МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет історії, політології та національної безпеки
Кафедра музеєзнавства, пам'яткознавства та інформаційно-аналітичної діяльності

СИЛАБУС
вибіркового освітнього компонента

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

підготовки першого **(**бакалаврського) рівня вищої освіти

Луцьк – 2025

Силабус освітнього компонента «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ» підготовки бакалаврського освітнього рівня.

Розробник: Петрович В. В., доцент кафедри музеєзнавства, пам'яткознавства та інформаційно-аналітичної діяльності, к.і.н., доцент.

Погоджено
Гарант освітньо-професійної програми:

Силабус освітнього компонента затверджений на засіданні кафедри музеєзнавства, пам'яткознавства та інформаційно-аналітичної діяльності

протокол № 1 від 28 серпня 2025 р.

Завідувач кафедри:  Світлана ГАВРИЛЮК

1. ОПИС ОСВІТНЬОГО КОМПОНЕНТА

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td>Денна форма здобуття освіти</td><td>Галузь знань
02 Культура і мистецтво</td><td>Вибірковий</td></tr>
<tr><td>Кількість годин/кредитів
150/5</td><td rowspan="2">Спеціальність
029 Інформаційна, бібліотечна та архівна справа</td><td>Рік навчання: 2-й
Семестр: 3-й</td></tr>
<tr><td rowspan="4">ІНДЗ: немає</td><td>Лекції: 10 год.</td></tr>
<tr><td>Практичні (семінарські): 20 год.</td></tr>
<tr><td>Освітньо-професійна програма
«Документаційне забезпечення управління та інформаційно-аналітична діяльність»</td><td>Самостійна робота: 110 год.</td></tr>
<tr><td rowspan="2">Освітній рівень
бакалаврський</td><td>Консультації: 10 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання українська</td><td>Навчальний план 2023 р. зі змінами 2025 р.</td></tr>
</table>

ІІ. Інформація про викладача

ПІП: Петрович Валентина Василівна.

Науковий ступінь: кандидат історичних наук.

Вчене звання: доцент.

Посада: доцент кафедри музеєзнавства, пам’яткознавства та інформаційно-аналітичної діяльності.

Контактна інформація: e-mail: valyavp@ukr.net

Дні занять: див. електронний розклад https://ps.vnu.edu.ua/cgi-bin/timetable.cgi?n=700

Електронний курс «Управління інформаційною безпекою»: https://moodle.vnu.edu.ua/course/view.php?id=3332

ІІІ. Опис освітнього компонента

1. Анотація курсу

Силабус освітнього компонента «Управління інформаційною безпекою» складено з урахуванням можливості формування індивідуальної освітньої траєкторії здобувачів освіти бакалаврського рівня. Він спрямований на: формування у здобувачів вищої освіти системного уявлення про сутність, завдання та принципи інформаційної безпеки, її місце в в системі

державного управління та інформаційній сфері. У межах освітнього компоненту розглядаються нормативно-правові засади створення і розвитку системи інформаційної безпеки в інформаційній сфері, класифікація кіберзагроз і ризиків, механізми управління інформаційними ресурсами. Особлива увага приділяється захисту конфіденційних даних, безпеці інформаційних систем і мереж, забезпеченню безперервності діяльності організацій, а також сучасним викликам у сфері кіберзлочинності, шкідливого програмного забезпечення, соціальної інженерії та кризових ситуацій, пов'язаних з інформаційними загрозами.

2. Мета і завдання освітнього компонента.

Мета освітнього компонента: формування знань з основ інформаційної політики та її змісту; визначення характеристик складових системи забезпечення та управління інформаційної безпеки в Україні; формування комплексного уявлення про основні напрями здійснення державної політики з інформаційної безпеки, зокрема шляхом створення ґрунтовної нормативно-правової бази у галузі; набуття навичок оцінювання ефективності заходів у сфері управління інформаційними ризиками, захисту даних і забезпечення стабільного функціонування організацій.

