ЗАТВЕРДЖЕНО

Вченою радою факультету національної безпеки, права та міжнародних відносин
01 вересня 2023 р., протокол №8
Голова Вченої ради
_____ Лариса СЕРГІЄНКО

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Інформаційна безпека професійної діяльності»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 262 «Правоохоронна діяльність»
освітньо-професійна програма «Правоохоронна діяльність»
факультет національної безпеки, права та міжнародних відносин
кафедра права та правоохоронної діяльності

Схвалено на засіданні кафедри
теорії та історії держави і права
29 серпня 2023 р., протокол № 8

В.о. завідувача кафедри
_____ Валерій НОНІК

Гарант освітньо-професійної програми
_____ Катерина КАТЕРИНЧУК

Розробники: д.ю.н., с.н.с., професор кафедри теорії та історії держави і права,
Віталій ЦИМБАЛЮК,
к.тех.н., доц., доцент кафедри комп'ютерної інженерії та кібербезпеки,
Надія ЛОБАНЧИКОВА

Житомир
2023– 2024 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань:
26 Цивільна безпека</td><td>нормативна</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність:
262 «Правоохоронна діяльність»</td><td>Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 1</td><td>1</td></tr>
<tr><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>2</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="9">Тижневих годин для денної форми навчання:
аудиторних – 4</td><td rowspan="9">Освітній ступінь:
«бакалавр»</td><td>32 год.</td></tr>
<tr><td>Практичні</td></tr>
<tr><td>32 год.</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>–</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>56 год.</td></tr>
<tr><td>Вид контролю: залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 53% аудиторних занять, 47% самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни «Інформаційна безпека професійної діяльності» є набуття здобувачами вищої освіти необхідних знань щодо сутності, проявів, наслідків інформаційної безпеки, механізмів правового забезпечення запобігання та усунення загроз в інформаційній сфері, спрямованими на формування здатності розв'язувати складні спеціалізовані задачі та практичні проблеми у сфері поводження з інформацією на всіх етапах професійної діяльності.

Завданнями вивчення навчальної дисципліни є:

– розкрити сутність основних понять в сфері інформаційна безпека;

– прищепити здобувачам вищої освіти навики самостійного аналізу загроз інформаційній безпеці;

– сформувати навики виокремлення тенденцій, які властиві сучасним загрозам інформаційній безпеці у соціальних Інтернет-сервісах;

– визначити напрями і можливості вдосконалення системи забезпечення інформаційної безпеки професійної діяльності.

Зміст навчальної дисципліни направлений на формування загальних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 262 «Правоохоронна діяльність»:

Загальні компетентності

ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність використовувати інформаційні та комунікаційні технології.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК8. Здатність приймати обґрунтовані рішення.

Спеціальні компетентності:

СК14. Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукових систем та баз даних.

СК18. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури.

СК19. Здатність забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом.

СК21. Здатність ефективно застосовувати ресурсні (інформаційні, організаційні, технічні та інші) можливості взаємодії із міжнародними поліцейськими організаціями у професійній діяльності.

Отримані знання з навчальної дисципліни «Інформаційна безпека професійної діяльності» стануть складовими наступних **програмних результатів** навчання за спеціальністю 262 «Правоохоронна діяльність»:

РН8. Здійснювати пошук інформації у доступних джерелах для повного та всебічного встановлення необхідних обставин.

РН9. Користуватись державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

РН14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності.

РН17. Використовувати основні методи та засоби забезпечення правопорядку в державі, дотримуватись прав і свобод людини і громадянина, попередження та припинення нелегальної (незаконної) міграції та інших загроз національної безпеки держави (кібербезпеку, економічну та інформаційну безпеку, тощо).

РН18. Застосовувати штатне озброєння підрозділу (вогнепальну зброю, спеціальні засоби, засоби фізичної сили); інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності.

РН21. Організовувати заходи щодо режиму секретності та захисту інформації.

