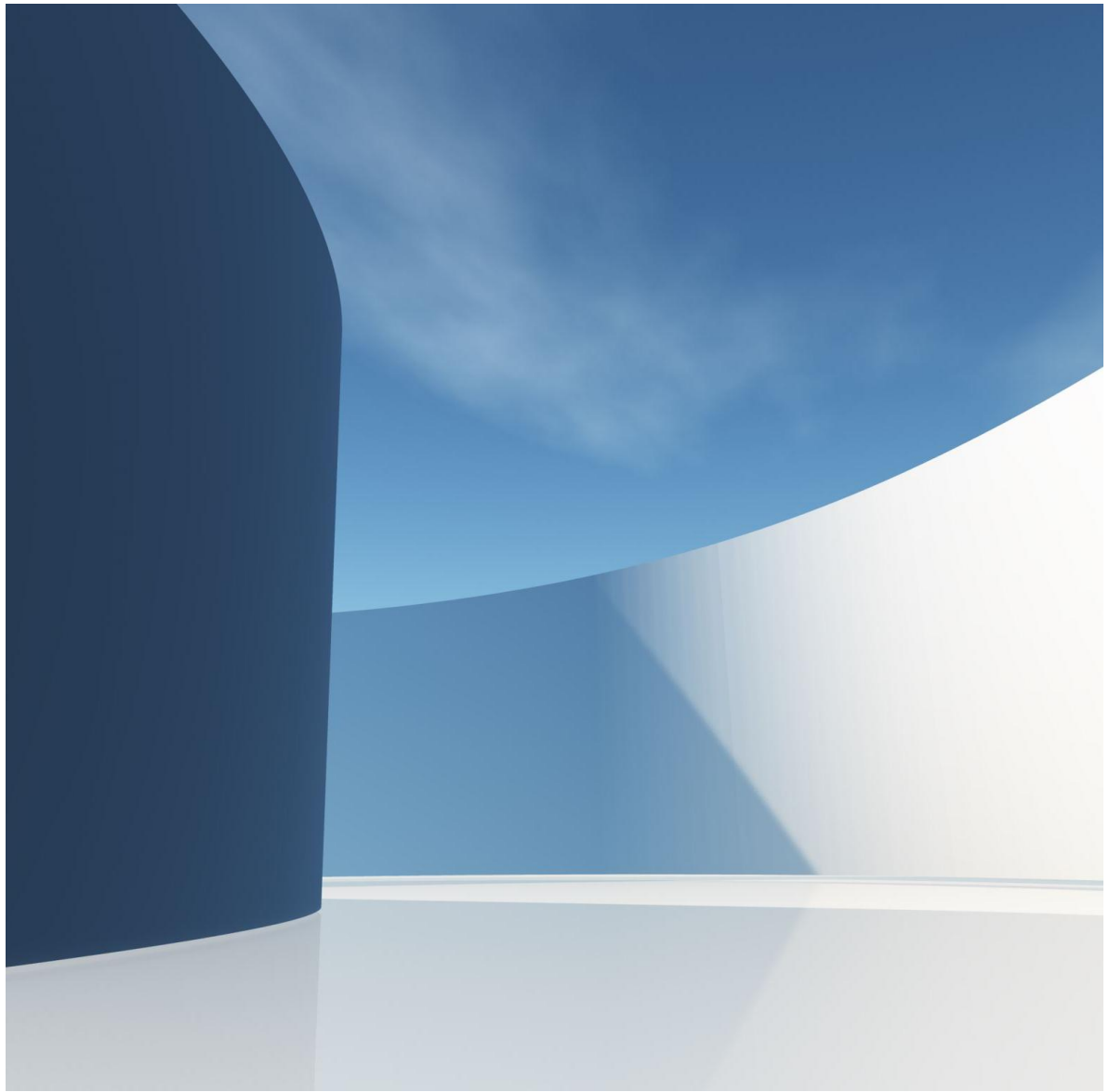
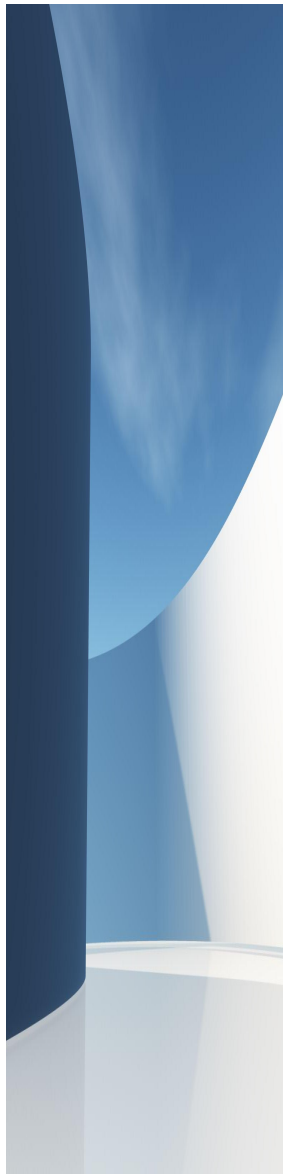


