ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Основи кібербезпеки

Лектор, к.т.н., доцент Лобанчикова Надія Миколаївна

2023-2024 навчальний рік

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Структура дисципліни:

Загальна кількість годин – 120 годин
Змістових модулів – 4 (4 модульні контрольні роботи)
Лекції – 32 годин (16 шт.)
Лабораторні роботи- 32 години (16 шт.)
Залік

Метою навчальної дисципліни є ознайомлення студентів з сутністю, задачами, принципами та сучасними інформаційними технологіями кібербезпеки та захисту інформації в інформаційно-телекомунікаційних системах, методологічними та законодавчими основами організації, планування та впровадження систем кібербезпеки та захисту інформації в інформаційних системах управління на підприємствах, а також основним аспектам практичної діяльності по їх створенню, забезпеченню функціонування та оцінці ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завданнями вивчення навчальної дисципліни є:

– оволодіння принципами побудови систем кіберзахисту;

– розуміння головних задач та сервісів кібербезпеки;

– оволодіння загальними теоретичними поняттями та основними нормативно-правовими документами у сфері кібербезпеки;

– отримання знань щодо основних складових інформаційної безпеки;

– отримання знань щодо існуючих моделей загроз та порушника, основних причин порушення безпеки;

– отримання знань щодо класифікації засобів кібербезпеки, організаційних та технічних заходів забезпечення кіберзахисту;

– оволодіння принципами захисту інформації від несанкціонованого доступу, методами аутентифікації та ідентифікації користувачів інформаційно-телекомунікаційних систем, методами контролю доступу;

– оволодіння теоретичними основами криптографічних та стеганографічних методів захисту інформації;

– оволодіння методами та засобами здійснення процедури оцінки ефективності систем кіберзахисту;

– оволодіння технологіями реалізації криптографічних алгоритмів захисту інформації;

– оволодіння методами розробки моделі загроз та моделі порушників інформаційної безпеки

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**:

Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання:

Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення з урахуванням основних засад кібербезпеки;

Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

Розробляти моделі загроз та порушника;

Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем

В межах ОК на освітньому порталі розміщено рейтинг лист, де детально можна ознайомитись з бали по кожному виду занять, поточному та підсумковому контролю: https://docs.google.com/spreadsheets/d/18VLwO02zhMzePvnLyxEwi9irqaAz2eWs/edit?usp=sharing&ouid=101536187150544780233&rtpof=true&sd=true

Посилання на курс: https://learn.ztu.edu.ua/course/view.php?id=4291&notifyeditingon=1

Шкала оцінювання

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

Лекція 1

Теоретичні основи та нормативно-правове забезпечення кіберзахисту

План лекції:

Вступ

1. **Дефініція поняття «Кіберпростір»**
2. **Дефініція поняття «Кібербезпека»**
3. **Дефініція поняття «Кіберборотьба»**
4. **Нормативно-правова база**

ВСТУП

Розвиток інформаційного суспільства призводить до розвитку нових інформаційних технологій та систем. Однак поряд з перевагами існують і недоліки. До негативних чинників слід віднести появу кіберзлочинності, що набирає обертів останнім часом за рахунок зростання попиту на користування інформаційно-телекомунікаційними системами та інформаційними технологіями.

Кібернетичні впливи стають ефективним інструментом щодо несилового контролю та управління об’єктами (в тому числі критичної інфраструктури), громадянами, колективами.

Протидія кібертероризму є пріоритетним завданням кожної високотехнологічної країни для забезпечення національної безпеки.

Кібербезпека - Світ експертів і злочинців

хакер - люди з хорошими навичками програмування (аматори, програмісти та студентів).

Там, де чарівники лягають спати пізно: витоки Інтернету (Where Wizards Stay up Late: The Origins of The Internet), яка опублікована у 1996 році, додали містики до хакерської культури. Культура хакерства постійно розвивається.

1. Дефініція поняття «Кіберпростір»

Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТ-систем (ІТС) і мережних технологій різного функціонального призначення, які в процесах обробки, передавання та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення (ПЗ) призвело, зрештою, до формування ***кіберпростору*** *[1].*