РН23. Організовувати взаємодію з міжнародними поліцейськими організаціями та застосовувати їх можливості у сфері запобігання та протидії злочинності.

Навчальна дисципліна орієнтована на розвиток загальної інформаційної культури, критичного мислення та громадянської свідомості здобувачів, а також на формування професійних знань фахівців в сфері правоохоронної діяльності щодо інформаційної безпеки.

3. Програма навчальної дисципліни

Тема 1. Нормативно-правова база у сфері інформаційної безпеки

1. Основні законодавчі положення у сфері забезпечення інформаційної безпеки
2. Нормативно-правові акти та міжнародні договори в сфері обігу інформації

Тема 2. Кібернетична безпека як складова інформаційної безпеки

1. Кібернетика як джерело небезпеки
2. Процеси створення та впровадження інформаційно-комунікаційних технологій (ІКТ) як об’єкт і предмет правового регулювання
3. Безпека глобальних інформаційних систем та мереж
4. Визначення поняття «кібернетична безпека» (кібербезпека)
5. Сутність понять інтернет-речей, блокчейн та криптотехнології вільного доступу
6. Об’єкти інформаційних та кіберзагроз
7. Зв’язок інформаційної безпеки та кібербезпеки

Тема 3. Основні засади забезпечення кібербезпеки України та особливості формування і реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації

1. Правові основи забезпечення кібербезпеки України
2. Критерії оцінки об'єкта інформаційної інфраструктури
3. Поняття політики безпеки, види політик безпеки
4. Особливості формування політики безпеки для об’єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації

Тема 4. Національні системи спецзв’язку

1. Перелік національних систем спецзв’язку
2. Особливості організації та принципи роботи Державної системи урядового зв’язку
3. Особливості організації та принципи роботи Національної системи конфіденційного зв’язку
4. Особливості використання IP-телефонії, голосових шлюзів, телефонів для забезпечення захисту інформації

Тема 5. Основи криптографічних методів кіберзахисту

1. Системи шифрування з відкритим та закритим ключем
2. Кваліфікований електронний підпис
3. Стеганографія та скремблювання

Тема 6. Основи технічного захисту інформації

1. Захист інформації від несанкціонованого доступу, у тому числі систем відеоспостереження, систем сигналізації, комплексних охоронних та пожежних системам
2. Технічні канали витоку інформації
3. Способи несанкціонованого зняття інформації
4. Методи та засоби блокування технічних каналів витоку інформації
5. Методи захисту інформації від витоку технічними каналами

Тема 7. Методи та засоби блокування технічних каналів витоку інформації

1. Основні загальні положення технічного захисту інформації
2. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації
3. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами
4. Захист інформації від несанкціонованого запису звукозаписувальними пристроями
5. Захист електронної інформації
6. Захист письмової інформації від оптичного зняття

Тема 8. Основи телекомунікацій та сучасні системи передачі інформації

1. Радіорелейний зв’язок; радіорелейні лінії зв’язку; кабельні і оптиковолоконні технології; мобільний зв’язок; супутникові технології
2. Сучасні телекомунікаційні мережі та засоби забезпечення мережної безпеки
3. Поняття інформації, повідомлення, сигналу і завад
4. Модуляція та маніпуляція сигналів
5. Кодування та шифрування інформації
6. Основи побудови радіопередавальних і радіоприймальних пристроїв, особливості користування радіочастотними ресурсами України

Тема 9. Організація та ведення секретного діловодства

1. Засоби зв'язку спеціального призначення
2. Урядовий фельд’єгерський зв’язок
3. Порядок поштово-телеграфного листування з іншими державними органами, органами місцевого самоврядування, підприємствами, установами і організаціями та їх режимно-секретними органами з питань забезпечення режиму секретності

Тема 10. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки

1. Адміністративна відповідальність за правопорушення в системі забезпечення інформаційної безпеки
2. Кримінальна відповідальність за правопорушення в системі забезпечення інформаційної безпеки
3. Цивільна відповідальність за правопорушення в системі забезпечення інформаційної безпеки