Основними завданнями вивчення освітнього компонента «Управління інформаційною безпекою» є: ознайомлення з основними концепціями забезпечення інформаційної безпеки України; надання базових знання про зміст і значення інформації як об'єкта захисту; визначення та характеристика видів загроз та методів несанкціонованого доступу; формування умінь та навичок щодо аналізу державної політики та критеріїв адаптації стандартів Європи у сфері інформаційної політики до України.

3. Soft skills. Вивчення освітнього компонента дозволить здобувачам освіти розвинути комунікативні навички (навички письмової комунікації, публічних виступів, ведення діалогу), критичне мислення (вміння аналізувати першоджерела, відрізняти факти від інтерпретацій та обґрунтовувати свої висновки), навички дослідницької роботи (самостійно шукати інформацію, систематизувати її та проводити міні-дослідження з обраної теми), аналітичні здібності, організаційні та навички управління часом, уміння працювати в команді, самостійність та відповідальність.

4. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Практ. (семін.)	Сам. роб.	Консуль-тації	Форма контролю/бали
1	2	3	4	5	6	7
Змістовий модуль 1. Концептуальні основи забезпечення інформаційної безпеки						
Тема 1. Вступ до освітнього компоненту. Інформаційна безпека та її місце в системі національної безпеки	12	2		9	1	ДС

Тема 2. Інформаційна безпека та її місце в системі національної безпеки	14		4	10		ДС, УО, Р, ІРС / 6+6
Тема 3. Інформаційні загрози	14	4		10		ДС
Тема 4. Інформація як об'єкт захисту. Загрози інформації. Методи та види несанкціонованого доступу	14		4	10		ДС, ДС, УО, Р, ІРС /6+6
Тема 5. Інформаційна безпека України у сфері прав і свобод людини	12	2		9	1	ДС
Тема 6. Інформаційна система персональних даних	12		2	9	1	ДС, УО, Р, ІРС / 6
Тема 7. Медійний вимір інформаційної безпеки	12		2	9	1	ДС, УО, Р, ІРС / 6
Тема 8. Органи забезпечення інформаційної безпеки та захисту інформації	12	2		9	1	ДС
Тема 9. Основні засади державної політики України в галузі інформаційної безпеки. Правове регулювання інформаційної безпеки	12		2	9	1	ДС, УО, Р, ІРС / 6
Тема 10. Технологічне управління механізмами інформаційної безпеки	12		2	9	1	ДС, УО, Р, ІРС / 6
Тема 11. Поняття та зміст інформаційного протиборства	12		2	9	1	ДС, УО, Р, ІРС / 6
Тема 12. Кіберзлочинність: види, наслідки та способи боротьби	12		2	8	2	ДС, УО, Р, ІРС / 6
Разом за змістовим модулем	150	10	20	110	10	60 балів
Робота на семінарських заняттях						60 балів (6 балів х 10 занять)
Відвідування і робота на лекційних заняттях						10 балів
Виконання завдань самостійної роботи						10 балів
Написання підсумкової контрольної роботи						20 балів
Усього годин/ балів	150	10	20	110	10	100 балів

Форма контролю*: ДС – дискусія, ДБ – дебати, Т – тести, ТР – тренінг, РЗ/К – розв'язування задач/кейсів, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота студента, РМГ – робота в малих групах, МКР/КР – модульна контрольна робота/ контрольна робота, Р – реферат, а також аналітична записка, аналітичне есе, аналіз твору, УО – усне опитування тощо.

6. Завдання для самостійного опрацювання

Самостійна робота здобувачів вищої освіти виконується за завданням і при методичному керівництві викладача, але без його безпосередньої участі. Самостійна робота здобувачів включає як повністю самостійне освоєння окремих тем дисципліни, так й опрацювання тем, які розглядаються під час аудиторної роботи. У ході самостійної роботи здобувачі вищої освіти опрацьовують та конспектують навчальну, наукову і довідкову літературу, виконують завдання, спрямовані на закріплення знань і формування умінь та навичок, готуються до поточного і проміжного контролю з дисципліни.

