Ю.П. ЛІСОВСЬКА

КІБЕРБЕЗПЕКА: РИЗИКИ ТА ЗАХОДИ

КОНДОР

Ю.П. ЛІСОВСЬКА

КІБЕРБЕЗПЕКА: РИЗИКИ ТА ЗАХОДИ

Навчальний посібник

КОНДОР

Київ, 2019

УДК 67.401.212я73
Л11

Рекомендовано до друку на засіданні Вченої Ради
Міжрегіональної Академії управління персоналом
(протокол № 2 від 31 жовтня 2018 року)

Рецензенти:

К.В. Муравйов — доктор юридичних наук, професор, завідувач кафедри адміністративного, фінансового та банківського права Міжрегіональної Академії управління персоналом;

В.В. Остроухов — доктор філософських наук, професор, завідувач кафедри філософії Національної академії Служби безпеки України;

В.С. Цимбалюк — доктор юридичних наук, старший науковий співробітник, Керівник Інституту інформаціології.

Л11 Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. — К.: Видавничий дім «Кондор», 2019. — 272 с.

ISBN 978-617-7729-49-4

У навчальному посібнику розкрито кібербезпеку як інноваційну систему віртуальності сучасного інформаційного простору. Показано правову ентропію як кібербезпекове явище якісно нового семантичного стану особи, держави та суспільства в процесі їх самовизначення. Акцентовано, що кібербезпекове управління інвестиційним ризиком є якісним забезпеченням антикорупційної інфраструктури України та країн світу. При цьому автор передбачає нову загрозу — аерокосмічний тероризм. В результаті цього, мають бути створені якісно нові наносупутники.

Міждисциплінарний посібник розраховано на науковців, студентів, курсантів, викладачів, а також співробітників спецслужб.

ISBN 978-617-7729-49-4 УДК 67.401.212я73

ЗМІСТ

ПЕРЕДМОВА

На сучасному етапі новітніх інформаційних технологій актуального значення набуває кібербезпека, що містить у собі міжвідомчий характер у глобалізованому світі. Адже кібербезпека є правозахисним проявом сучасного віртуального світу на тлі інноваційного розвитку інформаційних технологій в системі законного капіталу.

При цьому автор передбачає нову загрозу — аерокосмічний тероризм, що відбувається в результаті «застарілих» космічних об'єктів (супутників) навколо земної поверхні. Для цього мають бути створені якісно нові наносупутники з метою очищення «застарілих» небезпечних космічних об'єктів.

Від автора

РОЗДІЛ 1. КІБЕРБЕЗПЕКА ЯК ІНФОРМОЛОГІЧНА СИСТЕМА В СУЧАСНОСТІ

1.1. Сутність та підходи до визначення кібербезпеки

У сучасних умовах інформаційного світу особливе місце в наукових дослідженнях, які активізуються з кожним роком, посідає кібербезпека. Останнім часом кібербезпека і її окремі аспекти стали предметом численних робіт дослідників. Однак, проблема усвідомлення цього явища залишається відкритою, що є логічним і необхідним, враховуючи надвисокі темпи розвитку суспільних відносин в електронній сфері. Це пояснюється, в першу чергу, розширенням можливостей інформаційного впливу на суспільні відносини, що спричиняє виникнення нових загроз громадської безпеки та викликає необхідність оновлення та вдосконалення системи її забезпечення. Крім того, саме поняття кібербезпеки вимагає якісного переосмислення, викликаного швидкими сутнісними змінами феномена інформації і домінуючими тенденціями розвитку світового співтовариства, яке значною мірою отримує «інформаційний» вимір.

У цьому сенсі масштабність сучасних перетворень інформаційної сфери є причиною виникнення ряду теоретичних і практичних проблем, що потребують уточнення поняття кібербезпеки та надання йому більш потужного і системного характеру.

Варто почати з понять, які є значними для нашого дослідження. З метою окреслення особливостей сприйняття поняття «забезпечення кібербезпеки» у межах даного до-

слідження, доцільно акцентувати увагу на визначення самого поняття «забезпечення».

Тлумачні словники, у більшості випадків, наводять подвійне смислове семантичне значення слова «забезпечення»:

1) постачаючи щось у достатній кількості, задовольняти кого, будь-що у якихось потребах;

2) створювати надійні умови для здійснення будь-чого; гарантувати щось;

3) захищати, охороняти будь-кого, будь-що від небезпеки [27, с. 375].