Тема 11. Міжнародний досвід у сфері захисту інформації та боротьбі з комп'ютерною злочинністю

1. Міжнародний досвід в боротьбі із загрозами інформаційній безпеці
2. Використання міжнародно-правового досвіду протидії комп'ютерній злочинності
3. Взаємодія та міжнародне інформаційне співробітництво правоохоронних органів у сфері забезпечення інформаційної безпеки

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин			
	денна форма			
	усього	лекції	практичні	самостійна робота
Тема 1. Нормативно-правова база у сфері інформаційної безпеки	6	2	2	2
Тема 2. Кібернетична безпека як складова інформаційної безпеки	6	2	2	2
Тема 3. Основні засади забезпечення кібербезпеки України та особливості формування і реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації	6	2	2	2
Тема 4. Національні системи спецзв'язку	15	4	4	7
Тема 5. Основи криптографічних методів кіберзахисту	15	4	4	7
Тема 6. Основи технічного захисту інформації	15	4	4	7
Тема 7. Методи та засоби блокування технічних каналів витоку інформації	15	4	4	7
Тема 8. Основи телекомунікацій та сучасні системи передачі інформації	15	4	4	7
Тема 9. Організація та ведення секретного діловодства	15	4	4	7
Тема 10. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки	6	1	1	4
Тема 11. Міжнародний досвід у сфері захисту інформації та боротьбі з комп'ютерною злочинністю	6	1	1	4
ВСЬОГО	**120**	**32**	**32**	**56**

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Тема 1. Нормативно-правова база у сфері інформаційної безпеки	2
2	Тема 2. Кібернетична безпека як складова інформаційної безпеки	2
3	Тема 3. Основні засади забезпечення кібербезпеки України та особливості формування і реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації	2
4	Тема 4. Національні системи спецзв'язку	4
5	Тема 5. Основи криптографічних методів кіберзахисту	4
6	Тема 6. Основи технічного захисту інформації	4
7	Тема 7. Методи та засоби блокування технічних каналів витоку інформації	4
8	Тема 8. Основи телекомунікацій та сучасні системи передачі інформації	4
9	Тема 9. Організація та ведення секретного діловодства	4
10	Тема 10. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки	1
11	Тема 11. Міжнародний досвід у сфері захисту інформації та боротьбі з комп'ютерною злочинністю	1
РАЗОМ		**32**

6. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Тема 1. Нормативно-правова база у сфері інформаційної безпеки – Нормативно-правові акти та міжнародні договори в сфері обігу інформації	2
2	Тема 2. Кібернетична безпека як складова інформаційної безпеки – Об'єкти інформаційних та кіберзагроз – Зв'язок інформаційної безпеки та кібербезпеки	2
3	Тема 3. Основні засади забезпечення кібербезпеки України та особливості формування і реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації – Поняття політики безпеки, види політик безпеки	2
4	Тема 4. Національні системи спецзв'язку – Перелік національних систем спецзв'язку	7
5	Тема 5. Основи криптографічних методів кіберзахисту – Системи шифрування з відкритим та закритим ключем	7
6	Тема 6. Основи технічного захисту інформації – Технічні канали витоку інформації	7
7	Тема 7. Методи та засоби блокування технічних каналів витоку інформації – Захист електронної інформації – Захист письмової інформації від оптичного зняття	7

8	Тема 8. Основи телекомунікацій та сучасні системи передачі інформації – Сучасні телекомунікаційні мережі та засоби забезпечення мережної безпеки	7
9	Тема 9. Організація та ведення секретного діловодства – Засоби зв'язку спеціального призначення	7
10	Тема 10. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки – Цивільна відповідальність за правопорушення в системі забезпечення інформаційної безпеки	4
11	Тема 11. Міжнародний досвід у сфері захисту інформації та боротьбі з комп'ютерною злочинністю – Міжнародний досвід в боротьбі із загрозами інформаційній безпеці	4
РАЗОМ		**56**