№ теми	Види, зміст самостійної роботи
1	Опрацювання лекційного матеріалу. Розкрити сутність понять: «безпека», «державна безпека», «інформація», «інформаційне суспільство», «інформаційна безпека», «інформаційний захист», «інформаційна війна», «інформаційні відносини», «інформаційна безпека держави», «інформаційна безпека особи», «інформаційна безпека суспільства», «інформаційна боротьба», «інформаційне забезпечення в умовах інформаційної боротьби», «інформаційні ресурси», «конфіденційність», «конфіденційність інформації (даних) в інформаційній системі», «національні інтереси України в інформаційній сфері», «стратегія національної безпеки України», «стратегія кібербезпеки України», «управління інформаційною безпекою», «система управління інформаційною безпекою».
2	Опрацювання лекційного матеріалу. Опрацювати матеріали про складові системи забезпечення інформаційної безпеки держави.
3	Підготовка до семінарського заняття. Опрацювати матеріали про управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти.
4	Опрацювання лекційного матеріалу. Підготовка до семінарського заняття. Опрацювати матеріали про стратегію національної безпеки України.
5	Підготовка до семінарського заняття. Опрацювати матеріали про особливість системи багатофакторної аутентифікації.
6	Опрацювання лекційного матеріалу. Підготовка до семінарського заняття. Опрацювати матеріали про види інформаційних прав і свобод і їх зв’язок з іншими правами та свободами людини та громадянина.
7	Підготовка до семінарського заняття. Опрацювати матеріали про захист інформації в мобільних пристроях.
8	Підготовка до семінарського заняття. Опрацювати матеріали про удосконалення системи інформаційної безпеки телекомунікаційних мереж за допомогою страхування ризиків.
9	Підготовка до семінарського заняття. Визначте роль ЗМІ для забезпечення інформаційної безпеки в Україні. Наведіть приклади маніпулювання через ЗМІ.
10	Опрацювання лекційного матеріалу. Підготовка до семінарського заняття. Опрацювати матеріали про загальний аналіз міжнародних стандартів та вимог управління інформаційною безпекою.
11	Опрацювання лекційного матеріалу. Підготовка до семінарського заняття. Опрацювати матеріали про міжнародні критерії оцінки безпеки інформаційних ресурсів.
12	Підготовка до семінарського заняття. Здійснити класифікацію моделей захисту інформації.
13	Підготовка до семінарського заняття. Опрацювати матеріали про інформаційна безпека в умовах війни.
14	Підготовка до семінарського заняття. Опрацювати матеріали про стратегію кібербезпеки України.
15	Підготовка до семінарського заняття. Опрацювати матеріали про управління інформаційною безпекою та кіберзахистом у закладах вищої освіти.

IV. Політика оцінювання

При вивченні освітнього компонента «Управління інформаційною безпекою» застосовується поточний та підсумковий семестрові форми контролю. Також, передбачено обов’язковий контроль засвоєння навчального матеріалу освітнього компоненту, віднесеного на

самостійну роботу. Поточний контроль (засвоєння окремих тем) проводиться у формі усного опитування або письмового експрес-контролю на лекціях та семінарських заняттях, у формі виступів здобувачів вищої освіти з доповідями та під час дискусій при обговоренні навчальних питань на семінарських заняттях, у формі написання рефератів, виконання тематичних тестових завдань.

При вивченні освітнього компонента необхідно спиратися на конспект лекцій та рекомендовану навчальну, наукову і довідкову літературу. Вітається використання інших джерел з альтернативними поглядами на ті чи інші питання задля формування продуктивної дискусії з проблем курсу.

Відвідування занять є обов'язковим. У разі підписання здобувачем вищої освіти індивідуального плану обов'язковим є виконання індивідуальних завдань згідно зі встановленим викладачем графіком. Високо оцінюється прагнення здобувачів вищої освіти: регулярно відвідувати заняття; планомірно та систематично засвоювати навчальний матеріал; активно працювати на лекційних і семінарських заняттях, брати участь в обговоренні дискусійних питань; повною мірою долучатися до активних форм навчання; відпрацьовувати пропущені семінарські заняття. Навчання за індивідуальним графіком може бути організоване за допомогою дистанційних технологій навчання, або в інший спосіб (електронний особистий кабінет здобувача, електронна пошта, доступні аудіокомунікаційні сервіси).