Як вважає А.О. Стрельцов у своїх дослідженнях стосовно поняття «забезпечення»: «Забезпечення є сукупністю діяльності по забезпеченню, засобів забезпечення та суб'єктів забезпечення. Діяльність по забезпеченню полягає у наданні допомоги суб'єктам для досягнення поставлених цілей. Засоби забезпечення утворюють сукупність матеріальних, духовних, фінансових, правових, організаційних і технічних засобів, необхідних для здійснення діяльності по забезпеченню. Суб'єктами забезпечення є індивіди, організації та органи держави, що здійснюють діяльність по забезпеченню» [164, с. 44].

С.І. Ожегов словом «забезпечити» розуміє «зробити щось цілком можливим, дійсним, реально здійсненним» [116, с. 49].

Отже, термін «забезпечення» містить в собі відповідну діяльність у всій повноті змістовних та структурних елементів як сукупної матриці з її компонентами.

У науковій літературі існує багато різних думок щодо виникнення й походження слова «безпека». У словнику В.І. Даля «безпека» — це стан, властивість від прикметника «безпечний» та одночасно — дія від дієслова «убезпечити».

Безпечний означає відсутність небезпеки, загрози; збереженість і надійність. Безпека (кого, що) означає захищати, забезпечувати відсутність небезпеки [36, с. 167]. У словнику С.І. Ожегова поняття безпека визначається як «положення, при якому небезпека не загрожує кому-небудь або чому-небудь», в іншому трактуванні — це «відсутність небезпеки, збереження, надійність». При цьому, за С.І. Ожеговим, небезпека в загальному сенсі визначається як «можливість, загроза чого-небудь небезпечного», тобто «здатного викликати, заподіяти яку-небудь шкоду, нещастя» [117, с. 88–162].

Д.О. Беззубов виокремлює наступні риси категорії «безпека», які виступають універсальними ознаками цієї категоріїі: постійність, структурність, системність, альтернативність, визначеність, конкретність досягнення, результативність, статичність, особистісне (індивідуальне) та колективне (групове) спрямування, прогнозованість [18, с. 60].

У науковій літературі відсутній єдиний усталений погляд на зміст поняття «кібербезпека». Існує необхідність уточнення поняття кібербезпеки, яке сприятиме осмисленню перспективних змін кібербезпеки та дозволить повніше розкрити її зміст та надання йому більш широкого й системного характеру, що є належним.

Б.А. Кормич зазначає, що кібербезпека — це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави [77, с. 142].

Ряд дослідників на чолі з В.В. Остроуховим пропонують наступне авторське визначення «кібербезпеки» — це стан захищеності особи, держави і суспільства, при якому досягається інформаційний розвиток (технічний, інтелектуаль-

ний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди [60, с. 10]. Варто зазначити, що в даному визначенні присутня не тільки пасивна складова «ступінь захищеності», але й активна складова «інформаційний розвиток» (технічний, інтелектуальний, соціально-політичний, морально-етичний).

Вітчизняні дослідники В.І. Андрєєв, В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест з огляду кібербезпеки розуміють захищеність інформації та інфраструктури, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації й підтримуючої інфраструктури [14, с. 55].

В.М. Петрик тлумачить кібербезпеку як стан захищеності об'єктів (особистого, суспільства, держави, інформаційно-технічної інфраструктури), за якого досягається його нормальне функціонування незалежно від наявності внутрішніх і зовнішніх інформаційних впливів [126, с. 160–161].

О.А. Баранов дає визначення кібербезпеки як стану захищеності життєво важливих інтересів особистості, суспільства й держави, за якого зводиться до мінімуму заподіяння збитків через неповноту, несвоєчасність і недостовірність інформації, через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [16, с. 134].

Калюжний Р.А. вважає, що кібербезпека — це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин пов'язаних із створенням, розпо-

всюдженням, зберіганням та використанням інформації [128, с. 20].

Цимбалюк В.С. зазначає, що кібербезпека — це стан захищеності передбачених законодавством норм і параметрів інформаційної процесії та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктних процесів і відносин [135, с. 78–79].

Степко О.М. розкриває кібербезпеку як стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [161].

