

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

навчальної дисципліни вільного вибору

Управління інформаційною безпекою

Підготовки бакалавра

спеціальності 029 Інформаційна, бібліотечна та архівна справа

освітньо-професійної програми Документаційне забезпечення управління та інформаційно-аналітична діяльність


Луцьк – 2020

Силабус навчальної дисципліни «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ» підготовки бакалавра, галузі знань 02 Культура і мистецтво, спеціальності 029 Інформаційна, бібліотечна та архівна справа, за освітньо-професійною програмою Документаційне забезпечення управління та інформаційно-аналітична діяльність.

Розробник: Качковська Леся Ростиславівна, кандидат історичних наук

Силабус навчальної дисципліни затверджено на засіданні кафедри музеєзнавства, пам'яткознавства та інформаційно-аналітичної діяльності

протокол № 6 від 23 грудня 2020 р.

Завідувач кафедри:  (Гаврилук С. В.)

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

СИЛАБУС

I. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітня програма, освітній рівень	Характеристика навчальної дисципліни
Денна форма навчання	02 Культура і мистецтво	Вибіркова
Кількість годин / кредитів __180__/_6_	029 Інформаційна, бібліотечна та архівна справа ОП «Документаційне забезпечення управління та інформаційно-аналітична діяльність»	Рік навчання <u>2</u>
		Семестр <u>4-ий</u>
ІНДЗ: <u>є / немає</u>	на базі молодшого спеціаліста НП 2020 бакалавр	Лекції <u>30</u> год.
		Практичні (семінарські) <u>30</u> год.
		Самостійна робота <u>110</u> год.
		Консультації <u>10</u> год.
		Форма контролю: залік
Мова навчання	українська	

II. Інформація про викладача

Качковська Леся Ростиславівна
кандидат історичних наук
доцент
Контактна інформація (+38 050 2390883; kachkovska.lesja@vnu.edu.ua)
Дні занять (<http://194.44.187.20/cgi-bin/timetable.cgi?n=700>)

III. Опис дисципліни

Анотація курсу. В умовах посилення зовнішніх загроз і небезпек, що спостерігається в Україні, особливої актуальності набувають питання інформаційної безпеки. Навчальний курс спрямований на ознайомлення студентів з поняттями та визначеннями в галузі інформаційної безпеки. Висвітлено правові, організаційні аспекти забезпечення інформаційної безпеки, що має стати стратегічною основою державної політики України. Розглянуто питання інформаційної безпеки у різних сферах життя суспільства. Силабус складено відповідно до навчального плану підготовки бакалавра освітньо-професійної програми «Документаційне забезпечення управління та

інформаційно-аналітична діяльність» спеціальності 029 «Інформаційна, бібліотечна та архівна справа» та Стандарту вищої освіти за спеціальністю 029 «Інформаційна, бібліотечна та архівна справа», затвердженого 12.12.2018 р.

Зміст курсу: Поняття та зміст інформаційної безпеки. Державна політика в інформаційній сфері. Поняття та зміст загроз інформаційній безпеці. Адміністративно-правовий захист інформаційної безпеки України. Організаційна структура інформаційної безпеки. Система забезпечення інформаційної безпеки. Адаптація міжнародних стандартів Україною у сфері інформаційної безпеки.

Постреквізити: Кваліфікаційна робота.

Мета курсу: набуття знань з основ сучасної 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 в Україні шляхом створення ґрунтовної нормативно-правової бази у галузі інформаційної безпеки.

Завдання курсу:

- ознайомити з основними концепціями забезпечення інформаційної безпеки України;
- надати базові знання про зміст і значення інформації як об'єкта захисту;
- визначити та охарактеризувати види загроз та методи несанкціонованого доступу;
- сформувані вміння та навички щодо аналізу державної політики та критеріїв адаптації стандартів Європи у сфері інформаційної політики до України.

Перелік компетентностей та очікуваних результатів

Інтегральна компетентність	Здатність розв'язувати у процесі навчання спеціальні завдання у сфері інформаційної діяльності
Загальні компетентності	ЗК 7. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел. ЗК 8. Здатність оцінювати та забезпечувати якість виконуваних робіт.
Спеціальні компетентності	ФК 1. Здатність здійснювати відбір, аналіз, оцінку, систематизацію, моніторинг, організацію, зберігання, розповсюдження та надання в користування інформації та знань у будь-яких форматах. ФК2. Здатність використовувати методи систематизації, пошуку, збереження, класифікації інформації для різних типів контенту та носіїв. ФК14. Здатність до подальшого навчання з високим рівнем автономності, постійного підвищення рівня інформаційної культури.
Програмні результати навчання	РН5. Узагальнювати, аналізувати і синтезувати інформацію в діяльності, пов'язаній із її пошуком, накопиченням, зберіганням та використанням. РН7. Забезпечувати ефективність функціонування документнокомунікаційних систем. РН17. Бути відповідальним, забезпечувати ефективну співпрацю в команді. РН18. Навчатися з метою поглиблення набутих та здобуття нових фахових знань. РН19. Дотримуватися і реалізовувати основні засади охорони праці та безпеки життєдіяльності.