Недопустимими є: пропуски з неповажних причин та запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття (окрім випадків, передбачених навчальним планом та методичними рекомендаціями викладача); списування та плагіат.

Здобувачі вищої освіти мають дотримуватися академічної доброчесності: самостійно виконувати усі навчальні завдання, завдання підсумкового контролю. У разі використання ідей, тверджень, відомостей при виконанні усіх завдань, передбачених силабусом, необхідно у формі посилань вказувати на джерела інформації. Дотримуватись норм законодавства про авторське право і суміжні права. Дотримуватись положень «Кодексу академічної доброчесності ВНУ імені Лесі Українки».

У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття з поважних причин та надав підтверджуючий документ, на консультаціях він має право відпрацювати пропущені заняття (усно або у формі тестування) та добрати ту кількість балів, яку було визначено на пропущені теми. Пропущені з поважних причин заняття відпрацьовуються у визначений час згідно затвердженого графіка.

Консультації здобувачам вищої освіти надаються: на кафедрі згідно графіку; онлайн через Університетський портал – Office 365, за допомогою Viber чи електронної скриньки (за попередньою домовленістю з викладачем).

Результати навчання, здобуті здобувачем освіти шляхом неформальної та/або інформальної освіти, визнаються у ВНУ імені Лесі Українки шляхом валідації. Порядок та процедура визнання регламентується «Положенням про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у ВНУ імені Лесі Українки». Визнанню можуть підлягати такі результати навчання, отримані в неформальній освіті (професійні курси/тренінги, громадянська освіта, онлайносвіта, професійні стажування та ін.), які за тематикою, обсягом вивчення та змістом відповідають як освітньому компоненту в цілому, так і його окремому розділу, темі (темам), індивідуальному завданню, тощо, які передбачені силабусом освітнього компоненту. Визнання результатів навчання, отриманих у неформальній та/або інформальній освіті, відбувається в семестрі, що передує семестру початку вивчення освітнього компонента, або під час вивчення ОК (але не пізніше початку останнього місяця навчання, враховуючи ймовірність непідтвердження здобувачем результатів такого навчання).

Загалом оцінювання здобувачів здійснюється відповідно до «Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти ВНУ імені Лесі Українки». Максимальну кількість балів (100) можна набрати упродовж семестру за результатами виконання усіх видів робіт, які передбачені силабусом:

1. Робота на семінарських заняттях (максимум 60 балів – 6 балів х 10 занять).
2. Відвідування і робота на лекційних заняттях (максимум 10 балів).
3. Виконання завдань самостійної роботи (максимум 10 балів).
4. Написання підсумкової контрольної роботи (максимум 20 балів).

V. Підсумковий контроль

Семестровий залік виставляється здобувачам освіти на підставі результатів виконання усіх видів запланованої навчальної роботи упродовж семестру за 100-бальною шкалою. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи (шкала від 0 до 100 балів).

У випадку, якщо здобувач освіти протягом поточної роботи набрав менше як 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання, анульовуються. Максимальна кількість балів на залік під час ліквідації академічної заборгованості – 100. Повторне складання заліку допускається не більше як два рази: один раз – викладачеві, другий – комісії, яку створює декан факультету.

Терміни проведення підсумкового семестрового контролю встановлюються графіком навчального процесу.