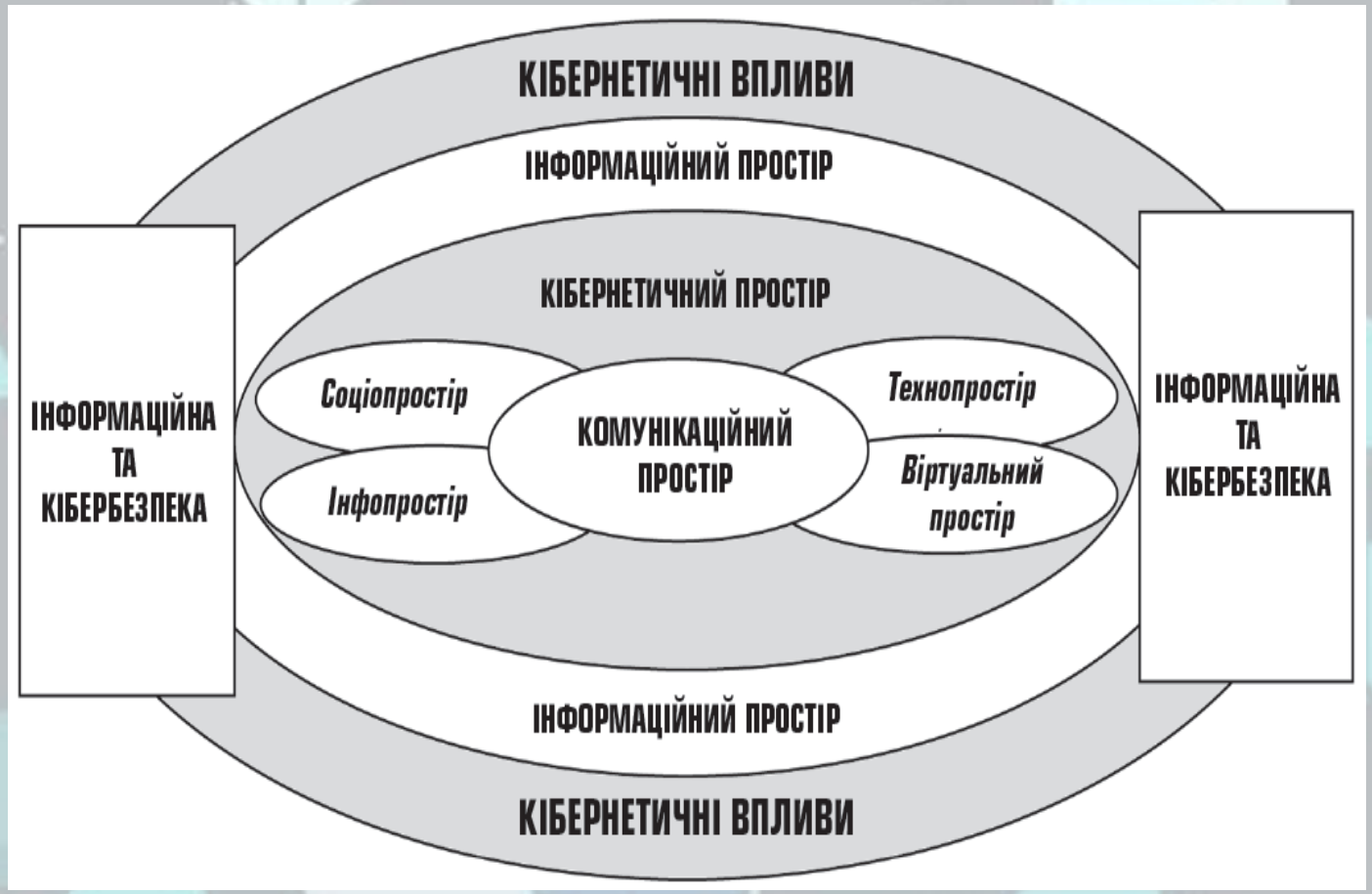

Рисунок 1 - Взаємозв’язок інформаційного та кіберпросторів

1) ***кіберпростір*** — це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі;
2) відповідно до нормативної бази США [1], ***кіберпростір*** — це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережні системи та пов'язану з ними фізичну інфраструктуру;
3) відповідно до офіційних документів Євросоюзу [1], ***кіберпростір*** — це віртуальний простір, в якому циркулюють електронні дані світових персональних комп'ютерів (ПК);
4) відповідно до офіційних документів Великобританії [1], ***кіберпростір*** — це всі форми мережної, цифрової активності, що включають у себе контент та дії, здійснювані через цифрові мережі;
5) відповідно до офіційних документів Німеччини [1], ***кіберпростір*** — це вся інформаційна інфраструктура, доступна через інтернет поза будь-якими територіальними кордонами.

Рисунок 2 - Дійові особи кіберпростору та їхній вплив на інформаційну і кібербезпеку

2. Дефініція поняття «Кібербезпека»

Кібербезпека – це захищеність від наявних та потенційно небезпечних проявів інформаційного впливу, що створюють небезпеку для функціонування інформаційних ресурсів, систем та мереж програмних та апаратних засобів, а а також свідомості, підсвідомості, морально-психологічного стану людини, соціальних груп та суспільства в цілому [2].