Структура навчальної дисципліни

Назви змістових модулів і тем	Усього	Лек.	Практ.	Сам. роб.	Конс.	*Форма контролю / Бали
Змістовий модуль 1. Концептуальні основи забезпечення інформаційної безпеки						
Тема 1. Вступ до навчального курсу. Інформаційна безпека та її місце в системі національної безпеки	11	2	2	7		Обговорення / 3
Тема 2. Інформація як об'єкт захисту	11	2	2	7		Обговорення / 3
Тема 3. Загрози інформації. Методи та види несанкціонованого доступу	12	2	2	7	1	Обговорення / 3
Тема 4. Модель порушника. Підготовчі дії порушника перед несанкціонованим доступом до інформації	13	2	2	8	1	Обговорення / 3
Тема 5. Основні засади державної політики України в галузі інформаційної безпеки	12	2	2	7	1	Обговорення / 3
Тестування за темами модулю 1						30
Разом за модулем 1	59	10	10	36	3	Поточне – 15 Модуль - 30
Змістовий модуль 2. Основи адміністративно-правового захисту інформаційної безпеки України. Організація структури інформаційної безпеки						
Тема 6. Правове регулювання інформаційної безпеки	12	2	2	7	1	Обговорення / 3
Тема 7. Роль та значення правового регулювання інформаційної безпеки	11	2	2	7		Обговорення / 2
Тема 8. Особливості реалізації адміністративно-правових форм та методів у сфері забезпечення інформаційної безпеки	12	2	2	7	1	Обговорення / 3
Тема 9. Органи забезпечення інформаційної безпеки та захисту інформації	12	2	2	7	1	Обговорення / 3
Тема 10. Напрями державної політики щодо сфери інформаційної безпеки	14	2	2	10		Обговорення / 2
Тема 11. Особливості інформаційної безпеки у різних сферах життя суспільства	12	2	2	7	1	Обговорення / 3
Тема 12. Ідентифікація. Автентифікація. Санкціонований доступ.	12	2	2	7	1	Обговорення / 3

Тема 13. Інформаційна безпека підприємств та організацій	12	2	2	7	1	Обговорення / 2
Тема 14. Системи інформаційної безпеки	11	2	2	7		Обговорення / 2
Тема 15. Механізми стратегічного інформаційного протиборства. Міжнародні аспекти інформаційної безпеки в умовах глобалізації.	12	2	2	8	1	Обговорення / 2
Тестування за темами модулю 2						30
Разом за модулем 2	121	20	20	74	7	Поточне – 25 Модуль - 30
Види підсумкових робіт (за потреби, на розсуд викладача, кафедри)						Бал
Модульна контрольна робота						60
ІНДЗ						-
Інше (вказати)						-
Всього годин / Балів	180	30	30	110	10	

Завдання для самостійного опрацювання.

1. Здійсніть порівняльний аналіз визначення «інформаційна безпека». Визначте об'єкт, суб'єкт, принципи та рівні інформаційної безпеки.
2. Розкрийте співвідношення понять «безпека інформації», «інформаційна безпека», «безпека інформаційної сфери».
3. Охарактеризуйте правовий статус інформаційної сфери в Україні.
4. Проаналізуйте систему правопорушень в інформаційній сфері.
5. Визначте джерела загроз інформаційній безпеці особи суспільства, держави.
6. Виділіть консультативно-дорадчі органи забезпечення інформаційної безпеки в Україні.
7. Визначте роль ЗМІ для забезпечення інформаційної безпеки в Україні.
8. Наведіть приклади маніпулювання через ЗМІ.
9. Прокоментуйте маніпулятивні технології на міжособистісному рівні.
10. Назвіть структуру загальнодержавної системи забезпечення інформаційної безпеки в Україні.
11. Охарактеризуйте основні реальні та потенційні загрози інформаційній безпеці в Україні.
12. Проаналізуйте основні поняття психологічного захисту.

IV. Політика оцінювання

Політика викладача щодо здобувача вищої освіти: всі здобувачі вищої освіти відвідують практичні заняття. Матеріал пропущених занять перевіряється шляхом індивідуальної бесіди або письмової відповіді.

Політика щодо академічної доброчесності. Здобувачі вищої освіти ознайомлюються з основними вимогами академічної доброчесності. Вони мають самостійно виконувати всі завдання, покликаючись на використані джерела.