Перелік питань для підсумкового контролю:

1. Визначення понятт «інформаційна безпека» та її місце в системі національної безпеки.
2. Об’єкти, суб’єкти та види інформаційної безпеки.
3. Складові інформаційної безпеки.
4. Визначення національних інтересів України в інформаційній сфері та шляхів їх забезпечення.
5. Система інформаційної безпеки.
6. Поняття «національних інтересів» і його відмінність від поняття «національна безпека».
7. Класифікація національних інтересів.
8. Інформація як об’єкт захисту.
9. Властивості інформації. Її види.
10. Відповідальність за порушення законодавства України про інформацію.
11. Визначення поняття «інформаційні загрози».
12. Класифікація загроз. Класифікація вразливостей систем безпеки.
13. Інформаційні ризики.
14. Витік інформації.
15. Види дестабілізуючих факторів.
16. Методи та види несанкціонованого доступу.
17. Модель порушника.
18. Підготовчі дії порушника перед несанкціонованим доступом до інформації.
19. Види інформаційних прав і свобод і їх зв’язок з іншими правами та свободами людини та громадянина.
20. Структура конституційного права на інформацію.
21. Маніпулювання в медіа як загроза інформаційній безпеці.
22. Соціальні медіа як середовище для поширення негативних інформаційних впливів.
23. Правові засади та державне регулювання діяльності медіа в Україні.
24. Загальні принципи управління безпекою об’єкта інформаційної діяльності.
25. Система управління інформаційною безпекою. Методи захисту інформації.
26. Технічні системи захисту даних. Функції технологічного управління механізмами безпеки.
27. Організаційні засоби захисту інформації.
28. Кіберзлочинність: види, наслідки та способи боротьби
29. Поняття та зміст інформаційного протиборства.
30. Нормативно-правове забезпечення інформаційної безпеки України.
31. Основні засади державної політики України в галузі інформаційної безпеки.

32. Роль та значення правового регулювання інформаційної безпеки.
33. Особливості реалізації адміністративно-правових форм та методів у сфері забезпечення інформаційної безпеки
34. Органи забезпечення інформаційної безпеки та захисту інформації.
35. Напрями державної політики щодо сфери інформаційної безпеки.
36. Особливості інформаційної безпеки у різних сферах життя суспільства.
37. Інформаційна безпека підприємств та організацій.
38. Системи інформаційної безпеки.
39. Механізми стратегічного інформаційного протиборства.
40. Міжнародні аспекти інформаційної безпеки в умовах глобалізації.

VI. Шкала оцінювання

Оцінка в балах	Лінгвістична оцінка
90 – 100	Зараховано
82 – 89	
75 – 81	
67 –74	
60 – 66	
1 – 59	Незараховано (необхідне перескладання)

VII. Рекомендована література та інтернет-ресурси

Нормативно-правові акти та стандарти

1. Положення про порядок здійснення криптографічного захисту інформації в Україні : Указ Президента України від 22 травня.1998 року № 505/98 (Редакція від 12.09.2009). URL : https://zakon.rada.gov.ua/laws/show/505/98#Text.

2. Положення про технічний захист інформації в Україні : Указ Президента України від 27 вересня 1999 року № 1229/99 (Редакція від 04.05.2008). URL : https://zakon.rada.gov.ua/laws/show/1229/99#Text.

3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 липня 1994 р. № 80/94ВР (Редакція від 20.04.2025). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

4. Про інформацію. Закон України від 02 жовтня 1992 року № 2657-XII (Редакція від 14.06.2025). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

5. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII (Редакція від 30.08.2025). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

6. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09 січня 2007 р. № 537-V (Редакція від 09.01.2007). URL: https://zakon.rada.gov.ua/laws/show/537-16#Text.

7. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 року № 392/2020 (Редакція від 07.01.2025). URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

8. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». Указ Президента України №152/2022. URL: https://www.president. gov.ua/documents/1522022-41761.

9. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. № 200.

10. ISO/IEC 27001:2022 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги. URL: URL: https://www.iso.org/standard/82875.html.

Основна література

1. Актуальні проблеми інформаційної безпеки : навч. посіб. / О. О. Тихомиров, А. В. Ватраль, Д. С. Мельник та ін. Одеса : Видавництво «Юридика», 2025. 264 с. URL: https://ippi.org.ua/sites/default/files/zmist_apib.pdf.

2. Бобало Ю. А., Горбатий І. В., Кіселичник М. Д., Бондарєв А. П. Інформаційна безпека : навч. посіб. Львів : Вид-во Львівської політехніки, 2019. 580 с. URL: https://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf.