Кібербезпека – комплекс заходів, спрямованих на захист комп’ютерів, цифрових даних і мереж, їх передачі від несанкціонованого доступу та інших дій, пов’язаних з маніпулюванням або крадіжкою, блокуванням, пошкодженням (викривленням), руйнуванням та знищенням як випадкового, так і цілеспрямованого впливу.

Аналіз дефініцій поняття кібербезпеки за базовими критеріями

Походження дефініції чи її автори	Базовий критерій									
	Virt	HF	Soft	PhI	Net	INet	IServ	IRes	MSys	IPr
Стандарт ISO/IES 27032	+	+	+	+	+	+	+			
Нормативна база США				+	+			+		+
Офіційні документи ЄС	+							+		
Концепція кібербезпеки Великобританії					+			+		+
Законодавство Німеччини				+		+				
В. Харченко, О. Корченко та ін.	+									+
В. Бурячок	+		+	+	+			+		+
М. Погорецький, М. Шеломенцев				+	+		+	+	+	+
С. Мельник, О. Тихомиров					+			+		+
Д. Дубов, М. Ожеван								+	+	

Примітка. Для позначення базових критеріїв використано такі ідентифікатори [2]: **Virt** — критерій віртуальності; **HF** — критерій урахування людського чинника; **Soft** — критерій урахування ПЗ; **PhI** — критерій наявності фізичної інфраструктури; **Net** — критерій наявності мережної складової; **INet** — критерій урахування поняття «Інтернету»; **IServ** — критерій можливості надання інформаційних послуг; **IRes** — критерій урахування інформаційних ресурсів; **MSys** — критерій наявності системи управління; **IPr** — критерій урахування інформаційних процесів.

Рисунок 3 - Місце кібернетичної безпеки згідно зі стандартом ISO/IEC 27032:2012 (E)

Стандарт зосереджується на двох основних питаннях:

1) безпека в кіберпросторі, яка зосереджена на усуненні прогалин між різними доменами (сферами) безпеки. Зокрема, стандарт надає рекомендації щодо запобігання виникненню типових загроз кібербезпеки;

2) співробітництво. Необхідна ефективна та безпечна передача інформації в Кіберпросторі між зацікавленими сторонами, а також у координації діяльності та вирішенні випадків/інцидентів, якщо вони трапляються.

