МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ
Кафедра музеєзнавства, пам’яткознавства та інформаційно-аналітичної діяльності

Валентина ПЕТРОВИЧ

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

(методичні рекомендації для здобувачів вищої освіти першого (бакалаврського) рівня підготовки спеціальності В13 «Бібліотечна, інформаційна та архівна справа»)

Луцьк – 2026

УДК 389 Д 439
П 30

Рекомендовано до друку науково-методичною радою
Волинського національного університету імені Лесі Українки
(Протокол № від 2026 р.)

Рецензент:
Пахолок В. М. – кандидат політичних наук, доцент, доцент кафедри політології та публічного управління Волинського національного університету імені Лесі Українки

Петрович В. В. Управління інформаційною безпекою: методичні рекомендації для здобувачів вищої освіти першого (бакалаврського) рівня підготовки спеціальності В13 «Бібліотечна, інформаційна та архівна справа». Луцьк, 2026. 40 с.

У методичному виданні представлено навчально-методичний комплекс з освітнього компонента «Управління інформаційною безпекою» для здобувачів вищої освіти спеціальності В13 «Бібліотечна, інформаційна та архівна справа» освітньо-професійної програми «Документаційне забезпечення управління та інформаційно-аналітична діяльність» першого (бакалаврського) рівня підготовки. Подано силабус, який дасть змогу ознайомитися із змістовою складовою та структурою освітнього компонента, темами, які виноситимуться на лекційні та практичні (семінарські) заняття, самостійну роботу; рекомендації щодо їх підготовки, наукова й навчальна література; термінологічний словник.

Рекомендовано здобувачам вищої освіти спеціальності В13 Бібліотечна, інформаційна та архівна справа.

УДК 389 Д 439

ЗМІСТ

ВСТУП

В умовах стрімкого розвитку технологій і зростання кількості кіберзагроз, питання інформаційної безпеки набуває особливої важливості. Зі збільшенням обсягу цифрових даних зростає ризик кібератак і незаконного використання цієї інформації. Захист таких даних стає не просто необхідністю, а стратегічним пріоритетом. Незалежно від сфери діяльності, актуальним залишається формування ефективної стратегії забезпечення інформаційної безпеки, що включає розробку та впровадження комплексу заходів для захисту конфіденційних даних та інформаційних процесів. Це передбачає також формування чітких вимог до персоналу, керівників і технічних служб. Важливо пам’ятати, що інформація стає одним із ключових активів бізнесу, і її втрата або пошкодження можуть спричинити значні фінансові збитки та підрив репутації. Тому забезпечення інформаційної безпеки включає не лише технічні рішення, але й організаційні заходи для захисту від подібних ризиків

Актуальність вивчення освітнього компоненту «Управління інформаційною безпекою» для здобувачів вищої освіти спеціальності В13 Бібліотечна, інформаційна та архівна справа базується на наукових досягненнях інформаційної галузі та її трансформаціях в умовах цифровізації комунікаційного простору, орієнтує на пізнання закономірностей функціонування документно-інформаційних систем, розвиток теорії управління інформаційними, архівними та бібліотечними установами.

Освітній компонент «Управління інформаційною безпекою» відіграє важливу роль у підготовці майбутніх фахівців до професійної діяльності. Метою даного освітнього компоненту є 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.

Її вивчення передбачає розв'язання низки завдань підготовки фахівців вищої кваліфікації, зокрема: 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.

Методичні рекомендації з нормативного освітнього компоненту «Управління інформаційною безпекою» підготовлені для здобувачів вищої освіти першого (бакалаврського) рівня підготовки спеціальності В13 Бібліотечна, інформаційна та архівна справа освітньої програми «Документаційне забезпечення управління та інформаційно-аналітична діяльність». Вони вміщають силабус нормативного освітнього компонента, теми та плани семінарських занять, рекомендації до організації самостійної роботи з освітнього компонента, політику оцінювання здобувачів, питання підсумкового контролю, список рекомендованої літератури та інтернет-ресурсів. Методичне видання включає також термінологічний словник, який включає найважливіші терміни, засвоєння розуміння яких дасть змогу якісно засвоїти навчальний матеріал курсу.

РОЗДІЛ 1
СИЛАБУС НОРМАТИВНОГО ОСВІТНЬОГО КОМПОНЕНТУ «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

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
В «Культура, мистецтво та гуманітарні науки</td><td>Нормативний</td></tr>
<tr><td>Кількість годин/кредитів 150/5</td><td rowspan="3">Спеціальність
В13 Бібліотечна, інформаційна 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 ступінь
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>

1. Анотація освітнього компонента. 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 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	12	2		9	1	ДС

інформаційної безпеки та захисту інформації						
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*: Форма контролю*: ДС – дискусія, Т – тести, Р – реферат, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота здобувача, УО – усне опитування тощо.

