ЗМІСТ

Штучний інтелект і безпека

Подивитись анотацію та купити на **jurkniga.ua**

Анотація

Книга присвячена актуальним векторам та проблемам розвитку штучного інтелекту як інструментарію безпеки та інтелектуальної зброї майбутнього.

Також в книзі викладені напрацювання практичної спрямованості щодо потенціалу, сучасних трендів і перспектив інтегрування штучного інтелекту у різні сфери господарської діяльності і життєдіяльності суспільства та людини.

Ю. І. Когут

ШТУЧНИЙ ІНТЕЛЕКТ І БЕЗПЕКА

Практичний посібник

За редакцією доктора технічних наук, професора,
заслуженого діяча науки і техніки України,
лауреата Державної премії України в галузі науки і техніки
Довгопологого А. С.

Київ
SIDCON INTERNATIONAL CONSULTING COMPANY
Видавничий дім Дакор
2024

УДК 351.746.1-049.5:004.89](100)
К 68

Рецензенти:

Стрельбицький Микола Павлович, доктор юридичних наук, професор, заслужений працівник освіти України.

Стрельбицька Лілія Миколаївна, доктор юридичних наук, професор, заслужений працівник освіти України.

Гордієнко Сергій Георгійович, доктор юридичних наук, доцент.

Когут Ю. І.

К 68 Штучний інтелект і безпека: практичний посібник / Ю. І. Когут; за ред. док-ра тех. наук, проф. А. С. Довгополого — Київ : Консалтингова компанія «СІДКОН» ; ВД Дакор, 2024. – 294 с.

ISBN 978-617-95333-3-4

Книга присвячена актуальним векторам та проблемам розвитку штучного інтелекту як інструментарію безпеки та інтелектуальної зброї майбутнього. Також в книзі викладені напрацювання практичної спрямованості щодо потенціалу, сучасних трендів і перспектив інтегрування штучного інтелекту у різні сфери господарської діяльності і життєдіяльності суспільства та людини.

УДК 351.746.1-049.5:004.89](100)

Усі права на матеріал належать ТОВ «Консалтингова компанія «СІДКОН».
Копіювання або використання фрагментів матеріалу можливе тільки
з письмового дозволу ТОВ «Консалтингова компанія «СІДКОН».

© КОГУТ Ю. І., 2024
© ТОВ «Консалтингова компанія «СІДКОН», 2024

ISBN 978-617-95333-3-4

ЗМІСТ

ПЕРЕДМОВА **7**

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ **17**

ВСТУП **18**

1. ВНЕСОК ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ СУСПІЛЬСТВА ТА ЛЮДИНИ ... 21

1.1. Стан розвитку штучного інтелекту у світі **21**

1.2. Світові стандарти штучного інтелекту **39**

1.3. Ризики впровадження і застосування штучного інтелекту **43**

1.4. Потенційна небезпека штучного інтелекту як інтелектуальної зброї майбутнього **56**

1.5. Забезпечення кібербезпеки впровадження штучного інтелекту: аналіз вразливостей, загроз і засобів захисту **64**

1.6. Нормативне регулювання штучного інтелекту у світі **70**

Європейський Союз 71

Artificial Intelligence Act — законопроєкт ЄС про штучний інтелект 77

США 86

Велика Британія 88

Китай 89

Південна Корея 90

Польща 91

Японія ... 91
Країни — члени G7 ... 92
ООН ... 93

1.7. Система управління і регулювання штучного інтелекту в Україні ... 94

2. ОСНОВНІ ВЕКТОРИ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ БЕЗПЕКИ НА ДЕРЖАВНОМУ Й МУНІЦИПАЛЬНОМУ РІВНЯХ ... 105

2.1. Державні стратегії з впровадження, розвитку й застосування штучного інтелекту ... 105

Панканадська стратегія ШІ ... 107
Стратегія розвитку ШІ Саудівської Аравії ... 109
Стратегія розвитку ШІ Мальти ... 110
Національна стратегія розвитку штучного інтелекту Німеччини ... 110
План розвитку ШІ для нового покоління Китаю ... 111
Законодавчі ініціативи зі штучного інтелекту в США: план розвитку ШІ ... 113
Стратегія розвитку ШІ Люксембургу ... 115
Стратегія розвитку ШІ Сербії ... 115
Стратегія цифрової трансформації для Африки, Цифровий генеральний план Асоціації держав Південно-Східної Азії ... 115