7. Індивідуальні завдання

Індивідуальна робота здобувачів включає написання рефератів / есе та їх захист на практичних заняттях. Орієнтовна тематика рефератів / есе:

1. Актуальні проблеми інформаційної безпеки в Україні і шляхи їх розв'язання
2. Інформація як предмет злочину: здійснити аналіз структури інформаційних ресурсів
3. Проблеми захисту персональних даних в Україні
4. Стан, тенденції та проблеми захисту інформації в інформаційних системах України
5. Правові аспекти і законодавче забезпечення захисту інформації в Україні:
6. Класифікація загрози інформації і каналів витоку сучасних інформаційних систем і мереж:
7. Європейська конвенція з кіберзлочинів і завдання щодо забезпечення інформаційної безпеки в Україні
8. Основи державної інформаційної політики у сфері захисту інформації
9. Інформаційні системи та технології як об'єкти інформаційної безпеки
10. Роль і місце інформаційної безпеки в загальній системі національної безпеки держави
11. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення
12. Інформаційна безпека в глобальній мережі Інтернет
13. Безпека інформації в комп'ютерних системах
14. Кіберзагрози для України в інформаційному просторі
15. Тема, запропонована здобувачем вищої освіти

Результати дослідження презентуються серед здобувачів вищої освіти

8. Методи навчання

В процесі викладання даного предмету використовуються:

а) методи організації і здійснення навчально-пізнавальної діяльності (пояснення, інструктаж, розповідь, лекція; ілюстрування, демонстрування, самостійне спостереження, вправи, практичні і дослідні роботи);

б) методи стимулювання навчальної діяльності (навчальна дискусія, створення ситуації інтересу у процесі викладення, створення ситуації новизни, опора на життєвий досвід здобувача);

в) методи контролю і самоконтролю у навчанні (усний, письмовий, тестовий, графічний, самоконтроль і самооцінка).

Для забезпечення освітньої діяльності використовуються наступні засоби:

1) Технічне забезпечення:

– Мережне та кібербезпекове обладнання лабораторії Cisco:

комутатори Cisco серій 2960/3560;

маршрутизатори Cisco серій 1800/2800/2900;

міжмережні екрани Cisco ASA 5510/5520/5540;

міжмережні екрани наступного покоління з підтримкою систем виявлення і протидії вторгненням Cisco ASA 5510-X/5512-X;

точки доступу до мережі Wi-Fi.

– Обладнання для забезпечення технічного захисту інформації:

дротові та бездротові відеокамери;

датчики руху, розбиття скла тощо;

системи сигналізації;

контролери систем контролю доступу, електронні замки, кнопки тощо.

– SDR-приймачі для візуалізації спектра радіовипромінювання на прикладі звукового та телевізійного мовлення, а також радіочастот радіоаматорів.

2) Програмне забезпечення:

Середовище симуляції роботи комп'ютерних мереж, інтернету речей, систем кібербезпеки Cisco Packet Tracer 8.2.1;

Середовище емуляції роботи кінцевих вузлів та пристроїв мереж Virtual Box 7.0.14, GNS3 2.2.45.

3) Інформаційні ресурси:

курс «Основи кібербезпеки» онлайнової платформи Cisco Netacad.com;

курс «CyberSecurity Essentials 3.0» онлайнової платформи Cisco SkillsforAll.com

9. Методи контролю

Контроль складається з поточного контролю виконання здобувачам самостійної роботи, модульного контролю, контролю виконання індивідуальних завдань.

Поточний контроль виконання самостійної роботи здійснюється шляхом усного опитування під час практичних занять, міні-колоквіумів, ділових ігор, перевірки домашнього завдання, тестування.

Підсумковий (семестровий) контроль (залік):

1. Накопичення рейтингових балів в межах дисципліни проводиться в балах, які у підсумку переводяться у національну шкалу та шкалу ЄКТС.

2. Загальна кількість балів на останньому занятті з навчальної дисципліни оприлюднюється здобувачам вищої освіти та виставляється в відомість обліку

успішності академічних груп.