Л.С. Харченко, В.А. Ліпкан, О.В. Логінов описують кібербезпеку як складову національної безпеки, процес управління загрозами та небезпеками (результат управління загрозами та небезпеками) державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [175, с. 46].

Ю.Є. Максименко підкреслює кібербезпеку як результат управління реальними чи (та) потенційними загрозами (небезпеками) з метою задоволення національних інтересів людини, суспільства та держави в електронній сфері [94, с. 52].

А.І. Марущак кібербезпеку описує через комплекс прав людини: а) вільно, безперешкодно, на свій розсуд бути суб'єктом інформаційних процесів шукати, отримувати і поширювати інформацію; б) комплекс прав людини на захист від неправомірного інформаційного втручання (право на конфіденційність інформації про особисте життя і право

на захист від поширення викривленої інформації, яка завдає шкоду її честі та репутації) [98, с. 82].

Ряд дослідників пропонують наступне визначення кібербезпеки: « ...це стан захищеності інформаційного простору, який забезпечує його формування і розвиток в інтересах громадян, організацій і держави в цілому, захист від неправомірного зовнішнього і внутрішнього втручання; стан інформаційної інфраструктури, процесів, за яких інформація використовується суворо за призначенням і не впливає негативно на інформаційну чи інші системи як самої держави, так й інших країн при її використанні [103, с. 196].

О.В. Олійник, О.В. Соснін, Л.Є. Шиманський кібербезпеку створюють через призму загроз як « ...комплекс системних упереджувальних заходів із наданням гарантій захисту життєво важливих інтересів особистості, суспільству і державі від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, самостійного і незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни, захисту від маніпулювання інформацією і дезінформацією та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз» [120, с. 540–541].

Таким чином, системний характер кібербезпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності. Для виокремлення складових його загальної структури найчастіше використовуються такі термінологічні конструкції як «напрями», «механізми» та «шляхи» за-

безпечення. Результати аналізу різноманітних джерел свідчать про недостатню розробленість та систематизованість структурних складових забезпечення кібербезпеки. Однак саме розуміння забезпечення кібербезпеки як комплексного виду діяльності дозволяє гармонізувати термінологію і здійснювати не лише структурний, а й глибокий змістовний аналіз, в повній мірі застосовуючи потенціал діяльнісного підходу.

Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. в системі забезпечення кібербезпеки розуміють сукупність інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів кібербезпеки, а також інфраструктури її забезпечення [85, с. 158].

Отже, автор пропонує розуміти в понятті «адміністративно-правове забезпечення кібербезпеки» комплекс превентивних дій економічного, політичного, юридичного, технологічного та організаційного характеру, спрямованих на попередження, виявлення і ліквідацію загроз інтересам особи, держави та суспільства в електронній сфері.

У сучасному інформаційному суспільстві система забезпечення кібербезпеки України створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в електронній сфері. Основу даної системи складають органи, сили та засоби забезпечення кібербезпеки, які застосовують комплекс адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління.

Згідно зі ст. 2 Закону України «Про основи національної безпеки України» правову основу у сфері національної безпеки України становлять Конституція, цей та інші закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти.

Серед таких актів слід окремо виділити Закони України: «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про Концепцію Національної програми інформатизації», «Про Національну програму інформатизації», «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації»; Проект Закону України «Про Концепцію національної інформаційної політики»; Указ Президента України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері кібербезпеки України».

Згідно ст. 2 Закону України «Про основи національної безпеки України», Стратегія національної безпеки України і Воєнна доктрина України є документами, обов'язковими для виконання, і основою для розробки конкретних програм за складовими державної політики національної безпеки [145].

Досліджуючи проблеми, пов'язані з кібербезпекою, необхідно враховувати, що кібербезпека є складовою частиною інформаційних технологій. Процес стрімкого розвитку та поширення нових інформаційних та телекомунікаційних технологій набуває в сучасному світі характер глобальної інформаційної революції. Цей процес безпосередньо впливає на всі сфери функціонування держави: політику, економіку, управління, фінанси, культуру, науку та розвиток ін-

формаційних відносин. Остання категорія не достатньо досліджена в працях сучасних вчених. Необхідно зазначити, що інформаційна складова виступає однією з основних у формуванні правової науки, в тому числі адміністративному праві як складової політики національної безпеки.

