*. № 2(33)/2020. С. 99-110

48. Які російські та проросійські хакери атакують Україну. *Державна служба спеціального зв'язку та захисту інформації України*. URL : https://cip.gov.ua/ua/news/yaki-rosiiski-ta-prorosiiski-khakeri-atakuyut-ukrayinu

49. Янковський О. Закон «Про кібербезпеку» як спроба тотального контролю. URL: https://www.pravda.com.ua/ columns/2017/06/10/7146438

Додаткові джерела

1. Бараненко Р.В. Кібератака як одна з форм кібертероризму. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки.* 2021, №1. Том 32 (71). Ч. 1. С. 45-50

2. Баскаков В.Ю. Інформація з обмеженим доступом: поняття та ознаки. Актуальні проблеми державотворення: матеріали науково-практичної конференції (Київ, 28 червня 2011 р.). – К. : ФОП О.С. Ліпкан, 2011. С. 47–49

3. Бойченко О.В., Ончурова О.О. Кібертероризм у складі сучасних проблем національної безпеки. *Фортеця права*. 2010. № 2. С. 57

4. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

5. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства. *Сучасна спеціальна техніка*. 2011. № 3 (26). С. 104–114

6. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

7. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. ... канд. юрид. наук : 12.00.07. Суми, 2018. 221 с.

8. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. *Економіка та суспільство*. 2017. № 11. С. 497-502. URL: http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf

9. Владленова І.В., Кальницький Е.А. Кіберзлочинність як виклик інформаційному суспільству. *Гілея*: науковий вісник : збірник наукових праць. 2013. Вип. 77. С. 142–146

10. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал.* 2020. № 2. С. 200-203.

11. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2021. 256 с.

12. Дикий А.П. Організація бухгалтерського обліку як інструмент забезпечення економічної безпеки підприємств: дис. ... канд. екон. наук: 08.00.09. Житомир, 2009. 172 с.

13. Діордіца І.В. Напрями державної політики кібербезпеки. *Прикарпатський науковий вісник*. 2017. № 3 (18). С. 116-122. URL: http://www.pjv.nuoua.od.ua/v3_2017/27.pdf

14. Залізняк В.А. Міжнародно-правове регулювання права на інформацію. *Підприємництво, господарство і право*. 2010. № 8. С. 69–72

15. Кіберзлочинність – загроза банківській системі. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Vnbu_2015_4_7.pdf

16. Клименко В. Внутрішні загрози інформаційній безпеці організації. *Вісник НБУ*. 2008. № 5. С. 62-63.

17. Клочко А.М. , Єременко А.О. Шахрайство з використанням банківських платіжних карток. *Юридичний науковий журнал*. 2016. № 1. С. 85-89. URL: http://www.lsej.org.ua/1_2016/24.pdf

18. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. К. : КНТ, 2006. 280 с.

19. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: автореф. дис. на здобуття

наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Київ, 2005. 20 с.

20. Мандзюк О.А. Роль аналітичної діяльності та аналітичних центрів у формуванні й реалізації кібербезпекової політики. URL: http://goal-int.org/rol-analitichnoi-diyalnosti-ta-analitichnix-centriv-u-formuvanni-j-realizacii-kiberbezpekovoi-politiki/

21. Настанови з кібербезпеки від експертів. URL: http://www.isaca.org.ua/index.php/press-center/news/191-translation-of-guidelines-on-cybersecurity

22. Островий О.В. Інструменти державної політики забезпечення кібернетичної безпеки. URL: https://www.inter-nauka.com/uploads/public/15596540123683.pdf

23. Пашнєв Д.В. Стратегія забезпечення кримінологічної кібернетичної безпеки органами внутрішніх справ. *Вісник Кримінологічної асоціації України*. 2014. № 8. URL: http://files.visnikkau.org/200000574-2ccb52dc47/Visnyk8_10.pdf

24. Рудник Л.І. Право на доступ до інформації: дис. ... канд. юрид. наук : 12.00.07. Київ, 2015. 247 с.

25. Савінова Н.А. Кібернетична інтервенція: до питань походження та потреби криміналізації в умовах формування та розвитку інформаційного суспільства. URL: http://justinian.ua/article.php?id=3912

26. Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз: монографія / Н. В. Лукова-Чуйко, С. В. Толюпа, В. С. Наконечний, М. М. Браіловський. Київ: Формат, 2021. 407 с.

27. Страдний І.О. Протидія кіберзлочинам у сфері використання платіжних систем. *Кібербезпека у системі національної безпеки України*: пріоритетні напрями розвитку: збірник матеріалів наукового круглого столу, м. Маріуполь, 26 квітня 2018 р. / Маріупольський державний університет;

уклад. Проценко О.Б., Меркулова К.В. Маріуполь: МДУ, 2018. 145 с. С. 34-36. URL: http://mdu.in.ua/Nauch/Konf/2018/kiberbezpeka_24_04.pdf

28. Стратегічні комунікації : словник / [Т. В. Попова, В. А. Ліпкан] ; за заг. ред. доктора юридичних наук В. А. Ліпкана. – К. : ФОП Ліпкан О.С., 2016. 416 с.