2.2. Застосування штучного інтелекту у сфері національної безпеки й обороноздатності держави ... 119

2.3. Штучний інтелект на службі держави — у сфері публічного управління й адміністрування: перспективи використання GovTech і підвищення рівня цифрової безпеки ... 133

2.4. Штучний інтелект у забезпеченні безпеки муніципального управління: основні тренди розвитку 140

2.5. Роль штучного інтелекту як ключового драйвера цифрової трансформації економіки в забезпеченні економічної безпеки держави 144

2.6. Використання штучного інтелекту в інформаційній безпеці держави 150

2.7. Штучний інтелект як інструмент зниження корупційних ризиків у сфері публічних (державних) закупівель 157

2.8. Застосування технологій штучного інтелекту в діяльності органів правопорядку та у забезпеченні громадської безпеки 163

2.9. Штучний інтелект у галузі правосуддя (судовій системі) 169

2.10. Штучний інтелект у сфері безпеки у транспорті та логістиці 176

3. ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ БЕЗПЕКИ СУЧАСНОГО БІЗНЕСУ: ПОТЕНЦІАЛ, СУЧАСНІ ТРЕНДИ ТА ПЕРСПЕКТИВИ ІНТЕГРУВАННЯ У РІЗНІ СФЕРИ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ І ЖИТТЄДІЯЛЬНОСТІ ЛЮДИНИ 186

3.1. Штучний інтелект як цифровий інструментарій забезпечення безпеки функціонування, конкурентоспроможності та антикризового менеджменту компаній. Інтегрування штучного інтелекту до бізнес-процесів компаній як ефективного інструменту управління 186

3.2. Перспективи застосування технологій штучного інтелекту у сфері кібербезпеки на корпоративному рівні 197

3.3. Основні напрями використання штучного інтелекту в управлінні персоналом і професійними ризиками на корпоративному рівні ... 208

3.4. Можливості застосування технологій штучного інтелекту для підвищення ефективності та безпеки функціонування банківських установ ... 217

3.5. Штучний інтелект у дослідженні ринку та запуску рекламних кампаній: ефективні методи й етичні аспекти ... 225

3.6. Використання технологій на основі штучного інтелекту в аудиті ... 230

3.7. Штучний інтелект як інструментарій забезпечення безпеки у промисловості та енергетиці ... 234

3.8. Штучний інтелект на захисті критичної інфраструктури ... 249

3.9. Інтелектуальні технології та системи штучного інтелекту для підтримки прийняття управлінських рішень ... 256

ВИСНОВКИ ... 266

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ... 269

ВІДОМОСТІ ПРО АВТОРІВ ... 284

ПЕРЕДМОВА

Останніми роками проблематика технологій штучного інтелекту посідає одне з провідних місць у структурі досліджень та суспільних дискусій, але переважно в прикладному технічному контексті реалізації цих технологій на практиці. Наразі ми стоїмо на порозі технологічної революції, коли штучний інтелект активно розвивається, а процеси автоматизації стають такими звичними в побуті. Штучний інтелект використовується у вразливих сферах суспільства, таких як судова система, критична інфраструктура, відеоспостереження тощо, що, однак, зумовлює необхідність забезпечення кібербезпеки застосування цих новітніх технологій. Але, крім вражаючих перспектив, технології штучного інтелекту несуть в собі й низку потенційних загроз. Тому у представленій читачеві книзі, над якою працював автор та колектив провідних експертів консалтингової компанії «Сідкон», детально розглянуті, з одного боку, можливості, переваги та недоліки застосування штучного інтелекту у сфері безпеки держави, суспільства, бізнесу як своєрідного інструментарію забезпечення безпеки, з іншого — питання кібербезпеки впровадження та використання таких технологій.

Значна увага у книзі приділена аналізу потенційної небезпеки штучного інтелекту як інтелектуальної зброї майбутнього, так як проблема штучного інтелекту і можливі наслідки його виходу з-під контролю людини є однією з найактуальніших тем сьогодення. Зокрема, на Давоському Всесвітньому економічному форумі, що розпочався 15 січня 2024 р., однією з найбільших загроз штучного інтелекту визначена дезінформація і масове поширення пропаганди, які генеруються за допомогою цієї технології.