Інформаційні технології все більше виступають каталізатором змін правових відносин у державі, стають одним із чинників досягнення максимально позитивного результату в соціальних відносинах. Але одночасно виникає проблема формування низки негативних аспектів, які пов'язані з використанням інформаційних технологій: незаконне використання авторських прав, несанкціонований доступ до приватної та секретної інформації на всіх рівнях (від приватного до державного), несанкціонований вплив на обчислювальні машини з метою виведення їх з ладу з допомогою спеціальних програм («кібертероризм»). Усі ці негативні фактори вимагають принципово нових підходів у вивченні проблем співвідношення понять «національна безпека», «адміністративно-правове регулювання інформаційних відносин» та «кібербезпека». Ці підходи повинні базуватися на досягненнях наукового аналізу, знаходячи відображення в прийнятті практичних рекомендацій щодо захисту інформаційного простору України від протиправних посягань окремих осіб та організацій.

У сучасній правовій науці проблеми формування та розвитку інформаційної сфери суспільної безпеки України в контексті адміністративного регулювання з боку держави розглядають такі відомі вчені-адміністративісти, як О.М. Бандурка, І.С. Братков, О.В. Копан, В.П. Столбовий, О.Г. Мурашин, В.А. Ліпкан, В.О. Заросило, В.О. Шамрай та ін. Розгляд цього питання відбувається в аспекті розвитку суспіль-

них відносин, які пов'язані з інформацією, та регулювання цих відносин з допомогою адміністративно-правових норм.

Завдання дослідження кібербезпеки України полягає у визначенні адміністративної складової забезпечення кібербезпеки в державі, принципу системності в електронній сфері, структурування рівнів впливу інформаційного середовища на адміністративне регулювання України й вироблення універсального алгоритму захисту суспільства, особи та держави від інформаційних небезпек в адміністративному середовищі.

Адміністративно-правове регулювання кібербезпеки, на нашу думку, є комплексом заходів законодавчого й адміністративного характеру з метою досягнення режиму законності та порядку у сфері інформаційних відносин і забезпечення прав всіх учасників суспільства у сфері інформації, що декларуються та охороняються державою.

Цей комплекс заходів складається з двох основних блоків: законодавчого та адміністративного. Законодавчий блок — це низка законодавчих актів, які декларують права всіх суб'єктів права України на вільний доступ до інформації, визначають права і свободи громадян та інших суб'єктів права в електронній сфері. До цих нормативних актів слід віднести Конституцію України [72], Закони України «Про інформацію» [141], «Про основи національної безпеки» [145] та «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [146].

Адміністративний блок визначається наявністю компетенції у відповідних органів державної виконавчої влади, завданням яких є підтримання стану інформаційного захисту суспільства від протиправних і злочинних посягань. До цих органів виконавчої влади належать загальні органи ви-

конавчої влади, а саме Кабінет Міністрів України, Міністерства та відомства спеціальної компетенції (Міністерство економіки, Міністерство оборони України, Міністерство інформаційної політики тощо) і спеціальні органи виконавчої влади, завданням яких є охорона правопорядку в Україні (Міністерство внутрішніх справ, Служба безпеки України, Державна прикордонна служба України).

Окремим блоком у системі розгляду проблеми кібербезпеки в адміністративному аспекті, на нашу думку, є науковий блок, який необхідно виокремити, оскільки ця проблематика розглянута в сучасній правовій науці неповно і фрагментарно. Саме відсутність чіткого взаємозв'язку між розв'язанням проблеми кібербезпеки на теоретичному рівні та впровадженням результатів досліджень у життя стає окремою загрозою суспільним відносинам у цій сфері.

Адміністративно-правова діяльність України в сфері забезпечення кібербезпеки є активною категорією правового життя, завдання якої — забезпечення наявності відносин в електронній сфері, тобто самого об'єкта охорони. Основний комплекс загроз і небезпек електронній сфері — це наявність суб'єктів та їх вольових дій з метою створення перешкод для функціонування інформаційних і телекомунікаційних мереж у державі.

Головною ланкою, яка пов'язує ці компоненти, є наукові розробки в галузі адміністративного захисту інформаційної сфери та вироблення прикладних засад протидії протиправним проявам у цій сфері життєдіяльності держави. Прикладним аспектом розгляду питання кібербезпеки є вироблення методологічних засад забезпечення безпеки інформаційних відносин у системі адміністративної діяльності держави [18, с. 222–225].