Політика щодо дедлайнів та перескладання. Всі завдання мають бути виконані відповідно до розкладу навчального процесу. У випадку невчасного виконання завдань, здобувач вищої освіти може індивідуально здати матеріал певних тем, виконати індивідуальні завдання, написати модульні контрольні роботи та ін. Окремі теми, змістовий модуль чи курс можуть бути перезараховані здобувачу вищої освіти відповідно до «Положення про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

Шкала оцінювання (національна та ECTS)

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсної роботи (проекту), практики	для заліку
90 – 100	A	Відмінно	Зараховано
82 – 89	B	Добре	
75 - 81	C		
67 -74	D		
60 - 66	E	Задовільно	Незараховано (з можливістю повторного складання)
1 – 59	Fx	Незадовільно	

РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Поточний контроль (мах - 40 балів)		Модульний контроль (мах - 60 балів)		Загальна кількість балів
Модуль 1		Модуль 2		
Змістовий модуль 1	Змістовий модуль 2	МКР 1	МКР 2	
15 загальна к-сть балів	25 загальна к-сть балів	30	30	100

Критерії оцінювання навчальних досягнень студентів на практичних заняттях:

Рівні навчальних досягнень	Критерії оцінювання
Початковий (понятійний)	Студент володіє навчальним матеріалом на рівні засвоєння окремих термінів, фактів без зв'язку між ними; відповідає на запитання, які потребують відповіді «так» чи «ні»
	Студент мало усвідомлює мету навчально-пізнавальної діяльності, робить спробу знайти способи дій, розповісти суть заданого, проте відповідає лише за допомогою викладача на рівні «так» чи «ні», може самостійно знайти в підручнику відповідь
	Студент намагається аналізувати на основі побутових знань і навичок; виявляє окремі властивості, спроби виконання вправ, дій репродуктивного характеру, за допомогою викладача робить прості розрахунки за готовим алгоритмом
Середній (репродуктивний)	Студент володіє початковими знаннями, знає близько половини навчального матеріалу, здатний відтворити його відповідно до тексту підручника або пояснень викладача, провести за зразком економічні розрахунки; слабо орієнтується у поняттях, визначеннях, самостійне опрацювання навчального матеріалу викликає значні труднощі
	Студент знає більше половини навчального матеріалу, розуміє сутність предмету, може дати визначення понять, категорій, однак із помилками, впевнено працювати з підручником, самостійно оволодіти частиною навчального матеріалу; робить прості розрахунки за алгоритмом, але висновки не логічні, не послідовні
	Студент розуміє основні положення навчального матеріалу, може поверхово аналізувати події, ситуації, робить певні висновки; відповідь може бути правильною, проте недостатньо осмисленою, самостійно відтворює більшу частину матеріалу; вміє застосовувати знання під час розв'язування завдань за алгоритмом, користуватися додатковими джерелами
Достатній (алгоритмічно-дієвий)	Студент правильно і логічно відтворює навчальний матеріал, розуміє основоположні теорії і факти, встановлює причинно-наслідкові зв'язки між ними, вміє наводити свої власні приклади на підтвердження певних думок, застосовувати теоретичні знання у стандартних ситуаціях; за допомогою викладача може скласти план реферату, виконати його і правильно оформити, самостійно користуватися додатковими джерелами, правильно використовувати термінологію, скласти прості таблиці, схеми
	Знання студента досить повні, він вільно застосовує вивчений матеріал у стандартних ситуаціях, логічно висвітлює суспільні події в державі і за рубежом, вміє аналізувати, робити висновки; відповідь його повна, логічна, обґрунтована, однак із деякими неточностями; вміє самостійно працювати, може підготувати реферат і захистити його положення
	Студент вільно володіє вивченим матеріалом, застосовує набуті знання у дещо змінених

	ситуаціях, вміє аналізувати і систематизувати інформацію, робить аналітичні висновки, використовує загальновідомі докази у власній аргументації, чітко тлумачить поняття, формулювання законів, нормативних документів, може самостійно опрацювати матеріал, виконує прості творчі завдання; має сформовані типові навички
Високий (творчий професійний)	Студент володіє глибокими і міцними знаннями та використовує їх у нестандартних умовах, ситуаціях; може визначати тенденції та суперечності процесів; робить аргументовані висновки, практично оцінює окремі нові факти, явища, процеси, самостійно визначає мету власної діяльності; розв'язує творчі завдання, може сприймати іншу позицію як альтернативну, знає суміжні дисципліни, використовує знання, аналізуючи політичні явища
	Студент володіє узагальненими знаннями з предмету, аргументовано використовує їх у нестандартних ситуаціях, уміє знаходити джерела інформації та аналізувати їх, ставити і розв'язувати проблеми, застосовувати вивчений матеріал для власних аргументованих суджень у практичній діяльності (диспути, дискусії, круглі столи), спроможний за допомогою викладача підготувати виступ на студентську наукову конференцію, самостійно вивчити матеріал, визначити програму своєї пізнавальної діяльності, знаходити інформацію в газетах, журналах, публікаціях, Інтернеті, мультимедійних програмах тощо, оцінювати явища в суспільстві, виявляє свою життєву позицію
	Студент має системні, дієві знання, виявляє неординарні творчі здібності у навчальній діяльності, використовує широкий арсенал засобів доказів своєї думки, розв'язує складні проблемні завдання, схильний до системно-наукового аналізу та прогнозу явищ; уміє ставити і розв'язувати проблеми, самостійно здобувати і використовувати інформацію, виявляє власне ставлення до неї, виконує науково-дослідну роботу, логічно та творчо викладає матеріал в усній та письмовій формі; розвиває свої здібності й нахили; використовує Інтернет, моделює ситуації в нестандартних умовах