29. Тімкін І.Ф., Новікова Н.Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України. URL: er.nau.edu.ua

30. Ткачук Н.А. Стан та проблемні питання реалізації стратегії кібербезпеки України. *Інформація і право*. 2019. № 1(28). С. 129-134

31. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 422 с.

32. Ткачук Н. Кібертероризм як новий виклик національній безпеці. *Протидія терористичній діяльності*: міжнародний досвід і його актуальність для України : матеріали Міжнар. наук.-практ. конф. (30 вересня 2016 року). Київ : Національна академія прокуратури України, 2016. С. 340–342

33. Толюпа С., Лукова-Чуйко Н., Шестак Я. Засоби виявлення кібернетичних атак на інформаційні системи. *Інфокомунікаційні технології та електронна інженерія.* 2021. №2 (2). С. 19-31

34. Цимбалюк В.С. Інформаційне право (основи теорії і практики) : [монографія] / В.С. Цимбалюк. – К.: «Освіта України» 2010. 388 с.

35. Цимбалюк В.С. Основи інформаційного права України: [навч. посібн.] / [В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін.]; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. – К.: Знання, 2004. 274 с.

36. Череповський К.П. Інкорпорація інформаційного законодавства України: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» . Запоріжжя, 2013. 19 с.

37. Шеломенцев В.П. Кримінологічна безпека у кіберпросторі: система понять. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. № 23. С. 342-348. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/boz_2010_23_41.pdf

38. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2. С. 299–309

39. Шипілова Ю. Правова база української кібербезпеки: загальний огляд і аналіз. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

40. Цаль-Цалко Ю.С., Мороз Ю.Ю. Облікова політика підприємства та її кібербезпека. *Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства*: збірник наукових праць, том IV, частина І, Житомир: ПП «Рута», 2017 С. 8-11

41. Domingues V. Finance and Cybersecurity Risk Management: Dissertation. 2018. 51 p. URL: https://www.researchgate.net/publication/344711134_Finance_and_Cybersecurity_Risk_Management

42. Dorothy E. Denning (May 23, 2000). “Cyberterrorism”. cs.georgetown.edu. Archived from the original on March 10, 2014. Retrieved June 19, 2016

43. Jureviciene A., Brilingaite A., Bukauskas L. Digital Human in Cybersecurity Risk Assessment. HCII 2021. Lecture Notes in Computer Science. 2021. Vol 12776. Springer, Cham. DOI: https:// doi.org/10.1007/978-3-030-78114-9_29. URL: https://link.springer.com/chapter/10.1007%2F978-3- 030-78114-9_29#citeas

44. Naidoo R. A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems. 2020. Vol. 29(3). P. 306-321. DOI: 10.1080/0960085x.2020.1771222

45. Savchenko V., Matsko O. Cybersecurity risk management on the basis of game-theoretic approach. Modern information security. 2019. Vol. 2(38). P. 6-16. DOI: 10.31673/2409-7292. 2019.020616

46. Williams Ch., Chaturvedi R., Chakravarthy K. Cybersecurity Risks in a Pandemic. Journal of Medical Internet Research. 2020. Vol 22. DOI: 10.2196/23692. URL: https://wwwjmir.org/2020/9/ e23692/

47. UlvenJ., Wangen G. A Systematic Review of CybersecurityRisks in Higher Education. Future Internet. 2021. Vol. 13. 39 p. DOI: 10.3390/fi13020039. URL: https://www.researchgate.net/publication/

Ресурси відкритого доступу

1. Каталог правових сайтів України - http://pravoved.in.ua
2. Єдиний веб-портал послуг - http://www.kmu.gov.ua
3. Національне антикорупційне бюро України - https://nabu.gov.ua
4. Офіс генерального прокурора - http://www.gp.gov.ua
5. Служба безпеки України - http://www.sbu.gov.ua
6. Міністерство внутрішніх справ - http://www.mvs.gov.ua
7. Департамент кіберполіції Національної поліції України - https://cyberpolice.gov.ua
8. Державна служба спеціального зв’язку та захисту інформації України - https://cip.gov.ua/ua
9. Державний центр кіберзахисту та протидії кіберзагрозам - https://scpc.gov.ua/uk
10. Антирейдерський союз підприємців України - http://antiraider.ua
11. Центр протидії корупції - http://antac.org.ua

НАВЧАЛЬНЕ ВИДАННЯ

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

для підготовки до практичних занять та самостійної роботи
здобувачів першого (бакалаврського) рівня вищої освіти
в галузі знань 12 «Інформаційні технології»
спеціальність: 125 «Кібербезпека та захист інформації»

Електронне видання

Укладачі:
Аркуша Лариса Ігорівна
Дикий Олег Вікторович
Мандриченко Жанна Василівна
Стоянов Микола Михайлович
Сидорчук Владислав Васильович

В авторській редакції