ТЕМА 1
МІЖНАРОДНО-ПРАВОВІ СТАНДАРТИ В СФЕРІ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ:



1. Правова база кібербезпеки України складається з міжнародних зобов'язань та національного законодавства

На міжнародному рівні діє Будапештська конвенція та Директива щодо мережевої та інформаційної безпеки (NIS).

У національному законодавстві мають знайти відображення зобов'язання, взяті на себе Україною як підписантом міжнародних угод і конвенцій, а також ті, які їх доведеться взяти, якщо вона й надалі демонструватиме прагнення вступити до Європейського Союзу.

Закон № 2163-VIII від 5 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України"» (далі - Закон про кібербезпеку)

Національна стратегія кібербезпеки України є основними документами, що регулюють цю сферу.

- У 2005 році Україна ратифікувала **Будапештську конвенцію** – єдиний юридично обов'язковий міжнародний документ з кібербезпеки, який встановлює спільну кримінальну політику щодо захисту від кіберзлочинності шляхом прийняття відповідного внутрішнього законодавства та сприяння міжнародному співробітництву. Проте не всі її положення інтегровані в національне законодавство, а повна реалізація потребуватиме внесення суттєвих змін до Кримінальн-опроцесуального кодексу.
- У 2016 році Європейський Парламент ухвалив першу частину єдиного для ЄС законодавства про кібербезпеку – Директиву NIS.
- Оскільки Україна не входить до ЄС, Директива NIS не є зобов'язуючою, однак вона служить настановою з питань належної практики. Деякі з її положень були добровільно впроваджені в українському законодавстві, проте інші залишаються без уваги. В останні роки Україна прийняла ряд актів, які регулюють питання кібербезпеки і становлять її національну правову базу в сфері кібербезпеки. У 2016 році Національною стратегією кібербезпеки України було визначено цілі та пріоритети кібербезпеки на період до 2020 року. Її положення були посилені у Законі про кібербезпеку, ухваленому в 2017 році. Цей закон визначає важливі терміни, розмежовує повноваження між агенціями з кібербезпеки і встановлює принципи повного регулювання захисту критичної інфраструктури (КІ) та державно-приватного партнерства

- В Україні ще не вирішено питання, як регулювати питання захисту критичної інфраструктури (**КІ**), і на якому рівні – первинного чи вторинного законодавства – це робити. Міністерство економічного розвитку і торгівлі розробило проект Закону про КІ та її захист, який було зареєстровано у Верховній Раді 8-го скликання, але не було розглянуто, то ж він вважається таким, що відкликаний. Враховуючи умови воєнного стану анси на прийняття цього законопроекту в найближчому майбутньому доволі низькі. Водночас Державна служба спеціального зв'язку та Міжнародна фундація виборчих систем (ДССЗЗІ) розробила проекти актів вторинного законодавства, що регулюють питання захисту КІ, але шанси на їх ухвалення в найближчі місяці теж досить низькі. Оскільки різні закони, що регулюють кібербезпеку, були прийняті в різний час, термінологія використовується в них непослідовно, і немає ясності щодо розмежування повноважень між агенціями з кібербезпеки, тож уся правова база кібербезпеки України потребує ретельного перегляду.

- в законодавстві існує ряд прогалин і неоднозначностей. До числа суттєвих моментів належать такі:
- невідповідність національного законодавства міжнародним зобов’язанням; • непослідовність у термінології;
- брак регулювання КІ;
- відсутність положення щодо проведення аудитів інформаційної безпеки КІ; • дублювання підвідомчості;
- відсутність чіткої вимоги до розпорядників об’єктів КІ та надавачів цифрових послуг повідомляти про кіберінциденти;
- відсутність стратегічного плану кібербезпеки;
- жорсткі бюджетні рамки, що обмежують здатність уряду платити конкурентоспроможні зарплати для залучення та утримання потрібних фахівців з питань кібербезпеки.