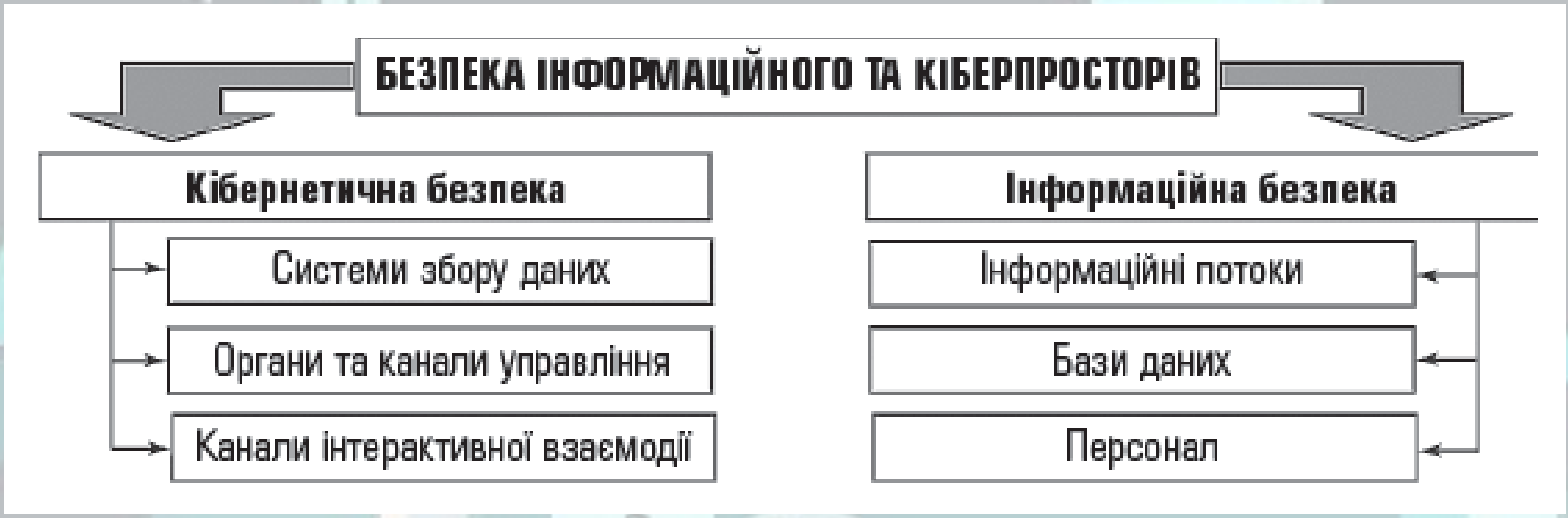

Рисунок 4 - Об’єкти впливу в інформаційному та кіберпросторі

Спектр інтересів ІБ щодо інформації, інформаційних систем та інформаційних технологій як об’єктів безпеки можна поділити на такі основні категорії: ***доступність*** — можливість за прийнятний час отримати певну інформаційну послугу; ***цілісність*** — актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованого змінювання; ***конфіденційність*** — захищеність від несанкціонованого ознайомлення

інформаційна безпека (ІБ) - *стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони*

Рисунок 5 - Структура поняття «інформаційна безпека»