Автор обґрунтовано доводить, що головна проблема у сфері штучного інтелекту нині полягає не в створенні ефективних систем штучного інтелекту — таких розробок у світі вже достатньо, а у відсутності дієвих підходів до створення ефективної системи контролю, насамперед етичного характеру, за штучним інтелектом.

Крім того, у книзі висвітлено досвід використання штучного інтелекту у захисті критичної інфраструктури, так як тривалий час у багатьох розвинених країнах світу система безпеки та стійкості критичної інфраструктури визнана пріоритетною та однією із базових складових національної безпеки. Розглянуто інструменти на основі штучного інтелекту, які доцільно використовувати на об'єктах критичної інфраструктури для кращого виявлення загроз і захисту від них.

Незважаючи на відсутність в Україні єдиної національної стратегії розвитку штучного інтелекту, автору вдалося дослідити і систематизувати стан системи управління та регулювання штучного інтелекту в Україні. Зокрема було висвітлено аспекти Концепції розвитку ШІ в Україні.

В цілому автор наголошує, що у питаннях впровадження штучного інтелекту пильної уваги потребують безпека, надійність, прозорість, справедливість, етика й рівність (неупередженість), запобігання порушенням основних прав людини, особливо коли неможливо передбачити наслідки застосування цих технологій. Існує потреба й у формалізації та стандартизації життєвого циклу розроблення та використання безпечних систем штучного інтелекту. Правова основа щодо штучного інтелекту повинна базуватися на трьох стовпах: Закону про штучний інтелект, державній Концепції та Стратегії розвитку штучного інтелекту.

Але варто зазначити, шо тематика штучного інтелекту є настільки широкою для дослідження, що потребує й подальшого опрацювання та висвітлення.

Книга заслуговує насамперед уваги керівників усіх рівнів національних та муніципальних установ, комерційних компаній, а також може використовуватися в освітніх цілях. Цю роботу можна рекомендувати керівникам вищої ланки, експертам служби безпеки, бізнес-менеджерам критичної інфраструктури, представникам органів влади та місцевого самоврядування, яким потрібна актуальна, надійна та повна інформація для прийняття своєчасних та оптимізаційних рішень на основі збору та обробки великих даних.

Анатолій Степанович Довгополий,
головний науковий співробітник Центрального науково-дослідного інституту озброєння та військової техніки (ЦНДІ ОВТ),
доктор технічних наук, професор, заслужений діяч науки і техніки України,
лауреат Державної премії України в галузі науки і техніки

Штучний інтелект є однією з ключових технологій сучасності, що відіграє визначальну роль у забезпеченні національної безпеки держав. Найбільш розвинуті країни світу вже розробили національні стратегії впровадження та розвитку штучного інтелекту з метою визначення пріоритетів та завдань у цій сфері для прискорення темпів свого соціально-економічного розвитку. Разом з тим дослідження проблем штучного інтелекту здійснюються переважно в прикладному та комерційному аспектах, без врахування ризиків, вразливостей та загроз його впровадження, а також потенційної небезпеки штучного інтелекту як інтелектуальної зброї майбутнього. З цих міркувань є всі підстави стверджувати, що обрана автором тема для дослідження у книзі, присвяченій проблемам безпечного використання штучного інтелекту у сфері безпеки держави, суспільства, бізнесу, має важливе теоретичне та прикладне значення й, безперечно, високий рівень актуальності.

Узагальнення значної кількості наукових та науково-практичних праць видатних вчених та експертів щодо штучного інтелекту дозволило автору сформувати низку висновків щодо стану розвитку штучного інтелекту у світі та внеску технологій штучного інтелекту в сфері забезпечення цифрової безпеки суспільства та людини. Зокрема, автор слушно виокремлює такі всесвітньо визнані принципи діяльності з розвитку штучного інтелекту, як інклюзивне зростання, стійкий розвиток та загальний добробут, людиноцентричні цінності та верховенство права, прозорість і зрозумілість, звітність, технологічна незалежність, безпека та надійність. При цьому автор обґрунтовано доводить, що загальновизнані світові стандарти штучного інтелекту сприятимуть ефективному використанню переваг машинних алгоритмів і технологій штучного інтелекту та водночас у разі їх втілення на практиці допомагають знизити ризики, пов'язані з прозорістю та конфіденційністю даних при впровадженні штучного інтелекту.