3. У випадку погодження здобувача вищої освіти з оцінкою поточної успішності, вона вважається остаточною, враховується як результат семестрового контролю і вноситься у залікову книжку.

4. У разі незгоди здобувача вищої освіти з результатами поточної успішності, оцінка з дисципліни виставляється за результатами дистанційного складання заліку. До тестування допускаються здобувачі, які отримали 50 і більше балів.

5. У разі, якщо студент отримав від 0 до 59 балів, то в відомість за національною шкалою виставляється оцінка «незараховано» («F» та «FX» відповідно до шкали ЄКТС).

10. Розподіл балів

Поточне тестування та самостійна робота												Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	ІЗ	100
5	5	5	11	11	11	11	11	11	5	5	9	

Шкала оцінювання

За шкалою	Залік	Бали
A	Зараховано	90-100
B	Зараховано	82-89
C		74-81
D	Зараховано	64-73
E		60-63
FX	Не зараховано	35-59
F	Не зараховано	0-34

11. Рекомендована література

Нормативно-правові акти

1. Доктрина інформаційної безпеки України: затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374.

2. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних, ратифікована згідно із Законом України № 2438–VI від 06.07.2010 р. URL: http://zakon1.rada.gov.ua/cgi–bin/laws/main. cgi?nreg=994_326.

3. Конвенція про кіберзлочинність ратифікована Законом України від 07.09.2005 р. № 2824–IV. URL: http://zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=994_575.

4. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV

5. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 року № 851-IV // ВВР, 2003, № 36, ст. 275

6. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX

7. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: рішення Ради національної безпеки і оборони України від 29 грудня 2016 р., введено в дію Указом Президента України від 13 лютого 2017 р. № 32/2017. URL: https://zakon.rada.gov.ua/laws/show/n0015525-16#Text

8. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 31 травня 2005 року № 2594-IV // ВВР, 2005, № 26, ст. 347

9. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII // ВВР, 1992, № 48, ст. 650

10. Про криптографічний та технічний захист інформації: Проект закону від 12.03.2016

11. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР // ВВР, 1998, № 27-28

12. Про Національну систему конфіденційного зв'язку: Закон України від 10.01.2002 № 2919-III

13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII

14. Про телекомунікації: Закон України від 18 листопада 2003 року № 1280-IV // ВВР, 2004, № 12, ст. 155

15. Стратегія кібербезпеки України: затверджено Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

Основна література

16. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с. URL: https://cutt.ly/lwJzWl5X

17. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с. URL: https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf

18. Інформаційна безпека держави: конспект лекцій для здобувачів вищ. освіти освіт. ступеню «бакалавр» спец. 262 «Правоохоронна діяльність» / уклад.: Ю. М. Ткач, С. М. Семендяй. Чернігів: НУ «Чернігівська політехніка», 2022. 133 с. URL: https://cutt.ly/swJznexp

19. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с. URL: https://cutt.ly/IwJzmGpN

20. Лобанчикова Н.М. Захист інформації в АСУ: навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.

21. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

22. Лобанчикова Н.М. Захист інформації в АСУ : навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.

23. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с.

Допоміжна література

24. Introduction to Information Security. URL: https://engineering.futureuniversity.com/BOOKS%20FOR%20IT/Book%20Introduction%20to%20Information.pdf

25. National Institute of Standards and Technology Special Publication 800-12 Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-12 Rev. 1, 101 pages (June 2017). URL: https://doi.org/10.6028/NIST.SP.800-12r1.

26. Грицишен Д. О., Драган І. О., Цимбалюк В. С. Правові аспекти протидії економічній злочинності в глобальному кіберпросторі. Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична. 2023. Випуск 36. С.349-355. http://dx.doi.org/10.5281/zenodo.8138965. URL: https://nzlubp.org.ua/index.php/journal/article/view/836/761

27. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз : наук-практ. посіб. / Б. Б. Теплицький, Л. Г. Шарай, К. М. Ковальов, С. А. Кузьмін. К.: ПАЛИВОДА А. В., 2019. 168 с.