V. Підсумковий контроль

Підсумковий контроль поводить у формі заліку з навчальної дисципліни. Оцінка за залік ставиться на основі балів, набраних за час вивчення курсу. За перший і другий змістові модулі здобувачі вищої освіти отримують 15 і 25 балів.

За результатами модульної контрольної роботи студент може набрати до 60 балів. Якщо здобувач вищої освіти хоче підвищити рейтинг, він може добрати бали, виконавши певний вид робіт (наприклад, здати пропущені теми, або перездати якусь тему, написати тести по темах, підготувати індивідуальні завдання).

Орієнтований перелік питань

1. Інформаційна безпека та її місце в системі національної безпеки
2. Інформація як об'єкт захисту
3. Властивості інформації. Її види
4. Поняття та складов інформаційної безпеки
5. Відповідальність за порушення законодавства України про інформацію
6. Загрози інформації
7. Види дестабілізуючих факторів
8. Методи та види несанкціонованого доступу
9. Модель порушника
10. Підготовчі дії порушника перед несанкціонованим доступом до інформації
11. Основні засади державної політики України в галузі інформаційної безпеки
12. Правове регулювання інформаційної безпеки
13. Роль та значення правового регулювання інформаційної безпеки
14. Особливості реалізації адміністративно-правових форм та методів у сфері забезпечення інформаційної безпеки
15. Органи забезпечення інформаційної безпеки та захисту інформації
16. Напрями державної політики щодо сфери інформаційної безпеки

17. Особливості інформаційної безпеки у різних сферах життя суспільства
18. Інформаційна безпека підприємств та організацій
19. Системи інформаційної безпеки
20. Механізми стратегічного інформаційного протиборства.
21. Міжнародні аспекти інформаційної безпеки в умовах глобалізації.

Тестові завдання:

Під інформацією розуміємо:

- a) задокументовані або оприлюднені відомості про події та явища, які відбуваються у суспільстві, державі чи навколишньому середовищі;
- b) органи влади, що регулюють відносини в галузі інформаційної безпеки та захисту інформації;
- c) захист відомостей, що становлять державну таємницю;
- d) те, що придумане людиною й у природі в готовому виді не зустрічається. Їх потрібно створювати, виробляти, а значить, витрачати час, докладати зусилля, тобто застосовувати певні ресурси.

Інформація як правова категорія має такі особливості:

- a) нематеріальність;
- b) матеріальність;
- c) невичерпність;
- d) безмежність;
- e) збережуваність;
- f) нестабільність;
- g) частковість.

Властивості інформації:

- a) конфіденційність;
- b) цілісність;
- c) нестабільність;
- d) доступність;
- e) публічність;
- f) масовість;
- g) непорушність.

Режим доступу до інформації передбачає:

- a) наявність відомостей, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними норм;
- b) наявність правових норм, порядок отримання, використання, розповсюдження та зберігання інформації;
- c) наявність доступу відомостей, які містяться на матеріальному носіїві або передані усно.
- d) державний орган, який призначений для забезпечення функціонування й розвитку державної системи урядового зв'язку.

Доступ до відкритої інформації забезпечують шляхом:

- a) систематичної публікації її в офіційних друкованих виданнях, бюлетенях, збірниках;
- b) оприлюднення відомостей, що становлять державну таємницю;
- c) надання допуску до таємної інформації посадовим особам;
- d) поширення її засобами масової інформації;
- e) надання грифів обмеження доступу, призначених для державної таємниці;
- f) безпосередньо надання інформації зацікавленим громадянам, державним органам чи юридичним особам.

Адміністративно-правова діяльність України в сфері забезпечення інформаційної безпеки є активною категорією правового життя, завданням якої є:

- a) гарантоване право на інформацію;
- b) забезпечення наявності відносин, тобто самого об'єкта охорони;
- c) достовірність і повнота інформації;
- d) заборона дискримінації.

Усі загрози інформації можна об'єднати у три групи:

- a) загроза розкриття;
- b) загроза викриття;

- c) загроза цілісності;
- d) загроза відмови в обслуговуванні;
- e) загроза замовчування дії;
- f) загроза накопичення даних.