Без розгляду у книзі не залишилися й такі важливі питання, як застосування штучного інтелекту у сфері національної безпеки та обороноздатності України. З цього приводу автор слушно наголошує, що штучний

інтелект допомагає фіксувати переміщення техніки та особового складу окупантів, збивати ворожі ракети, ефективніше наводити БПЛА на цілі, проводити розмінування, навіть системи протиповітряної оборони (ППО) вже оснащені ШІ, що визначає траєкторії польотів об'єктів тощо. В Україні наразі прийнято шість програмних довгострокових документів у безпековому напрямі, які стосуються питань національної безпеки та обороноздатності України і проблематики використання штучного інтелекту та сучасних інформаційно-комунікаційних технологій. Ці програмні документи розглядаються та аналізуються у книзі.

Поряд з цим хотілося особливо наголосити на розгляді автором на основі вивчення значного обсягу емпіричної бази дослідження і таких цікавих для читачів питань, як нормативне регулювання штучного інтелекту у світі та аналіз державних стратегій з впровадження, розвитку та застосування штучного інтелекту. Окремої уваги заслуговують розділи книги, де висвітлюються основні вектори впровадження штучного інтелекту у сфері безпеки на державному та муніципальному рівнях, а також потенціал, сучасні тренди та перспективи інтегрування штучного інтелекту у різні сфери господарської діяльності і життєдіяльності людини. Певним елементом новизни у процесі розгляду автором зазначених питань є аналіз різних підходів до створення інтелектуальних систем підтримки прийняття рішень, інтелектуальних систем управління та гібридних систем на основі штучного інтелекту.

У роботі поєднані теоретичне осмислення проблеми безпечного впровадження та застосування технологій штучного інтелекту та концептуальних шляхів її вирішення з практичними рекомендаціями щодо пріоритетних напрямків розвитку штучного інтелекту в сфері забезпечення цифрової безпеки держави, суспільства, бізнесу та людини.

Книга представляє інтерес для наукових співробітників та аналітиків, державних діячів та представників бізнесу, які займаються проблемами впровадження та застосування штучного інтелекту.

Микола Павлович Стрельбицький,

доктор юридичних наук, професор, заслужений працівник освіти України

На сьогодні світова наукова громадськість приділяє велику увагу штучному інтелекту як надійному інструменту підвищення конкурентоспроможності держав на міжнародних ринках, забезпечення переходу країн на принципово новий рівень розвитку національного господарства та його управління. Результатом цього стало включення урядами багатьох держав ШІ в пріоритетний список інновацій. Разом з тим, незважаючи на важливість і перспективність застосування штучного інтелекту, у повному обсязі не визначено використання технологій ШІ та прийняття безпечних рішень на його основі в суспільному житті та бізнесі. Тому цікавою з цього приводу є книга автора, яка створена на основі багаторічної роботи компанії «Сідкон» у безпековому секторі та присвячена актуальним питанням застосування штучного інтелекту як інструментарію безпеки.

У книзі здійснено ґрунтовний аналіз нормативного регулювання штучного інтелекту у світі, системи управління та регулювання штучного інтелекту в Україні та державних стратегій впровадження, розвитку та застосування штучного інтелекту. Висновки й пропозиції підтверджені належними інформаційними даними. Заслуговує на підтримку положення, що штучний інтелект — це один із інструментів, завдяки якому наддержави планують забезпечити собі світове домінування, а державні стратегії розвитку штучного інтелекту є індикаторами стану загальної цифровізації тієї чи іншої держави та готовності перенацілити ресурси на сферу застосування штучного інтелекту.

Можна позитивно оцінити намагання автора визначити напрями застосування штучного інтелекту у сфері національної безпеки та обороноздатності держави, на службі держави — у сфері публічного управління та адміністрування, муніципального управління, як ключового драйвера цифрової трансформації економіки, в інформаційній безпеці держави, в діяльності органів правопорядку, у галузі правосуддя (судовій системі), у транспорті та логістиці.