28. Кібербезпека та ризики цифрової трансформації компаній : практичний посібник / Ю. І. Когут ; за ред. ректора Державного університету інтелектуальних технологій і зв'язку Назаренка О. А. Київ : Консалтингова компанія «СІДКОН»; ВД «ДАКОР», 2023. 378 с.

29. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології) : практичний посібник / Ю. І. Когут. Київ : Консалтингова компанія «СІДКОН»; ВД «Дакор» 2022. 284 с.

30. Кібертероризм (історія, цілі, об'єкти) : практичний посібник / Ю. І. Когут. Київ : Консалтингова компанія «СІДКОН», 2021. 304 с.

31. Марущак А.І., Кудрявцева Н.О. Доступ до інформації про діяльність Служби безпеки України в контексті протидії дезінформації. Вісник Харківського національного університету внутрішніх справ. 2022. № 2. С. 281-291. URL: http://nbuv.gov.ua/UJRN/VKhnuvs_2022_2_28

32. Новицький В.Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. Інформація і право. 2022. № 1. С. 111-118. URL: http://nbuv.gov.ua/UJRN/Infpr_2022_1_13

33. Субіна Т.В. Методичні підходи до вивчення питання інформаційної безпеки в органах ДФС України. Ірпінський юридичний часопис. 2021. № 1(5), С. 123-135. URL: https://doi.org/10.33244/2617-4154.1(5).2021.123-135

34. Цимбалюк В.С. Кібернетичне право як відгук на виклики міжнародному порядку. Закарпатські правові читання. Право як інструмент стійкості розвитку в умовах сучасних цивілізаційних викликів : Матеріали XV міжнародної науково-практичної конференції, м. Ужгород, 27 квітня 2023 р. Частина ІІ. Львів – Торунь : Ліха-Прес, 2023. С.36-39. http://catalog.liha-pres.eu/index.php/liha-pres/catalog/book/194 DOI: https://doi.org/10.36059/978-966-397-298-5-85

35. Цимбалюк В.С. Кібернетичне право, як прояв модернізації правової системи в умовах світової інтеграції. Модернізація вітчизняної правової системи в умовах світової інтеграції: матеріали міжнар. наук.-практ. конф., м. Кропивницький, 22-23 березня 2023 р. 2023. С.282-285. Режим доступу: https://dspace.sfa.org.ua/bitstream/123456789/2021/1/Skliar%20Yermolenko-Kniazieva%20Osoblyvosti%20pravovoho%20reg.pdf

36. Цимбалюк В.С. Кібернетичне право, як чинник забезпечення правопорядку. Забезпечення правопорядку в умовах воєнного стану та мировідбудови : зб. наук. ст. за матеріалами Всеукр. наук.-практ. конф. (Житомир, 21 квітня 2023 р.) /Мін-во освіти і науки України ; Поліський нац. ун-т. – Житомир, 2023.С.21-24.

37. Цифрова трансформація економіки та проблеми кібербезпеки : практич. посіб. / Ю. І. Когут. Київ: Консалтингова компанія «СІДКОН»; ВД «ДАКОР», 2023. 368 с.

12. Інформаційні ресурси в Інтернеті

1. Курс «Основи кібербезпеки» онлайнової платформи Cisco Netacad.com;
2. Курс «CyberSecurity Essentials 3.0» онлайнової платформи Cisco SkillsforAll.com
3. http://www.rada.gov.ua – офіційний веб-сайт Верховної Ради України.
4. http://www.kmu.gov.ua – офіційний веб-сайт Кабінету Міністрів України.
5. http://www.mvs.gov.ua – офіційний веб-сайт Міністерства внутрішніх справ України.
6. http://www.gp.gov.ua – офіційний веб-сайт Офісу Генерального прокурора
7. http://www.minjust.gov.ua – офіційний веб-сайт Міністерства юстиції України.