РОЗДІЛ 2
ПЛАНИ ПРАКТИЧНИХ (СЕМІНАРСЬКИХ) ЗАНЯТЬ І ПОРАДИ ЩОДО ЇХ ПІДГОТОВКИ

Практичні заняття – це форма освітнього процесу, яка передбачає обговорення питань, які стосуються раніше прослуханої лекції або наперед визначеної теми чи розділу освітнього компонента. Завдання викладача під час практичного (семінарського) заняття – організувати роботу так, щоб здобувачі змогли поглибити і закріпити теоретичні знання, отримані під час лекцій, самостійної роботи, загалом у процесі вивчення освітнього компонента. Готуючись до семінарів і у ході їх проведення важливо розвивати аналітичне мислення, уміння аналізувати й творчо застосовувати на практиці теоретичний матеріал, старатися зрозуміти, де він може згодитися при практичній діяльності. При підготовці до семінарів і під час їх проведення увага приділяється виробленню у здобувачів професійних навичок, дослідницького підходу до матеріалу, що вивчається, формується вміння оперувати відповідною термінологію, розуміти її суть, аналізувати й узагальнювати наукову інформацію.

Практичні (семінарські) заняття не дублюють лекції, а є їх логічним продовженням, оскільки поглиблюють знання здобувачів освіти, розвивають творчу самостійність, цікавість до наукових досліджень, дозволяють поєднати науково-теоретичні положення з практичним застосуванням. На семінарських заняттях здобувачі оволодівають новими дефініціями, вчяться вести наукові дискусії, відстоювати й аргументувати власну точку зору, здобувають навики оформлення рефератів, уміння усного та письмового викладу матеріалу, прилюдного захисту наукових положень і висновків.

Семінарське заняття проводиться в академічній групі викладачем за наперед визначеними темами і планами, як правило, після прочитаної лекції з відповідної теми освітнього компоненту і самостійної підготовки здобувачів

освіти. Питання, які виносяться на самостійне опрацювання здобувачів, наведені у силабусі. Під час заняття здобувачі вищої освіти виступають із доповідями та повідомленнями, інші доповнюють їх виступи, ставлять запитання, беруть участь у дискусії. Викладач спрямовує обговорення виступів, ставить запитання, щоб викликати обмін думками, уточнює. Усі здобувачі повинні готувати запропоновані питання відповідної теми, щоб мати змогу доповнити, заперечити, аргументувати власну думку. Здобувачі виступають за бажанням або за викликом викладача. Викладач заохочує їх до пошуку додаткових джерел і наукової літератури з теми, спонукає до дослідницької роботи.

Особливість практичного (семінарського) заняття полягає в тому, що здобувачі освітнього ступеня «бакалавр» на основі запропонованих викладачем джерел і наукової літератури самостійно вивчають певну тему освітнього компонента, готують презентації, реферати, повідомлення, рецензування, матеріал для доповнення викладених напрацювань попереднього доповідача, беруть участь у розгорнутій дискусії тощо. Для перевірки знань на семінарському занятті можуть проводитися контрольні роботи у вигляді тестів або розгорнутих відповідей на запропоновані викладачем питання. Здобувачі освіти під час семінарів можуть усно і письмово викладати навчальний матеріал. Кожна із форм відповіді оцінюється відповідними балами.

Найпоширенішим, на нашу думку, видом практичного заняття (семінару) є семінар-доповідь (повідомлення). Він потребує ґрунтовної підготовки кожного питання теми, використання низки джерел і наукової літератури. Семінар розпочинається вступним словом викладача, який звертає увагу на тему, яка буде розглядатися, питання, що винесені на обговорення, окремі організаційні аспекти. На семінарському занятті здобувач послідовно викладає свої думки, підтверджує їх фактами, ілюструє переконливими прикладами, може підготувати презентацію. Решта здобувачів уважно його слухають, аби бути готовими до доповнень, підтверджуючи чи спростовуючи викладене.