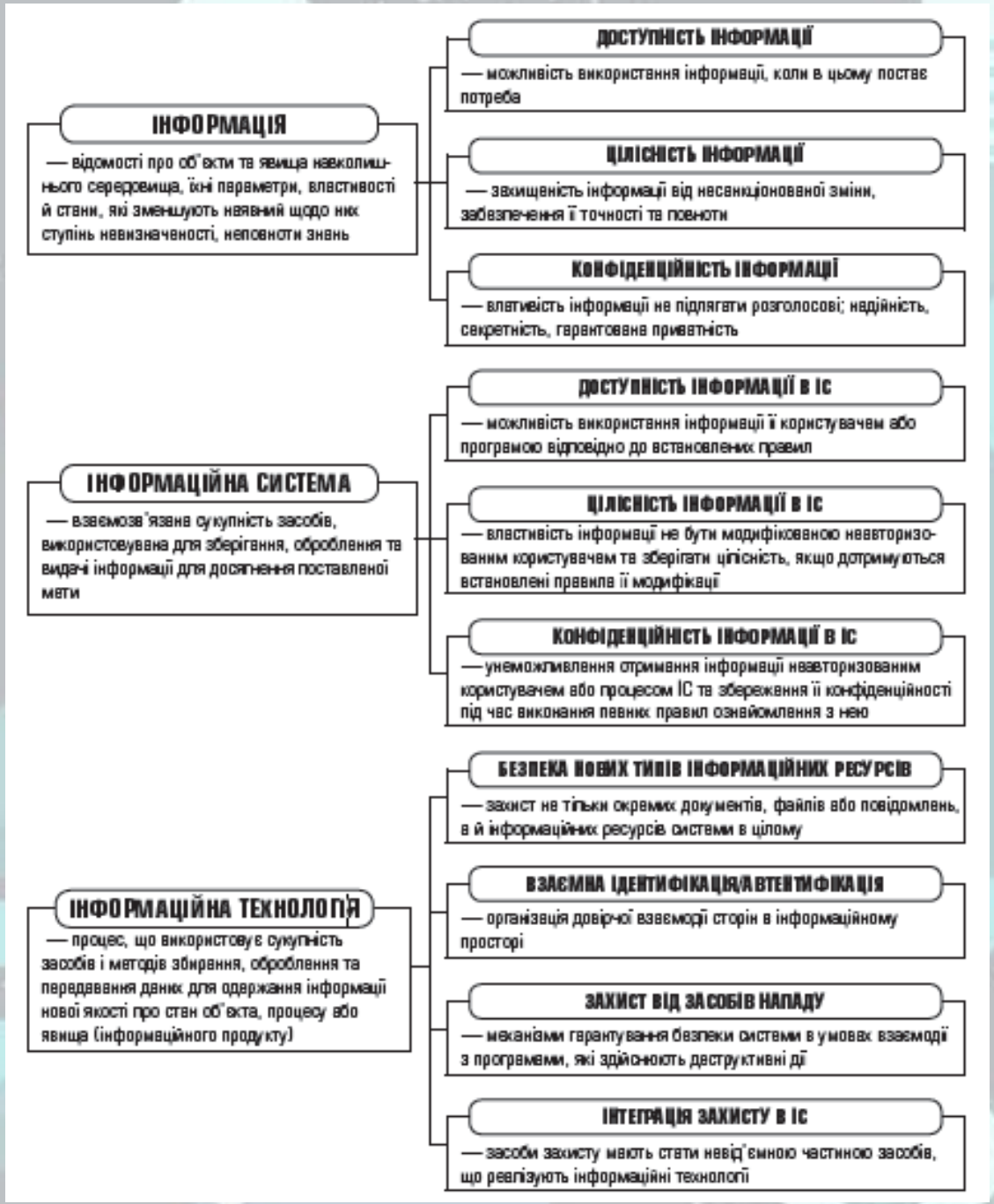

Рисунок 6 - Інформаційні системи та технології як об'єкти ІБ

Рисунок 7 - Способи нанесення збитку інформаційній безпеці

Рисунок8 -Основні методи забезпечення інформаційної безпеки

3. Дефініція поняття «Кіберборотьба»

кіберборотьба *— комплекс заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані ІТ-системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів завдяки використанню спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань.*

Кібербезпеку можна визначити як *стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам*

Рисунок 9 - Складові кібернетичної безпеки

Рисунок 10 - Взаємозв’язки і мотивація здійснення кібервпливів

Рисунок 11 - Критично важливі складові фізичної, інформаційної та кіберінфраструктури

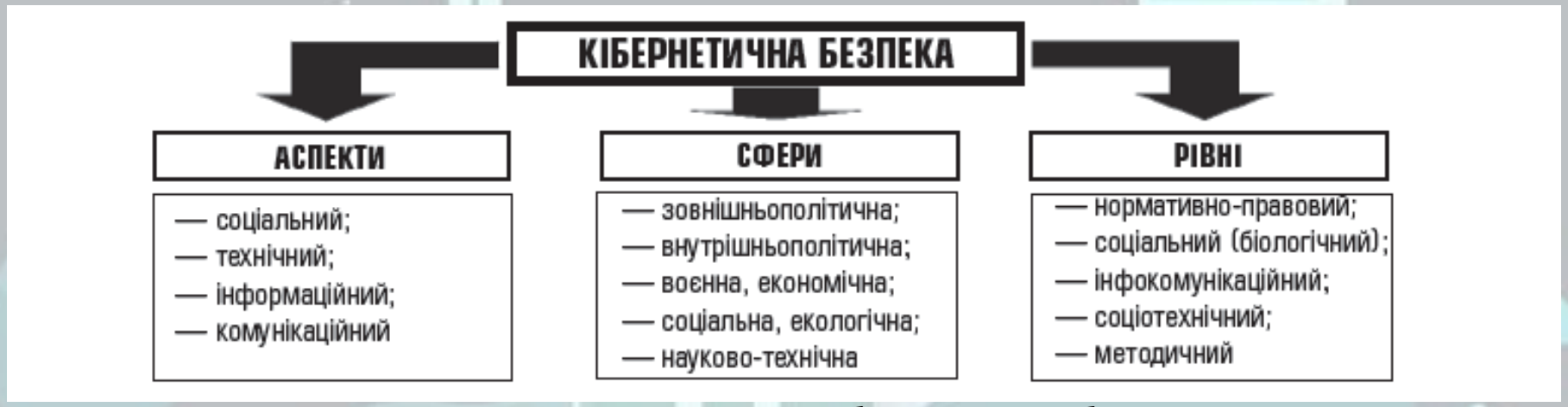

Рисунок 12 - Сутність кібернетичної безпеки

4. Нормативно-правова база :

•Конвенція Ради Європи про кіберзлочинність [10], ратифікована Законом України від 7.09.2005 року № 2824-IV;

• Закони України «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв’язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики» , «Про об’єкти підвищеної небезпеки» ;

• Укази Президента України, зокрема про Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України;

• окремі положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБОУ.

При цьому ключову роль у забезпеченні кібербезпеки відіграють:

1) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТ-системах;

2) Закон України «Про Основні засади розвитку інформаційного суспільства України на 2007–2015 роки» , у запропонованих змінах до якого наголошується на необхідності створення національної системи кібербезпеки;

3) запропонований Міністерством внутрішніх справ (МВС) законопроект «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» , яким має бути впроваджено низку термінів, пов’язаних із кібербезпекою.

Література:

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

2. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія /Р.В. Грищук, Ю.Г. Даник; за заг. ред. проф. Ю.Г. Даника. Житомир : ЖНАЕУ, 2016 – 636 с.

Нормативні документи:

1.Закон України «Про інформацію» № 2657-ХИ від 02.10.1992. - ВВР, 1992, № 48, ст. 650
https://zakon.rada.gov.ua/laws/show/2657-12#Text

Інтернет ресурси:

1. https://cert.gov.ua