В галузі кібербезпеки важливо розробити механізми генерації нових рішень, що дозволять адекватно реагувати на погрози кібербезпеки або передбачати нові погрози та вміти їм протистояти.

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 [141].

Крім того, кібербезпека — це стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через:

- ✓ неповноту, невчасність та невірогідність інформації, що використовується;
- ✓ негативний інформаційний вплив;
- ✓ негативні наслідки застосування інформаційних технологій;
- ✓ несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [146].

У цьому змісті кібербезпека має кілька напрямків:

1. Система заходів, спрямованих на недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації або порушення цілісності. Цей напрямок часто називають «Informational Security».

2. Захист політичних, державних і громадських інтересів країни, захист загальних моральних цінностей, недопущення закликів до порушення територіальної цілісності, заборона інформації, яка включає ідеї війни, насилля, дискримінації і посягання на права людини.

3. Запобігання розповсюдженню відомостей, що становлять державну таємницю, а також відомостей з обмеженим доступом до інформації закритого типу, що переміщаються через державний кордон [132].

Сьогодні в Україні сформовано певну законодавчу базу функціонування інформаційного простору України. З огляду інформаційного законодавства розуміється комплекс законів, міжнародних договорів і нормативних актів, що регламентують правовідносини в галузі збирання, опрацювання, збереження і використання інформації. Базовим законом у даній сфері відносин є Закон України «Про інформацію» від 2 жовтня 1992 р. У цьому Законі закріплені основні принципи інформаційних відносин. Такими принципами є:

- гарантованість права на інформацію — «Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір» (ст. 34 Конституції України);
- відкритість, доступність інформації, свобода обміну інформацією — «Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе... » (ст. 32 Конституції України), «Закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, мають бути доведені до відома населення...» (ст. 57 Конституції України);
- захищеність особи від втручання в її особисте та сімейне життя — «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України» (ст. 32 Конституції України);
- достовірність і повнота інформації — «Кожному гарантується судовий захист права спростовувати недостовір-

ну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації» (ст. 32 Конституції України);

- свобода вираження поглядів і переконань — «Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань» (ст. 34 Конституції України);
- правомірність одержання, використання, поширення, зберігання та захисту інформації — «Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір» (ст. 34 Конституції України).

Для створення відкритого інформаційного простору в Україні, перш за все, необхідно запустити механізм практичної реалізації конституційного права на свободу одержання інформації. Правовою основою такого механізму повинні стати законодавчо закріплені чіткі правила, умови та порядок отримання громадянами та інституційними структурами суспільства інформації в органах державної влади і місцевого самоврядування, від інших державних і недержавних юридичних осіб, а також прямого доступу до державних і недержавних інформаційних ресурсів [29].

Відповідна державна політика проводиться і щодо підтримки розвитку саме інформаційної сфери — сфери засобів масової інформації, сфери науково-технічної інформації, видавничої справи та реклами, сфери статистики, сфери бібліотечної та архівної справи, сфери інформатики та обчислювальної техніки тощо. У такому вигляді ця політика

легалізована та легітимізована у законах України: «Про Національну програму інформатизації» [144], «Про Концепцію Національної програми інформатизації» [142], «Про інформацію» [23] тощо.

В Конституції України (ст. 17) чітко закріплено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та кібербезпеки є найважливішими функціями держави, справою всього Українського народу [72].

Сучасне суспільство значним чином здобуває риси інформаційного суспільства, і як результат зростаюча роль інформації в суспільному житті обумовлює необхідність зосередження уваги на проблемах забезпечення кібербезпеки.

Дослідження проблеми кібербезпеки, як правило, починається з виявлення кола її суб'єктів. До суб'єктів забезпечення кібербезпеки належать:

- держава, що здійснює свої функції через відповідні органи:
  - Президент України;
  - Верховна Рада України;
  - Кабінет Міністрів України;
  - Рада національної безпеки і оборони України;
  - міністерства та інші центральні органи виконавчої влади (Міністерство освіти і науки України, Національний інститут стратегічних досліджень, Міністерство інформаційної політики, Національна Рада України з питань телебачення і радіомовлення; Державний комітет телебачення і радіомовлення, Державне агентство з питань науки, інновацій та інформатизації;
  - суди загальної юрисдикції;
  - прокуратура України;

– місцеві державні адміністрації та органи місцевого самоврядування;
– Служба безпеки України, Міністерство внутрішніх справ України, Міністерство оборони України, Збройні сили України, а також інші правоохоронні органи та військові формування, утворені відповідно до Законів України;
• громадяни, громадські або інші організації та об'єднання, які мають повноваження щодо забезпечення кібербезпеки відповідно до законодавства (ЗМІ, політичні партії, професійні спілки).