Доповіді та повідомлення здобувачів мають включати такі складові як короткий вступ, основний зміст викладу питання, обов'язково – висновок. Кожна з таких складових відіграє вагому роль, несе певне смислове навантаження. Якість виступу залежить від наперед сформованого плану виступу (певної концепції), чіткості його побудови, здатності переконливо аргументувати наведені твердження та зробити об'єктивні ґрунтовні висновки. У вступі, зокрема, варто наголосити на актуальності питання, з якого виступає студент, ролі означеного питання у поглибленому вивченні теми. Здобувач повинен коротко поінформувати про проведену роботу з підготовки питання: які джерела опрацював, наукову літературу кого з дослідників та вчених вдалося прочитати й опрацювати, звернути увагу на методи узагальнення опрацьованої інформації. Усе це дозволить здобувачам краще зорієнтуватися у предметі обговорення, налаштуватися на сприйняття думок доповідача, виявити певний інтерес до питання.

Основний зміст виступу на семінарі повинен включати вагомі теоретичні положення, факти, розкривати зміст і методи проведених досліджень, подавати аналіз отриманих результатів, узагальнювати їх. Відповідь на кожне питання теми повинна завершуватися висновками (певними підсумками, узагальненнями, рекомендаціями тощо). Якщо, на думку виступаючого, тема потребує подальшого вивчення, то необхідно зазначити, які саме аспекти теми є суперечливими і на чому у подальших дослідженнях варто зосередити увагу.

Практичні (семінарські) заняття з ОК «Вступ до фаху» можуть, як варіант, відбуватися у формі семінару-диспуту, семінару-конференції, інше. На кожному практичному (семінарському) занятті можуть заслуховуватися попередньо підготовлені здобувачами вищої освіти реферати, повідомлення, що значно урізноманітнює такі форми проведення навчальних занять. За підготовку і виголошення рефератів в оцінюванні передбачені окремі бали.

№ з/п	Тема	Кількість годин
1-2	**Інформаційна безпека та її місце в системі національної безпеки**	4

План:

1. Визначення поняття «інформаційна безпека».
2. Об’єкти, суб’єкти та види інформаційної безпеки.
3. Визначення національних інтересів України в інформаційній сфері та шляхів їх забезпечення.
4. Система інформаційної безпеки.
5. Поняття «національних інтересів» і його відмінність від поняття «національна безпека».
6. Обумовленість національних інтересів.
7. Класифікація національних інтересів.
8. Національні інтереси в інформаційній сфері.

3-4	**Інформація як об’єкт захисту. Загрози інформації. Методи та види несанкціонованого доступу**	4

План:

1. Інформація як об’єкт захисту.
2. Модель порушника. Підготовчі дії порушника перед несанкціонованим доступом до інформації.
3. Визначення поняття «загроза». Сучасні загрози.
4. Класифікація зовнішніх загроз:
   а) шкідливі програми (віруси, трояни, черв’яки і т. п.);
   б) атаки хакерів;
   в) Dos-атаки, Ddos-атаки$
   г) таргінг атаки;
   д) спам;
   е) фішинг;
   ж) промислові загрози;
   з) шпигунське програмне забезпечення;
   к) ботнети або зомбі-мережі.
4. Технологія інфраструктури відкритих ключів.
5. Системи одноразових паролів.
6. Криптографічний захист даних.
7. Електронний підпис (ЕП).

5	**Основні засади державної політики України в галузі інформаційної безпеки. Правове регулювання інформаційної безпеки** **План:** 1. Поняття державно-правового механізму інформаційної безпеки. 2. Поняття та особливості інформаційної політики держави. 3. Напрями державної інформаційної політики. 4. Нормативно-правова основа політики національної безпеки в інформаційній сфері.	2
6	**Медійний вимір інформаційної безпеки** **План:** 1. Поняття, історія та класифікація медіа. 2. Маніпулювання в медіа як загроза інформаційній безпеці. 3. Соціальні медіа як середовище для поширення негативних інформаційних впливів. 4. Правові засади та державне регулювання діяльності медіа в Україні.	2
7	**Технологічне управління механізмами інформаційної безпеки** **План:** 1. Загальні принципи управління безпекою об’єкта інформаційної діяльності (ОІД). 2. Система управління інформаційною безпекою. Методи захисту інформації. 3. Технічні системи захисту даних. Функції технологічного управління механізмами безпеки. 4. Організаційні засоби захисту інформації. 5. Механізми інформаційної безпеки. 6. Управління ризиками інформаційної безпеки (стандарт ISO/IEC 27000).	2
8	**Кіберзлочинність: види, наслідки та способи боротьби**	2

План:

1. Характеристика кіберзлочинності.
2. Стан кіберзлочинності в Україні.
3. Боротьба із кіберзлочинами.