3. Гребенюк А. М., Рибельченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпроп. держ. ун т внутріш. справ, 2020. 144 с. URL: https://surli.cc/jxjlgr.

4. Гур'єв В. І., Мехед Д. Б., Ткач Ю. М., Фірсова І. В. Інформаційна безпека держави : навч. посіб. Ніжин : ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с. URL: https://ir.stu.cn.ua/server/api/core/bitstreams/f2ce2b33-6c76-4b1c-811e-bbb3f2f3346c/content.

5. Законодавчі питання інформаційної безпеки : електр. навч. посіб. / укл. : Кушнір М. Я., Цеханський В. Д. Чернівці : Чернівецький національний університет, 2024. 102 с. URL: https://drive.google.com/file/d/1r7JUzLpdq-RM2Oq-iDM_Uzk3nG4V2wAC/view.

6. Нестеренко Г. Інформаційна безпека : курс лекцій. Київ : НАУ, 2022. 102 с. URL: https://duikt.edu.ua/uploads/l_1426_56444238.pdf.

7. Управління інформаційною безпекою : консп. лекцій : навч. посіб. / КПІ ім. Ігоря Сікорського ; уклад. : С. О. Носок, О. М. Фаль, В. М. Ткач. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с. URL: https://ela.kpi.ua/items/30243ca5-b522-4179-993c-f32eab6b0fd1.

8. Управління інформаційною безпекою : навч. посіб. ; уклад.: Толюпа С. В., Політанський Л. Ф., Політанський Р. Л., Лесінський В. В. Чернівці : Чернівецький нац. ун-т ім. Ю. Федьковича, 2021. 540 с. URL: https://drive.google.com/file/d/160LvEO5XQnbtZFsQb2L_wA8bJEnjBnch/view.

9. Якименко І. З. Менеджмент інформаційної безпеки. Конспект лекцій. Тернопіль, 2019. 136 с. URL: https://surl.li/ohkciz.

Додаткова література

1. Гаврильців М. Т. Інформаційна безпека держави у системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200–203. URL: http://lsej.org.ua/2_2020/54.pdf.

2. Горулько В. Роль та місце інформаційної безпеки в загальній системі національної безпеки держави. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2022. № (34). С. 103–108. URL: https://doi.org/10.26565/2075-1834-2022-34-12.

3. Желновач Є. Інформаційне суспільство в умовах війни: українські реалії та правові аспекти. *Юридичний вісник*. 2023. № 4. С. 184–191. URL: http://yurvisnyk.in.ua/v4_2023/24.pdf.

4. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

5. Івануса А. І., Ткачук Р. Л., Маслова Н. О., Ящук В. І., Ткаченко А. М. Управління інформаційною безпекою та кіберзахистом у закладах вищої освіти. *Bulletin of Lviv State University of Life Safety*. 2025. № 31. С. 101–116. URL: https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/16220/1/%d0%a1%d1%82%d0%b0%d1%82%d1%82%d1%8f%20%282%29.pdf.

6. Іванченко Н. О., Подскребко О. С. Особливості реалізації системи управління інформаційною безпекою. *Scientific method: reality and future trends of researching*. 2023. С. 19–21. URL: https://previous.scientia.report/index.php/archive/article/view/813.

7. Капелюшна Т. В., Легомінова С. В., Мужанова Т. М. Регуляторне поле формування політики управління інформаційною безпекою організації. *Кібербезпека: освіта, наука, техніка.* 2024. № 2 (26). С. 235–243. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/693.

8. Капля О. М. Правове регулювання інформаційної безпеки громадянина під час дії воєнного стану. *Експерт: парадигми юридичних наук і державного управління*, 2023. № 6(24). С. 16–20. URL: https://doi.org/10.32689/2617-9660-2022-6(24)-16-20.

9. Клочкова Д. Ю., Пшеничних С. В. Класифікація моделей систем захисту інформації. Інформаційно-комунікаційні технології та кібербезпека : матеріали Міжнар. наук.-тех. конф. м. Харків, 7–8 груд. 2023. Харків, 2023. С. 196–197. URL: https://ice.nure.ua/wp-content/uploads/2024/01/59_Klochkova-D.Iu.-Pshenychnykh-S.V._2._Str.196-197.pdf.