Причинами загроз інформації можуть бути:

- a) навмисні та природні фактори;
- b) об'єктивні та суб'єктивні причини;
- c) особисті та мотиваційні підстави;
- d) отримання прибутку легальним шляхом.

Основний комплекс загроз і небезпек інформаційної сфери:

- a) наявність суб'єктів та їх вольових дій з метою створення перешкод для функціонування інформаційних і телекомунікаційних мереж у державі;
- b) наявність відкритості та доступності інформації;
- c) створення відкритого інформаційного простору;
- d) наявність нормативно-правової бази у сфері інформаційного захисту.

До навмисних факторів загроз інформації належать:

- a) стихійні лиха;
- b) розкрадання носіїв інформації;
- c) підключення до каналів зв'язку;
- d) збої апаратури;
- e) нещасні випадки;
- f) несанкціонований доступ;
- g) розголошення та копіювання інформації;
- h) наявність соціальних обставин.

Дестабілізуючими факторами являються:

- a) явища чи події, що можуть з'являтися на будь-якому етапі життєвого циклу інформаційної системи, і наслідком яких можуть загрози інформації;
- b) відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними норм;
- c) власники інформаційних ресурсів, які мають раво здійснювати контроль за виконання вимог із захисту інформації;
- d) демократичний цивільний контроль над військовою організацією держави та іншими структурами в системі національної безпеки.

Порушник – це:

- a) людина, яка дбає про свою безпеку і застосовує мирні заходи для її забезпечення;
- b) людина, яка має намір допомогти іншій людині;
- c) людина, яка чинить несвідомі шкідливі (помилкові) дії;
- d) людина, яка чинить свідомі (злочинні) дії.

Зловмисник – це:

- a) людина, яка чинить свідомі (злочинні) дії;
- b) людина, яка дбає про свою безпеку і застосовує мирні заходи для її забезпечення;
- c) людина, яка має намір допомогти іншій людині;
- d) людина, яка чинить несвідомі шкідливі (помилкові) дії;

Основна відмінність хакера від кракера:

- a) кракер вирішує дослідницьку задачу з оцінювання та знаходження слабких місць із метою подальшого підвищення надійності роботи та безпеки інформаційної системи;
- b) хакер вирішує дослідницьку задачу з оцінювання та знаходження слабких місць із метою подальшого підвищення надійності роботи та безпеки інформаційної системи;
- c) кракер виконує вторгнення в систему з метою руйнування, крадіжки, псування, змінювання інформації та вчиняє правопорушення з корисливими намірами швидкого збагачення;
- d) хакер виконує вторгнення в систему з метою руйнування, крадіжки, псування, змінювання інформації та вчиняє правопорушення з корисливими намірами швидкого збагачення.

Основні мотиви порушень:

- a) безвідповідальність;
- b) самоствердження;
- c) творчий задум;
- d) публічний виступ;

- e) підкуп;
- f) відповідальність;
- g) патріотичність;
- h) ідеологічні мотиви;
- i) шантаж.

Перед здійсненням несанкціонованого доступу до ресурсів інформаційної системи порушнику потрібно, як правило, здійснити підготовчі дії:

- a) зібрати відомості про інформаційну систему;
- b) зареєструватися як ФОП;
- c) стати громадянином держави;
- d) виконати потрібні спроби входження до інформаційної системи;
- e) офіційно бути працевлаштованим.

В галузі інформаційної безпеки важливим є:

- a) публічність інформаційних об'єктів у всіх сферах діяльності людини;
- b) ухилення від адміністративної відповідальності;
- c) сформованість певної законодавчої бази, яка частково забезпечує захист на інформацію;
- d) розробка механізмів генерації нових рішень, що дозволяють адекватно реагувати на погрози інформаційної безпеки або передбачати нові погрози та вміти їм протистояти.

Положення «Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів» прописане у:

- a) Конституції України;
- b) ЗУ «Про інформацію»;
- c) ЗУ «Про основи національної безпеки України»;
- d) ЗУ «Про національну програму інформатизації».

Інформаційна безпека – це

- a) відкритість, доступність інформації, свобода обміну інформацією;
- b) достовірність і повнота інформації;
- c) стан захищеності важливих інтересів людини, суспільства і держави, за якою запобігається нанесення шкоди;
- d) запобігання розповсюдження відомостей, що становлять державну таємницю.

Основні принципи інформаційних відносин:

- a) неповнота, невчасність та невірогідність інформації, що використовується;
- e) гарантованість права на інформацію, відкритість, доступність інформації, свобода обміну інформацією, захищеність особи від втручання в її особисте та сімейне життя, достовірність і повнота інформації;
- b) мирне вирішення міжнародних конфліктів, повага прав людини, суверенна рівність, матеріальний добробут;
- c) територіальна цілісність, непорушність кордонів держав;
- d) рівноправність і самовизначення народів, міжнародне співробітництво.