9 **Інформаційна система персональних даних** 2

План:

1. Нормативні документи захисту даних.
2. Конфіденційність персональних даних.
3. Захист персональної інформації.
4. Європейська система захисту персональних даних.

10 **Поняття та зміст інформаційного протиборства** 2

План:

1. Основні форми інформаційного протиборства.
2. Основні форми інформаційної війни.
3. Інформаційна зброя в інформаційній війні.

РОЗДІЛ 3
РЕКОМЕНДАЦІЇ ДО ОРГАНІЗАЦІЇ САМОСТІЙНОЇ РОБОТИ

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

№ 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.

РОЗДІЛ 4
ПОЛІТИКА ОЦІНЮВАННЯ ЗДОБУВАЧІВ

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).

РОЗДІЛ 5
ПИТАННЯ ДО ПІДСУМКОВОГО КОНТРОЛЮ

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.

Шкала оцінювання знань здобувачів освіти з освітнього компонента

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

РОЗДІЛ 6
ТЕРМІНОЛОГІЧНИЙ СЛОВНИК

Аналіз ризиків передбачає вивчення моделі загроз для інформаційної сфери організації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в організації.

Безпека – складне соціальне явище, багатопланове та багатогранне у своїх структурних складових і проявах, що відображає розбіжність інтересів різних соціальних суб'єктів.

Воєнна безпека – захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз.

Громадська безпека і порядок – захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини та громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації й захисту національних інтересів.

Державна безпека – захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру.

Забезпечення інформаційної безпеки держави – це сукупність заходів, призначених для досягнення стану захищеності потреб особи, суспільства й держави в інформації.

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особи, суспільства й держави в інформаційній сфері.

Загрози національній безпеці України – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.

Інтереси держави в інформаційній сфері полягають у створенні умов: для гармонійного розвитку державної інформаційної інфраструктури; для реалізації конституційних прав і свобод людини та громадянина в галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Інтереси особи в інформаційній сфері полягають: у реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку; у захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають: у забезпеченні інтересів особи в цій сфері; у зміцненні демократії; у створенні правової соціальної держави; у досягненні та підтриманні суспільного спокою; у духовному відновленні держави.

Інформатизація:

1) сукупність взаємопов’язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку й використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки;

2) діяльність, спрямована на створення та широкомасштабне використання в усіх сферах життя суспільства інформаційних технологій.

Інформатика: наукова діяльність, що вивчає інформаційні структури та процеси збирання (набуття, придбання), відображення, реєстрації, накопичення, збереження і поширення (розповсюдження, реалізацію) інформації за допомогою комп'ютерної техніки.

Інформація:

1) документовані або публічно проголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі;

2) відомості про осіб, предмети, технології, засоби, ресурси, події та явища, що відбуваються в усіх сферах діяльності держави, життя суспільства, та навколишньому природному середовищі, незалежно від форми їх представлення, будь-які знання про предмети, факти, поняття і т. ін. проблемної сфери, якими обмінюються користувачі системи оброблення даних.

Інформаційна агресія – незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом обмеженого та локального по своїх масштабах застосування сили.

Інформаційна безпека – захищеність (стан захищеності) основних інтересів особи, суспільства і держави у сфері інформації, включаючи інформаційну й телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі як повнота, об'єктивність, доступність і конфіденційність. Інформаційна безпека є складовою національної безпеки. Але особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо.

Інформаційна боротьба – це боротьба з використанням спеціальних способів і засобів для впливу на інформаційну сферу (середовище) конфронтуючої сторони, а також для захисту власної інформаційної сфери в

інтересах досягнення поставленої мети. Інформаційна боротьба може бути як самостійним видом, так і складовою частиною будь-якого іншого різновиду боротьби (збройної, ідеологічної, економічної і т. ін.). Вона ведеться постійно як у мирний, так і у воєнний час. Масштаби інформаційної боротьби настільки великі, що її підготовка й ведення повинні носити плановий, систематичний характер, заснований на глибоких знаннях законів і закономірностей інформаційної боротьби.

Інформаційна війна – найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктів між державами, націями, класами й соціальними групами шляхом широкомасштабної реалізації народами, засобів і методів інформаційного насильства (інформаційної зброї); процес боротьби між суб'єктами із застосуванням інформаційної зброї.

Інформаційна зброя: засоби, які дозволяють здійснювати замислені дії з повідомленнями, що передаються, обробляються, створюються, знищуються і сприймаються.