10. Лисенко С. О. Принципи державного управління інформаційною безпекою та їхня характеристика. *Держава та регіони. Серія: Публічне управління і адміністрування*. 2024. № 1. С. 169–174. URL: http://pa.stateandregions.zp.ua/archive/1_2024/29.pdf.

11. Мазуренко Л. Інформаційна безпека громадянина в умовах воєнного стану: проблеми правового регулювання. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони*: *проблеми, досвід, перспективи* : матеріали IV міжнар. наук.-практ. конф. м. Київ, 27 верес. 2023 р. К. : НУОУ, 2023. С. 189–191.

12. Національні системи оцінювання ризиків і загроз: кращі світові прак тики, нові можливості для України : аналіт. доп. ; за заг. ред. О. О. Резнікової. Київ : НІСД, 2020. 84 с. URL: https://niss.gov.ua/sites/default/files/2020-07/dopovid.pdf.

13. Панченко В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти. *Актуальні проблеми правознавства.* 2020. № 1 (21). С. 103–109. URL: https://dspace.wunu.edu.ua/bitstream/316497/38493/1/%d0%9f%d0%b0%d0%bd%d1%87%d0%b5%d0%bd%d0%ba%d0%be.pdf.

14. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення. *Науковий вісник Ужгородського національного університету, Серія право*. 2017. Вип. 42. С. 16–22. URL: https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/2918c010-b328-442c-a033-6078dee83336/content.

15. Правдюк А. Л. Конституційні гарантії інформаційної безпеки людини і громадянина. *Юридичний науковий електронний журнал*. 2021. № 12. С. 303–305. URL: http://www.lsej.org.ua/12_2021/76.pdf.

16. Француз-Яковець Т. А. Інформаційна безпека в умовах війни. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)* : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 черв. 2022 р.). Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 329–331. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/1c25aa92-f044-4b06-bbf6-c4fe7219ea77/content.

17. Храпкін О. Стратегічне управління інформаційною безпекою підприємства: сучасні підходи та виклики. *Проблеми і перспективи економіки та управління*. 2023. № 4(36). С. 86–94. URL: https://ir.stu.cn.ua/server/api/core/bitstreams/5dc62dbb-938e-4870-a307-da7d14198d7a/content.

18. Чмир Я. Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2022. Вип. 2 (62) С. 149–154. URL: https://doi.org/10.32689/2523-4625-2022-2(62)-23.

19. Bosak A., Verzhykovskyi V., Kalinin I., Maksymiv I., Prystupa D., Ryvak O. Principles of formation of enterprise information security. *International scientific journal «Internauka». Series: «Economic Sciences»*. 2023. № 11(79). URL: https://doi.org/10.25313/2520-2294-2023-11-9157.

20. Kurii Y., Opirskyy I. (). ISO 27001: analysis of changes and peculiarities of compliance with the new version of the standard. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2023. Т. 3. № 19. С. 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655.

21. Xing J. The Application of Artificial Intelligence in Computer Network Technology in Big Data Era. 4thInternational Workshop on Materials Engineering and Computer Sciences. 2019. S. 211–215. URL: https://doi.org/10.25236/ iwmecs.2019.044.

Інтернет-ресурси з профілю ОК

1. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 26 берез. 2021 р.). Київ : НА СБУ, 2021. 346 с. URL: https://eportfolio.kubg.edu.ua/data/conference/7238/document.pdf.

2. Актуальні проблеми управління інформаційною безпекою держави : зб. матер. всеукр. наук.-практ. конференції. Київ : Нац. акад. СБУ, 2023. 618 с. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/12539/1/p_57_92088934.pdf.

3. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: https://www.gurt.org.ua/articles/34602/.

4. Стратегія розвитку інформаційного суспільства в Україні. URL: https://www.old.nas.gov.ua/siaz/Ways_of_development_of_Ukrainian_science/article/12116.1.083.pdf