Шкодою інформаційній безпеці являється:

- a) неповнота, невчасність та невірогідність інформації, що використовується;
- b) запобігання розповсюдження відомостей, що становлять державну таємницю;
- c) правовий захист інформаційної сфери;
- d) негативний інформаційний вплив та негативні наслідки застосування інформаційних технологій;
- e) захист політичних, державних і громадських інтересів країни;
- f) несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Який законодавчий документ чітко визначає, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу:

- a) Конституції України;
- b) ЗУ «Про інформацію»;
- c) ЗУ «Про основи національної безпеки України»;
- d) ЗУ «Про національну програму інформатизації».
- e) Про Концепцію Національної програми інформатизації.

Об'єктами національної безпеки є:

- a) людина, громадянин, держава;
- b) юридична особа, фізична особа, державна установа;
- c) дитина, батьки, державні службовці;
- d) Президент України, Верховна Рада України, Кабінет Міністрів України.

До суб'єктів інформаційної безпеки належать:

- a) Президент України, Верховна Рада України, Кабінет Міністрів України; Рада національної безпеки і оборони України, міністерства та інші органи виконавчої влади та органи місцевого самоврядування;
- b) Міністерство освіти і науки України, Міністерствокультури України; об'єднані територіальні громади;
- c) фізичні особи підприємці, науково-педагогічні працівники; школярі, студенти.
- d) люди пенсійного віку.

Нормативно-правовою основою правового регулювання державного управління інформаційною сферою є:

- a) галузь цивільного права;
- b) галузь кримінального права;
- c) галузь адміністративного права;
- d) галузь сімейного права.

Нині в нашій державі управління інформаційною сферою здійснює 5 основних органів державної влади:

- a) Національна рада України з питань телебачення і радіомовлення, Національна комісія регулювання у сфері зв'язку та інформатизації, Державний комітет з телебачення і радіомовлення України, Держінформнауки України, Державна служба спеціального зв'язку та захисту інформації України;
- b) Національний банк України, Державна фінансова інспекція України, Департамент політики міжбюджетних відносин та місцевих бюджетів, Управління міжнародного співробітництва, Фонд розвитку інновацій;
- c) Департамент фінансової політики, Департамент прогнозування доходів бюджету, Державна іпотечна установа, НЕК «Укренерго», Державна митна служба України;
- d) Міністерство цифрової трансформації України, Директорат розвитку електронних послуг, Директорат розвитку Національної програми інформатизації, Директорат розвитку цифрових інструментів протидії корупції, Директорат електронних реєстрів.

Загалом розвиток законодавчої бази в галузі інформаційної безпеки йде за чотирма основними напрямками:

- a) захист відомостей, що становлять державну таємницю;
- b) захист конфіденційної інформації;
- c) розповсюдження рекламних відомостей;
- d) захист авторського права в сфері інформатизації;
- e) відкритий доступ до публічної інформації;
- f) захист прав на доступ до інформації;
- g) оприлюднення інформації про події і явища в світі;
- h) охорона особистих майнових прав.

До державної системи інформаційної безпеки й захисту інформації входять:

- a) органи законодавчої, виконавчої й судової влади;
- b) матеріальні блага громадян України;
- c) законодавство, що регулює відносини в галузі інформаційної безпеки, захисту інформації та інформаційних ресурсів;
- d) правове забезпечення громадського порядку;
- e) захист авторського права у сфері виробництва;
- f) нормативно-правова база із захисту інформації;
- g) служби (органи) захисту інформації підприємств, організацій, установ;
- h) охорона навколишнього середовища;
- i) незаконне ввезення піратської продукції.

До повноважень Служби безпеки України у сфері захисту інформації визначено:

- a) це державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України і підпорядкований Президенту України, виконує безпосередньо функції захисту державної таємниці.
- b) це державний орган, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку;
- c) це державний орган, який веде боротьбу з правопорушниками;
- d) це державний орган, який здійснює нагляд за виконанням законодавства України.

Категорії методів захисту від несанкціонованого доступу:

- a) хвильові, польові, звукові, інформаційні;
- b) правові, організаційні, технологічні, фізичні, апаратні, програмні;
- c) неофіційні, матеріальні, природні, громадські;
- d) імітація роботи, знищення інформації, змінювання алгоритмів завдань, перегляд інформації.

VI. Шкала оцінювання

Оцінка в балах за всівидинавчальної діяльності	Оцінка
90 – 100	Відмінно
82 – 89	Дуже добре
75 - 81	Добре
67 -74	Задовільно
60 - 66	Достатньо
1 – 59	Незадовільно

VI. Рекомендована література та інтернет-ресурси

Основна:

1. Бобало Ю. А., Горбатий І. В., Кіселичник М. Д., Бондарев А. П. Інформаційна безпека : навчальний посібник. Львів : Вид-во Львівської політехніки, 2019. 580 с.
2. Лісовська Ю. П. Інформаційна безпека України : навчальний посібник. К. : Видавничий дім «Кондор», 2018. 172 с.