Інформаційна зброя атаки – це інформаційна зброя, за допомогою якої здійснюється вплив на інформацію, що зберігається, обробляється й передається в інформаційно-обчислювальних мережах (ІОМ) і (або) порушуються інформаційні технології, що застосовуються в ІОМ.

Інформаційна експансія – діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою: поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії; витіснення положень національної ідеології і національної системи цінностей і заміщення їхніми власними цінностями й ідеологічними установками; збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і

національними ЗМІ; нарощування присутності власних ЗМІ в інформаційній сфері об’єкта проникнення і т. ін.

Інформаційна інфраструктура: сукупність взаємодіючих систем виробництва, накопичення, збереження і розвитку інформаційних продуктів та їх доставки, виробництво інформаційних технологій, сервісного обслуговування інфраструктури й системи підготовки кадрів.

Інформаційна кооперація – форма забезпечення інформаційної безпеки між рівноправними суб’єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі й інформаційні загрози та захист від них доступними законними способами і засобами.

Інформаційна протидія – сукупність заходів інформаційної боротьби, спрямованих на протидію інформаційному забезпеченню протиборчої сторони. Інформаційна протидія включає блокування добування, обробки й обміну інформацією та впровадження дезінформації на всіх етапах інформаційного забезпечення. Завдання інформаційної протидії вирішуються шляхом маскування, контррозвідки, радіоелектронного придушення й руйнування інформаційних систем противника. Інформаційний захист – це сукупність заходів захисту від інформаційної протидії противника, які включають дії з деблокування інформації, необхідної для вирішення завдань управління, і блокування дезінформації, що поширюється й упроваджується в систему управління.

Інформаційна система – організаційно впорядкована сукупність інформаційних ресурсів та інформаційних технологій і засобів забезпечення інформаційних процесів.

Інформаційна сфера – це сфера діяльності суб’єктів, пов’язана із створенням, перетворенням і споживанням інформації. Інформаційна сфера умовно поділяється на три основні предметні частини: створення і поширення

вихідної та похідної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації; створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення; створення й застосування засобів і механізмів інформаційної безпеки.

Інформаційне забезпечення: підтримка засобами систем баз даних і баз знань процесів виробництва, торгівлі, керування, навчання, наукових досліджень та будь якої іншої діяльності в усіх сферах життя суспільства, які спрямовані на створення умов для задоволення інформаційних потреб людини, суспільства та держави.

Інформаційне забезпечення в умовах інформаційної боротьби являє собою комплекс заходів добування інформації про противника в умовах протиборства, збирання інформації про свої сили і засоби, обробка інформації й обмін нею між органами керування з метою організації і ведення бойових дій. Результативність інформаційного забезпечення залежить від багатьох факторів і умов, які, зрештою, здійснюють вплив на два основних елементи: інформування органу керування і сприйняття одержаної ним інформації.

Інформаційне протиборство – суперництво соціальних систем (країн, блоків країн) в інформаційній сфері щодо впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку; форма забезпечення інформаційної безпеки при здійсненні навмисних деструктивних дій суб’єктів інформаційного процесу.

Інформаційне середовище: усталене поєднання окремих суб’єктів національного інформаційного простору України, інформаційної інфраструктури та інформаційних ресурсів, що взаємодіють в інформаційних процесах.

Інформаційне суспільство: 1) суспільство, в якому більшість робітників займаються створенням, збиранням, відображенням, реєстрацією,

накопиченням, збереженням і поширенням інформації, особливо її вищої форми – знань; 2) суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку.

Інформаційні відносини – відносини, які виникають у всіх сферах життя й діяльності держави, суспільства і людини при одержанні, використанні, поширенні та зберіганні інформації.

Інформаційні ресурси:

1) сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

2) організована сукупність інформаційних продуктів певного призначення, що необхідні для забезпечення інформаційних потреб громадян, суспільства, держави в певній сфері життя чи діяльності.

Інформаційний захист досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки.

Інформаційний патронат (лат. patronatys від patronys – «захисник») – форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави.

Інформаційний простір (національний):

1) інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту та поширення інформації, інформаційних продуктів і ресурсів, на яке поширюється юрисдикція держави;

2) сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства і держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб'єктів держави на всій її

території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм.

Інформаційний ринок: система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг. Інформаційний продукт (продукція):

1) документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

2) документована інформація, яку підготовлено відповідно до потреб користувачів і яка призначена для задоволення потреб користувачів;

3) створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача.