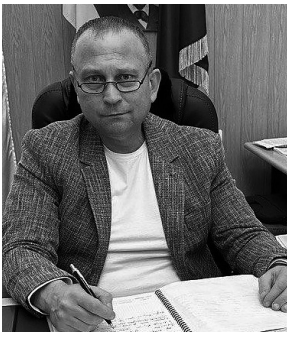
Цілком обґрунтованим та науково виваженим є наголошений висновок автора, що кожній країні, яка вирішила впроваджувати технології

штучного інтелекту у різні сфери життєдіяльності, важливо створити правове підґрунтя функціонування технологій штучного інтелекту, визначити основні сфери їх використання, напрями розвитку та правила їх застосування в кожній окремій галузі, окреслити чіткі етичні та правові межі, в яких впроваджуються технології ШІ.

При цьому значна увага у книзі приділена питанням ШІ у сфері безпеки сучасного бізнесу: як цифрового інструментарію функціонування, конкурентоспроможності та антикризового менеджменту компаній, кібербезпеки на корпоративному рівні, в управлінні персоналом та професійними ризиками, для підвищення ефективності банківських установ, у дослідженні ринку та запуску рекламних кампаній, в аудиті, у промисловості та енергетиці, на захисті критичної інфраструктури, для підтримки прийняття управлінських рішень. Ми підтримуємо позицію автора, що на даний момент штучний інтелект вже став стратегічним фактором стійкого зростання економіки та забезпечення конкурентних переваг будь-якої компанії.

Книгу можна рекомендувати державним діячам, працівникам муніципальних органів, бізнесменам, у тому числі керівникам підприємств критичної інфраструктури, а також студентам профільних ЗВО.

Лілія Миколаївна Стрельбицька,
доктор юридичних наук, професор, заслужений працівник освіти України



Штучний інтелект (ШІ) — сучасна область науки і технології, яка займається розробленням машин і систем, що демонструють інтелектуальні здібності, подібні до тих, які властиві людському інтелекту. ШІ — це технологія, що створює системи, здатні аналізувати дані, вчитися на досвіді, приймати рішення та виконувати завдання. Головною метою створення систем ШІ є полегшення повсякденної праці людини, подальший розвиток технологій та суспільства у цілому. Багато світових транснаціональних компаній вкладають щороку мільйони доларів у дослідження та експерименти у цій галузі.

У той же час безпековий аспект використання систем та технологій ШІ у різних сферах життєдіяльності суспільства на сьогодні не отримав комплексного аналізу. Робота «Штучний інтелект і безпека» демонструє системний і комплексний підхід до аналізу можливостей, переваг і недоліків використання ШІ, у тому числі як інструменту забезпечення безпеки. Тому своєчасність та актуальність цієї роботи є очевидною.

У першому розділі книги розглянуті сучасний стан розвитку систем та технологій ШІ, а також ризики їх впровадження та застосування, зокрема, детально проаналізовані вразливості та загрози системам ШІ. Значна увага у цьому розділі приділена аналізу напрацьованих багатьма країнами світу підходів до нормативного регулювання сфери впровадження і розвитку технологій ШІ.

Другий розділ присвячений питанням державних стратегій впровадження, застосування та розвитку ШІ у різних країнах світу, а також низки питань щодо використання ШІ для забезпечення цифрової трансформації економіки, забезпечення національної, інформаційної, економічної безпеки тощо. Детально розглянуто методи використання систем ШІ для захисту від різноманітних кіберзагроз, підкреслено дедалі зростаючу роль ШІ у створенні новітніх систем кіберзахисту. У той же час системи ШІ несуть значні загрози, наприклад, можуть бути використані для створення та поширення дезінформації (наприклад, технологія діпфейк). Ці питання також ґрунтовно проаналізовані у другому розділі роботи.

Третій розділ книги присвячений аналізу перспектив використання ШІ у сфері безпеки господарської діяльності на корпоративному рівні. Детально розглянуті переваги впровадження ШІ для комерційних компаній, що підвищує безпеку їхнього функціонування та конкурентоспроможність, зокрема, використання ШІ в системах управління бізнес-процесами. Описуються сучасні методи використання ШІ для захисту критичної інфраструктури держави, що є надзвичайно важливим завданням у сучасних умовах.