Таким чином, система суб'єктів забезпечення кібербезпеки України включає в себе систему суб'єктів, які забезпечують реалізацію державної політики в електронній сфері. Інтегруючим чинником для діяльності цих суб'єктів має бути спільна мета — забезпечення інформаційного суверенітету України.

1.2. Видова характеристика кібербезпеки

Захист кібербезпеки здійснюється шляхом проведення виваженої та збалансованої політики держави в електронній сфері. Враховуючи, що політика в системі кібербезпеки як всебічне суспільне явище має комплексний характер і включає внутрішньо і зовнішньополітичні, економічні, технологічні, військові та інші елементи. Тому вона потребує комплексного підходу на підставі норм адміністративного права у формуванні кібербезпеки. Оскільки йдеться саме про проведення державної політики, тобто певних владних відносинах. Адже за умов посилення зовнішніх загроз і небезпек, а також соціально-економічної й суспільно-політичної кризи, що спостерігається в Україні, особливої актуальності набувають питання забезпечення кібербезпеки. Пере-

творення, які відбуваються в Україні, охопили і гуманітарну сферу, що є важливим чинником відтворення нації. При таких умовах нагального значення набуває формування виваженої державної інформаційної політики на основі системних наукових досліджень явищ інформаційної сфери. Провідне місце серед яких займає кібербезпека.

Дослідження здійснюється із застосуванням різних методологічних підходів, зокрема системного, логіко-функціонального, індуктивного, системного аналізу та синтезу. Тому виділення і деталізація складових політики, що забезпечують кібербезпеку на основі названих методів, сприяє формуванню комплексу належних заходів, спрямованих на оптимізацію інформаційного розвитку України та інтеграції у світовий інформаційний простір.

Разом з тим, особливості загальної структури забезпечення кібербезпеки залишаються недостатньо розкритими, що негативно позначається на формуванні державної інформаційної політики. Вдосконалення правових механізмів забезпечення кібербезпеки має стати пріоритетним напрямком державної політики України.

Міждисциплінарний характер кібербезпеки, що охоплює технічні (технологічні), правові, економічні, психологічні аспекти, призводить до надзвичайної складності і багаторівневості системних зв'язків, складових забезпечення кібербезпеки. Усвідомлення особливостей кожної з них буде сприяти процесам осягнення комплексності забезпечення кібербезпеки, формування комплексу тактичних і стратегічних напрямів діяльності у сфері забезпечення кібербезпеки, гармонізації національного інформаційного законодавства, що в сукупності створює важливі основи ефективної державної інформаційної політики [169, с. 164].

Водночас, слід зазначити, що у чинному законодавстві механізм управління сферою безпеки недостатньо врегульований, відсутня чітка регламентація понятійно-категорійного апарату. Законом не визначено статус екологічної, економічної, інформаційної та державної безпеки, міру їх співвідношення з вихідним терміном «національна безпека». При аналізі категорії «національна безпека» використовуються два підходи: перший розглядає національну безпеку крізь призму «національних інтересів», другий — пов'язує національну безпеку з системою базових національних цінностей як на структурному, так і на функціональному рівнях [104, с. 88–92].

Учені в галузі адміністративного права визначають національну безпеку з огляду діяльності спеціальних органів, які її забезпечують. Так, Ю.П. Битяк національну безпеку розуміє як «стан захищеності державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави і прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб» [21, с. 445]. О.В. Копан під національну безпеку вважає як «стан країни, завдяки якому система державно-правових і суспільних гарантій забезпечує реалізацію суверенітету, конституційного порядку і територіальної цілісності держави, всебічний розвиток і захист інтересів усього населення країни від розвідувально-підривної діяльності іноземних спеціальних служб, зазіхань з боку окремих організацій, груп і осіб» [75, с. 256].

Отже, визначення проблем забезпечення національної безпеки, їх пріоритетів, послідовності та системної реалізації регламентовано в Стратегії національної безпеки Украї-

ни, що затверджена Указом Президента України від 26 травня 2015 р.