Інформаційний суверенітет – здатність держави контролювати й регулювати потоки інформації поза межами держави з метою дотримання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

Інформаційні технології: 1) цілеспрямована організована сукупність інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування; 2) цілеспрямовано організована сукупність інформаційних процесів для створення і використання інформаційних продуктів або надання інформаційних послуг; 3) технологічний процес, предметом перероблення й результатом якого є інформація; 4) процес матеріалізації знань у продукцію і послуги за допомогою комп'ютерно-телекомунікаційних систем; 5) система методів і способів використання комп'ютерної техніки та систем зв'язку для створення, пошуку, одержання, відображення, реєстрації, накопичення, збереження, захисту й поширення інформаційних продуктів.

Комп'ютерні віруси (від лат. virus – «отрута»)] – це спеціальні програми, які здатні самочинно розмножуватися, створюючи свої копії, і поширюватися, модифікуючи (заражаючи) інші програми шляхом приєднання до них для наступного одержання управління та відтворення нових копій.

Концепція інформаційної безпеки в організації представляє систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації.

Конфіденційна інформація – це відомості, які є у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються на їх бажання відповідно до передбачених ними умов.

Конфіденційність – захист від несанкціонованого доступу до інформації.

Конфіденційність інформації (даних) в інформаційній системі – це властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом інформаційної системи. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Концепція інформаційної війни – це система поглядів на інформаційну війну та шляхи її ведення.

Національні інтереси України – життєво важливі інтереси людини, суспільства й держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності й добробут її громадян.

Національні інтереси України в інформаційній сфері – збалансована сукупність соціальних інтересів особистості, суспільства та держави, що реалізуються в інформаційній сфері.

Об'єкт інформаційної безпеки організації – це об'єкт (об'єкти) організації, вплив порушника інформаційної безпеки на який (які) може призвести до реалізації загрози інформаційній безпеці організації. Управління об'єктом відповідно до заданої політики інформаційної безпеки організації щодо

специфічних дій, що відносяться до інформаційної безпеки організації, здійснюється єдиним керівним органом (адміністратором) системи забезпечення інформаційної безпеки організації.

Органи інформаційної війни – це органи керування інформаційною війною та люди (фахівці, офіцери, підрозділи) для її ведення.

Політику з інформаційної безпеки організації можна визначити як сукупність вимог та правил з інформаційної безпеки організації для об'єкта інформаційної безпеки, вироблених з метою протидії заданій множині загроз інформаційній безпеці організації з урахуванням цінності інформаційної сфери, що підлягає захисту та вартості системи забезпечення інформаційної безпеки.

Система забезпечення інформаційної безпеки організації (СЗІБ) являє собою сукупність правових норм, організаційних та технічних заходів, служб інформаційної безпеки та механізмів захисту, органів управління та виконавців, спрямованих на протидію заданій множині загроз інформаційній безпеці організації з метою звести до мінімуму можливі збитки користувачу або оператору зв'язку організації. Адміністратором (керівним органом) системи забезпечення інформаційної безпеки організації може бути фізична або юридична особа, яка є відповідальною за реалізацію політики забезпечення інформаційної безпеки організації.

Сприйняття інформації – процес формування в органі керування уявлення про ситуацію, включаючи її кількісні та якісні параметри. Найбільш суттєві характеристики при цьому – розпізнавальні ознаки істинних і неправдивих елементів ситуації.

Стратегія воєнної безпеки України – документ, у якому викладається система поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їх виникненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів.

Стратегія громадської безпеки та цивільного захисту України – документ довгострокового планування, що розробляється на основі Стратегії національної безпеки України за результатами огляду громадської безпеки та цивільного захисту і визначає напрями державної політики щодо гарантування захищеності життєво важливих для держави, суспільства та особи інтересів, прав і свобод людини і громадянина, цілі та очікувані результати їх досягнення з урахуванням актуальних загроз.

Стратегія кібербезпеки України – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Стратегія національної безпеки України – документ, що визначає актуальні загрози національній безпеці України та відповідні цілі, завдання, механізми захисту національних інтересів України та є основою для планування й реалізації державної політики у сфері національної безпеки.

Система управління інформаційною безпекою – складна, створена для збору, аналізу і переробки інформації з метою отримання максимального кінцевого результату при певних обмеженнях (політичний імідж, економічна та військова могутність тощо).

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ ТА ІНТЕРНЕТ-РЕСУРСІВ

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.