Додаткова:

1. ДК 010-98. Державний класифікатор управлінської документації. [Чинний від 1999-06-01]. К. : Держстандарт України, 1999. 50 с. URL : <https://zakon.rada.gov.ua/rada/show/v1024217-98#Text>
2. ДСТУ 2732:2004. Діловодство й архівна справа. Терміни та визначення понять. [Чинний від 2004-05-29]. К. : Держспоживстандарт України, 2005. 36 с. URL : [https://vn.court.gov.ua/userfiles/27_2732-2004\(1\).pdf](https://vn.court.gov.ua/userfiles/27_2732-2004(1).pdf)
3. ДСТУ 3843-99. Державна уніфікована система документації. Основні положення. [Чинний від 1999-09-29]. К. : Держстандарт України, 2000. 7 с.
4. ДСТУ 3844-99. Державна уніфікована система документації. Формуляр-зразок. Вимоги до побудови. [Чинний від 2000-07-01]. К. : Держстандарт України, 2000. 8 с.
5. ДСТУ 4163-2003. Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів. [Чинний від 2003-09-01]. К. : Держспоживстандарт України, 2003. – 26 с. URL : http://www.vru.gov.ua/content/file/Doc_007.pdf
6. Підсумкові документи Всесвітнього саміту з питань інформаційного суспільства. URL : <http://apitu.org.ua/wsis> (дата звернення: 18.12.2019).
7. План заходів з реалізації Стратегії реформування державного управління України на 2016–2017 роки. URL : <http://www.kmu.gov.ua/document/249175747/R0474.doc> (дата звернення: 18.12.2019).
8. Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 р. № 505/98. *Офіційний вісник України*. 1998. № 21. С. 759. URL : <https://zakon.rada.gov.ua/laws/show/505/98#Text>

9. Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229. *Офіційний вісник України*. 1999. № 39. С. 28. URL : <https://zakon.rada.gov.ua/laws/show/1229/99#Text>
10. Посібник з прав людини для Інтернет-користувачів та пояснювальний меморандум. К. : Інжиніринг, 2015. 56 с.
11. Про внесення змін до плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України № 1072-р від 25.12.2013 р. *Урядовий кур'єр*. 05.02.2014. № 22. С. 15.
12. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 03.11.2006 р. № 328-V. *Відомості Верховної Ради України*. 2006. № 51. С. 519. URL : <https://zakon.rada.gov.ua/laws/show/3475-15#Text>
13. Про державну таємницю: Закон України від 21.01.1994 № 3856-XII. *Відомості Верховної Ради України*. 1994. № 16. URL : <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
14. Про доступ до публічної інформації : Закон України від 13.04.2012 № 4652-VI. *Відомості Верховної Ради України*. 2013. № 21. С. 208. URL : <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
15. Про електронні документи та електронний документообіг: Закон України від 05.10.2017 № 2155-VIII. *Відомості Верховної Ради України*. 2017. № 45. С. 400. URL : <https://zakon.rada.gov.ua/laws/show/851-15#Text>
16. Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації : Постанова Кабінету Міністрів України від 14.04.1997 р. № 348. URL : <https://zakon.rada.gov.ua/laws/show/348-97-%D0%BF#Text>
17. Про затвердження Класифікатора звернень громадян : Постанова Кабінету Міністрів України від 24.09.2008 р. № 858. URL : <https://zakon.rada.gov.ua/laws/show/858-2008-%D0%BF#Text>
18. Про затвердження плану дій із впровадження Ініціативи «Партнерство «Відкритий Уряд» у 2014–2015 роках : Розпорядження Кабінету Міністрів України від 26 листопада 2014 р. № 1176-р. Режим доступу : <http://zakon2.rada.gov.ua/laws/show/1176-2014-%D1%80> (дата звернення: 16.12.2019).
19. Про затвердження плану заходів з виконання завдань, передбачених Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» : Розпорядження Кабінету Міністрів України від 15.08.2007 р. № 653-р. URL : <http://zakon1.rada.gov.ua/laws/show/653-2007-%D1%80> (дата звернення: 16.12.2019).
20. Про затвердження плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 26.09.2011 р. № 1014-р. *Урядовий кур'єр*. 28.10.2011. № 200. С. 18.
21. Про затвердження Положення про Державне агентство з питань електронного урядування України : Постанова Кабінету Міністрів України від 1 жовтня 2014 р. № 492. URL : <http://zakon3.rada.gov.ua/laws/show/492-2014-%D0%BF> (дата звернення: 16.12.2019).
22. Про затвердження Положення про формування та виконання Національної програми інформатизації : Постанова Кабінету Міністрів України від 31.08.1998 № 1352. URL : <http://zakon5.rada.gov.ua/laws/show/1352-98-%D0%BF> (дата звернення: 03.12.2019).
23. Про затвердження Порядку формування та виконання галузевої програми і проекту інформатизації : Постанова Кабінету Міністрів України від 18.12.2001 р. № 1702.