У цьому відношенні зазначена Стратегія національної безпеки України окреслює відновлення територіальної цілісності України та цілісності демократичних інститутів на всій її території, реінтеграція тимчасово окупованих територій після їх звільнення. Основними цілями Стратегії є:

- мінімізація загроз державному суверенітету та створення умов для відновлення територіальної цілісності України у межах міжнародно-визнаного державного кордону України, гарантування мирного майбутнього України як суверенної і незалежної, демократичної, соціальної, правової держави;
- утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції України до Європейського Союзу та формування умов для вступу в НАТО [147].

Для реалізації політики національної безпеки в країні створено Раду національної безпеки і оборони, яка на основі Конституції України і Закону України «Про Раду національної безпеки і оборони» визначає першочергові завдання у сфері національної безпеки, пріоритети і стратегію реагування на загрози, що з'являються, в т.ч. інформаційні, стратегію запобігання ймовірним загрозам, дає доручення відповідним відомствам, які й забезпечують відповідні напрями — складові національної безпеки. Результатом існування та розвитку національної безпеки є створення системи національної безпеки [33, с. 3].

При цьому, складовими національної безпеки виступають інформаційна, інтелектуальна (безпека культури, осві-

ти, науки), політична, воєнна, економічна, державна, екологічна та інші елементи безпеки країни.

Досліджуючи питання кібербезпеки, Б.А. Кормич стверджує, що держава, в арсеналі якої є величезний набір засобів впливу на суспільні відносини в електронній сфері, природно має виступати головним суб'єктом політики кібербезпеки. Якщо розглядати кібербезпеку як певні умови, параметри і характеристики інформаційних процесів, що відбуваються в електронній сфері держави, то саме держава має можливість за допомогою нормативно-правового регулювання визначити єдині, загальнообов'язкові стандарти інформаційних процесів, що відповідають уявленням про безпеку тих сил, які здійснюють політичну владу в цій державі [76, с. 248].

Сьогодні для України, на наш погляд, логічним кроком на шляху до інформаційного майбутнього є розробка цілісної гнучкої динамічної державної політики кібербезпеки, яка враховуватиме багатоаспектність явища кібербезпеки, перспективні тенденції змін інформаційного простору, особливості геополітичного становища, економічного стану країни і знайде своє відображення в суспільній свідомості, а також на правовому концептуально-доктринальному рівні та на рівні ефективного інформаційного законодавства, що має систематизований характер.

Виходячи з вищесказаного, з наукової точки зору, доцільним і раціональним є виділення дисциплінарних аспектів розуміння (політичного, правового, соціологічного, ідеологічного, психологічного, технічного тощо) в рамках єдиного широкого підходу до кібербезпеки як до складного соціально-технічного явища як сучасного глобального аналізу.

Так, вітчизняні дослідники Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва визначили, що державна політика забезпечення кібербезпеки України є невід'ємною складовою державної політики національної безпеки України і містить в собі офіційно прийняту систему поглядів і практичну діяльність органів державної влади та управління, спрямовану на забезпечення такого положення соціальних суб'єктів, при якому дія будь-якої інформаційної загрози не призводить до зниження рівня їх кібербезпеки нижче допустимого, небезпечного високою ймовірністю реалізації негативних інформаційних впливів [46, с. 187].

Крім того, важливим напрямом реалізації державної політики кібербезпеки є формування національної самосвідомості, національного світогляду на основі національної ідеї.

Актуальність формування національної самосвідомості особливо зростає на сучасному етапі розвитку нашої держави в умовах жорсткого інформаційно-психологічного протиборства між розвинутими країнами світу, коли об'єктами такого впливу виступають свідомість, підсвідомість людини, її ціннісні орієнтації, а також емоційно-вольова, мотиваційна та інтелектуальні сфери. При цьому беззаперечним є виховання українських громадян на основі національної ідеї [150, с. 492–500]. Поки що не сформовано такої національної ідентичності, яка б однаково задовольняла Схід і Захід.

Правова ідеологія спроможна посприяти законодавчому забезпеченню шляхів становлення України як країни, правової держави і громадянського суспільства, суттєво посилити вітчизняну правову систему, складовою якої вона є разом із законодавством і юридичною практикою [101, с. 25]. Адекватні відповіді на виклики, ризики і небезпеки

сьогодення, можна вирішити лише на засадах врахування специфіки національного, його відповідної ідентифікації в єдності трьох його складових — соціальної істини, соціального позиціонування та конструювання України як країни, держави і суспільства.