Робота містить великий перелік наукової літератури та документів, у тому числі англійською мовою, щодо багатьох питань технології ШІ. Наявність такого переліку, безумовно, значно збільшує корисність цієї книги для читача.

Безперечно, що завдяки всім перерахованим перевагам робота «Штучний інтелект і безпека» буде становити значний інтерес для бізнес-аналітиків, науковців, представників державних структур, допоможе в навчанні аспірантам і студентам закладів вищої освіти, а також стане корисною для всіх, хто цікавиться новітніми тенденціями в технологіях безпечного використання ШІ в умовах стрімкого розвитку цифрової економіки в усьому світі.

Олександр Аскольдович Назаренко,

ректор Державного університету інтелектуальних технологій і зв'язку

Технології штучного інтелекту за останні роки стрімко проникають у різні сфери економіки, перетворюючись із технологічної новації в невід'ємний елемент різних сфер бізнесу та життя. Сьогодні можна стверджувати, що штучний інтелект — це не просто технологічна інновація, але й величезний крок у розвитку людського суспільства, що трансформує практично всі аспекти нашого життя. У цьому захопливому та важливому процесі, який безповоротно змінює наш світ, особливе місце відводиться сфері безпеки держав, суспільства та бізнесу. Використання штучного інтелекту несе перспективу істотних змін, тому сприйняття його поляризувалося від пропозицій обмежити і контролювати до всіляко сприяти поширенню та просувати. Але найбільш важливим є пошук нових можливостей застосування штучного інтелекту у бізнесі та повсякденному житті.

Книга «Штучний інтелект і безпека» є одним з перших комплексних досліджень, яке формує розуміння, як сучасні технології можуть вплинути на аспекти безпеки на різних рівнях: суспільства в цілому, сфери державного та муніципального управління, окремих сфер бізнесу.

Представляє інтерес систематизація автором досвіду різних країн у сферах нормативного регулювання штучного інтелекту та запровадження державних стратегій його розвитку. Значний досвід автора в сфері безпекових технологій дозволив успішно дослідити не тільки ризики та загрози впровадження технологій штучного інтелекту в різні сфери життя, а й розглянути можливості використання цих технологій на користь забезпечення безпеки в різних сферах корпоративного та державного управління, таких як антикризове управління, кібербезпека та інші. Автор глибоко досліджує взаємодію між штучним інтелектом та аспектами безпеки, розкриваючи, як нові технології можуть сприяти превентивній діяльності, ефективному реагуванню на загрози та забезпеченню стійкості у різних сферах життя.

Ми живемо в еру, коли важливо не тільки відстежувати технологічний прогрес, але і розуміти, як він впливає на нашу безпеку та стабільність. Ця книга є важливим кроком у розкритті та розумінні нових викликів

і можливостей, які приносить із собою штучний інтелект у сфері безпеки держави, суспільства і бізнесу. Вона стане важливим джерелом інформації для всіх, хто цікавиться майбутнім безпеки та готовий розглядати інновації як ключовий елемент сучасного суспільства.

Ця книга є запрошенням до подорожі світом майбутнього, де штучний інтелект виявляється ключовим чинником у зміцненні безпеки держав, підтримці стійкості суспільства та розвитку інноваційного бізнесу.

Володимир Борисович Родченко,

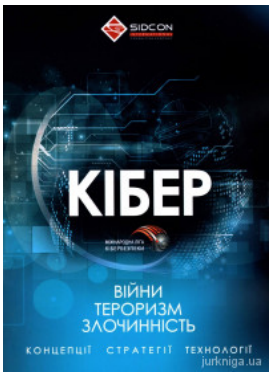
доктор економічних наук, професор, асистент-професор кафедри менеджменту університету Грегора Менделя в Брно

Книги, які можуть вас зацікавити

Основи візуального спостереження

Резолюції Генеральної Асамблеї ООН: характер і значення у контексті війни РФ проти України

Адвокатська техніка (підготовка до процесу і методики переконання)



Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології)

Суспільна мораль та антропологія в Україні: кримінально-правовий дискурс

Реадмісія нелегальних мігрантів (міжнародно-правова і внутрішньодержавна регламентація)

Перейти до галузі права
Інформаційне право

ЮРКНИГА
від теорії до практики

Перейти на сайт →