Упродовж останніх кількох років Україна здійснила ряд позитивних кроків для виконання своїх міжнародних зобов'язань та вдосконалення законодавства в сфері кібербезпеки, однак у цьому відношенні все ще потрібні значні зусилля. Моменти, що потребують удосконалення в першу чергу:

- подальше поліпшення існуючого законодавства для усунення прогалин і невідповідностей згідно з міжнародними зобов'язаннями, зокрема, чіткіше дотримання Будапештської конвенції та Директиви NIS;
- розробка та прийняття всеохоплюючого законодавства з питань кібербезпеки, представлення послідовної термінології; встановлення вимог щодо інформування про інциденти;
- розробка та прийняття законодавства про державно-приватні партнерства;
- прийняття нових підзаконних актів щодо встановлення спільних критеріїв і методології для віднесення об'єктів до категорії критичної інфраструктури та процедур атестації, категоризації та аудиту. Пріоритетом має стати ухвалення Закону про КІ та її захист;
- роз'яснення щодо сфер дублювання підвідомчості шляхом внесення змін до процедурних та матеріальних норм; • роз'яснення щодо ознак кіберзлочину, що кваліфікує їх як злочин;
- розмежування підвідомчості та кримінальної відповідальності за кіберзлочини проти державних чи інформаційних ресурсів, критичної інфраструктури та інших об'єктів; та
- оновлення Стратегії кібербезпеки та Стратегічний план кібербезпеки України.

- **В розділі ІІ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ** визначено заходи, яких має здійснювати на національному рівні країна, яка підписала цей документ та ратифікувала його.
- В сфері матеріального кримінального права - що стосується визначення правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем Зокрема щодо криміналізації незаконного доступу (ст.2 Конвенції)
- Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це. Сторона може вимагати, щоб таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

- Щодо **НЕЛЕГАЛЬНОГО ПЕРЕХОПЛЕННЯ**

- Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані. Сторона може вимагати, щоб таке правопорушення було вчинене з недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

- **Щодо ВТРУЧАННЯ У ДАНІ** (ст. 5)

- Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це. Сторона може залишити за собою право вимагати, щоб поведінка, описана у пункті 1, завдавала серйозну шкоду.

- **Щодо ВТРУЧАННЯ У СИСТЕМУ** (ст.6)

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.

- щодО **ЗЛОВЖИВАННЯ ПРИСТРОЯМИ** (ст.6)

- 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це:

- **a.** ***виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим*** чином:

- i. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у статтях 2 - 5 вище;
  ii. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2 - 5; та
  b. ***володіння предметом, перерахованим у підпунктах a.i або ii вище, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у статтях 2 - 5.*** Сторона може передбачити у законодавстві, що для встановлення кримінальної відповідальності необхідно володіти певною кількістю таких предметів.

- щодО **ЗЛОВЖИВАННЯ ПРИСТРОЯМИ** (ст.6)

- Ця стаття не тлумачиться як така, що встановлює кримінальну відповідальність у разі, якщо виготовлення, продаж, придбання для використання, розповсюдження чи надання для використання іншим чином або володіння, зазначені у пункті 1 цієї статті, не призначені для вчинення будь-якого зі злочинів, перерахованих у статтях 2 - 5 цієї Конвенції, такі як дозволене випробування або захист комп'ютерної системи.
- 3. Кожна Сторона може залишити за собою право не застосовувати пункт 1 цієї статті, за умови, що таке застереження не стосується продажу, розповсюдження або надання для використання іншим чином предметів, перерахованих у підпункті 1.a.ii цієї статті.

- **Правопорушення, пов'язані з комп'ютерами**

Підробка, пов'язана з комп'ютерами (ст.7)

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти. Сторона може вимагати наявність наміру обману або подібної нечесної поведінки для встановлення кримінальної відповідальності.

ШАХРАЙСТВО, ПОВ'ЯЗАНЕ З КОМП'ЮТЕРАМИ (ст.8)

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом:

a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних,

b. будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи.