- URL : <http://zakon3.rada.gov.ua/laws/show/1702-2001-%D0%BF> (дата звернення: 16.12.2019).
24. Про затвердження Порядку формування та виконання регіональної програми і проекту інформатизації: Постанова Кабінету Міністрів України від 12.04.2000 р. № 644. URL : <http://zakon2.rada.gov.ua/laws/show/644-2000-%D0%BF> (дата звернення: 16.12.2019).
 25. Про затвердження Регламенту Кабінету Міністрів України : Постанова Кабінету Міністрів України від 18.07.2007 р. № 950. URL : <http://zakon2.rada.gov.ua/laws/show/ru/950-2007-%D0%BF> (дата звернення: 16.12.2019).
 26. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 81/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. С. 286. URL : <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
 27. Про звернення громадян: Закон України від 02.10.1996 № 394/96-ВР. *Відомості Верховної Ради України*. 1996. № 47. С. 256. URL : <https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text>
 28. Про інформацію: Закон України від 02.10.1992 р. № 2657-ХІІ. URL : <http://zakon4.rada.gov.ua/laws/show/2657-12> (дата звернення: 16.10.2019).
 29. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. №75/98-ВР. *Відомості Верховної Ради України*. 1998. № 27–28. С. 181–182.
 30. Про ліцензування видів господарської діяльності: Закон України від 02.07.2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40-41. С. 379. URL : <https://zakon.rada.gov.ua/laws/show/222-19#Text>
 31. Про Національну систему конфіденційного зв'язку: Закон України від 18.11.2003 р. № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. С. 155. URL : <https://zakon.rada.gov.ua/laws/show/2919-14#Text>
 32. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09.01.2007 р. № 537-V. *Відомості Верховної Ради України*. 2007. № 12. С. 102.
 33. Про Програму діяльності Кабінету Міністрів України : Постанова Верховної Ради України від 14.04.2016 р. № 1099-VIII. URL : <http://zakon2.rada.gov.ua/laws/show/1099-19> (дата звернення: 14.12.2019).
 34. Про рекламу: Закон України від 3.07.1996 р. № 271/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. С. 182. URL : <https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text>
 35. Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні : Постанова Верховної Ради України від 01.12.2005 р. № 3175-IV. URL : <http://zakon3.rada.gov.ua/laws/show/3175-15> (дата звернення: 14.12.2019).
 36. Про Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» : Постанова Верховна Рада України від 03.07.2014 р. № 1565-VII. *Відомості Верховної Ради*. 2014. № 33. С. 23–30.
 37. Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України»: Постанова Верховної Ради України від 31.03.2016 р. № 1073-VIII. *Відомості Верховної Ради України*. 2016. № 17. С. 38.
 38. Про Стратегію сталого розвитку «Україна–2020»: Указ Президента України від 12.01.2015 р. № 5/2015. *Офіційний вісник Президента України*. 20.01.2015. № 2. С. 14.

39. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 13.12.2010 р. № 2250-р. *Урядовий кур'єр*. 05.01.2011. №1. С. 26.
40. Про схвалення плану дій з впровадження в Україні Ініціативи «Партнерство «Відкритий Уряд» : Розпорядження Кабінету Міністрів України від 05.04.2012 р. № 220-р. *Урядовий кур'єр*. 2012. № 76. С.7.
41. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. *Урядовий кур'єр*. 13.06.2013. № 105. С. 26–27.
42. Про телекомунікації: Закон України від 24.06.2004 № 1876-IV. *Відомості Верховної Ради України*. 2004. № 48. С. 526. URL : <https://zakon.rada.gov.ua/laws/show/1280-15#Text>.
43. Титюк М., Качковська Л. Інформаційна безпека в системі електронного урядування. Молода наука Волині: пріоритети та перспективи досліджень: матер. XIV Міжнар. наук.-практ. конф. студ. і аспір. (Луцьк, 12–13 травня 2020 р.). Луцьк, 2020. С. 649–651. https://ra.eenu.edu.ua/wp-content/uploads/2020/05/Moloda-nauka-Volyni_2020_12-13travnnya.pdf.
44. Федорчук Р., Качковська Л. Реінжиніринг: актуальні питання практичної реалізації. Молода наука Волині: пріоритети та перспективи досліджень: матер. XIV Міжнар. наук.-практ. конф. студ. і аспір. (Луцьк, 12–13 травня 2020 р.). Луцьк, 2020. С. 653–655. https://ra.eenu.edu.ua/wp-content/uploads/2020/05/Moloda-nauka-Volyni_2020_12-13travnnya.pdf