- **Правопорушення, пов'язані зі змістом**
- **ПРАВОПОРУШЕННЯ, ПОВ'ЯЗАНІ З ДИТЯЧОЮ ПОРНОГРАФІЄЮ (ст.9)**

- 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, наступних дій:

- a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;
- b. пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;
  c. розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;
  d. здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;
  e. володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.

- 2. Для цілей пункту 1 вище "дитяча порнографія" включає в себе порнографічний матеріал, який візуально зображує:
- a. неповнолітню особу, задіяну у явно сексуальній поведінці;
  b. особу, яка виглядає як неповнолітня особа, задіяну у явно сексуальній поведінці;
  c. реалістичні зображення неповнолітньої особи, задіяної у явно сексуальній поведінці.

- **Правопорушення, пов'язані зі змістом**

- **Правопорушення, пов'язані з порушенням авторських та суміжних прав (ст.10)**

- 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Паризьким Актом від 24 липня 1971 р. щодо Бернської Конвенції про захист літературних та художніх творів, Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

- **Правопорушення, пов'язані зі змістом**

- **Правопорушення, пов'язані з порушенням авторських та суміжних прав (ст.10)**

- Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.
- 3. Кожна Сторона може залишити за собою право не встановлювати кримінальну відповідальність відповідно до пунктів 1 і 2 цієї статті у обмежених випадках, за умови існування інших ефективних засобів впливу, і за умови того, що таке застереження не порушує міжнародних зобов'язань Сторони відповідно до міжнародних документів, на які містяться посилання у пунктах 1 і 2 цієї статті.

правопорушення		кодексу України
Незаконний доступ	**Стаття 2:** Доступ до цілої комп'ютерної системи або її частини без права на це.	359, 361
Незаконне перехоплення	**Стаття 3:** Перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані.	163, 359, 362(2)
Втручання у дані	**Стаття 4:** Пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації без права на це.	362 (1)
Втручання у систему	**Стаття 5:** Серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.	361 (1), 363-1
Зловживання пристроями	**Стаття 6 (b):** Володіння предметом, включаючи комп'ютерну програму, створеним або адаптованим, у першу чергу, з метою вчинення будь-якого зі злочинів; або комп'ютерним паролем, кодом доступу або подібними даними, з наміром його використання для вчинення незаконного доступу/ незаконного перехоплення/втручання у дані/втручання у систему.	361-1
Підробка, пов'язана з комп'ютерами	**Стаття 7:** Навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти.	362 (1)
Шахрайство, пов'язане з комп'ютерами	**Стаття 8:** Вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних, або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи.	190 (3)
Шахрайство, пов'язане з комп'ютерами	**Стаття 9:** Вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем; пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем; розповсюдження або	301

- **Будапештська конвенція визначає такі правопорушення, які включені до українського кримінального законодавства:**

Тип правопорушення	Стаття Будапештської конвенції	Кримінального кодексу України
Правопорушення, пов'язані з порушенням авторських та суміжних прав	**Стаття 10:** Порушення авторських прав, як це визначено Паризьким Актом від 24 липня 1971 р., Угодою проторгівельні аспекти прав інтелектуальної власності та Угодою ВОІВ про авторське право або Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція).	176
Корпоративна відповідальність	**Стаття 12:** Відповідальність юридичних осіб за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на їх користь будь-якою фізичною особою, як індивідуально, так ів якості частини органу такої юридичної особи; така фізична особа має займати керівну посаду в рамках юридичної особи, в силу повноважень представляти цю юридичну особу; або повноважень приймати рішення від імені цієї юридичної особи; або повноважень здійснювати контроль	96

- **Будапештська конвенція визначає такі правопорушення, які включені до українського кримінального законодавства:**

- Література до теми 1:

- 1. Конвенція про кіберзлочинність. Конвенцію ратифіковано із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71. https://zakon.rada.gov.ua/laws/show/994_575#Text
- 2. Правова база української кібербезпеки: загальний огляд і аналіз Усі права захищені. © Міжнародна фундація виборчих систем в Україні, 2019. https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf
- 3. Про основні засади забезпечення кібербезпеки України: Закону України від 05.10.2017 р. № 2163-VIII URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text
- 4. Про Стратегію кібербезпеки України: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text
- 5. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи / Тарасюк А. В. : монографія / А. В. Тарасюк. Київ; Одеса : Фенікс, 2020. 404 с.
- 6. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. КиївОдеса : Фенікс, 2020. 260 с.