Захист кібербезпеки має здійснюватися, насамперед, шляхом проведення виваженої та збалансованої політики держави в електронній сфері, яка має три основні вектори: захист інформаційних прав і свобод людини, захист державної безпеки в електронній сфері та захист національного інформаційного ринку, економічних інтересів держави в електронній сфері, національних виробників інформаційної продукції [77, с. 146]. Основними цілями інформаційної політики України є забезпечення [37, с. 153]:

- захист інформаційного суверенітету держави (особливо захист національного інформаційного простору з інформаційним ресурсом і систем формування масового суспільної свідомості) в сучасних умовах глобалізації та інтернаціоналізації процесів в електронній сфері;
- рівня інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами;
- реалізацію конституційних прав і свобод громадян, суспільства і держави на інформацію.

Варто акцентувати, що політика кібербезпеки носить багатовекторний характер. Її головними складовими (векторами) є:

- регулювання інформаційних відносин з метою забезпечення національної безпеки, територіальної цілісності та громадського порядку, підтримання законності;
- регулювання інформаційних відносин з метою забезпечення прав і свобод громадян, здоров'я і моральності;

– регулювання інформаційних відносин у сфері комерційної інформації.

Враховуючи національні інтереси та загрози в електронній сфері, законодавець пропонує такі основні напрями державної політики з питань національної безпеки в електронній сфері:

– забезпечення інформаційного суверенітету України;
– удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
– активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;
– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в електронній сфері і переслідування журналістів за політичні позиції;
– застосування комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [145].

Крім того, єдність і взаємозв'язок напрямів державної політики щодо кібербезпеки можливо забезпечувати визначеними на законодавчому рівні правовими механізмами, серед яких:

- чітко сформульованими цілями і завданнями державної політики у цій сфері;
- забезпеченням взаємодії державних і громадських інститутів з реалізації міжвідомчих напрямів державної політики забезпечення кібербезпеки;
- організацією системи інформування суб'єктів, що діють у сфері забезпечення кібербезпеки, про актуальні проблеми, виявленні потенційних і реальних загроз і небезпек та їх джерелах, а також доцільні заходи і засоби щодо їх попередження, нейтралізації та ліквідації можливих наслідків;
- забезпеченням узгоджених і цілеспрямованих дій суб'єктів, що діють у різних сферах життєдіяльності суспільства і держави з питань адекватного реагування на виявлені потенційні і реальні загрози і небезпеки;
- забезпеченням загальнодержавного керівництва, координації та контролю у сфері кібербезпеки [119, с. 270].

Варто відзначити, що в Указі Президента України «Про Міжвідомчу комісію з питань інформаційної політики та кібербезпеки при Раді національної безпеки і оборони України» від 8 лютого 2002 була створена Міжвідомча комісія з питань інформаційної політики та кібербезпеки при Раді національної безпеки і оборони України як консультативно-дорадчий орган, що має своїми завданнями:

1) аналіз стану і можливих загроз національній безпеці України в електронній сфері та узагальнення міжнародного досвіду з формування та реалізації інформаційної політики;

2) аналіз здійснення галузевих програм і виконання заходів, пов'язаних з реалізацією міністерствами та іншими центральними органами виконавчої влади державної політики в електронній сфері;

3) розроблення та внесення Президентові України та Раді національної безпеки і оборони України пропозицій щодо:

- визначення національних інтересів України в електронній сфері, концептуальних підходів до формування державної інформаційної політики та забезпечення кібербезпеки України;
- здійснення системних заходів, спрямованих на вдосконалення інформаційної політики України, реалізацію державної стратегії розвитку і захисту національного інформаційного простору та входження України у світовий інформаційний простір;
- удосконалення системи правового та наукового забезпечення кібербезпеки України;
- розвитку інформаційної інфраструктури держави, з питань модернізації її матеріально-технічної бази та належного фінансового забезпечення;
- організації та порядку міжвідомчої взаємодії міністерств, інших центральних органів виконавчої влади у сфері забезпечення кібербезпеки;
- удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України (в тому числі альтернативною інформацією) у сфері національної безпеки і оборони [177, с. 104.].

Дослідження завдань вищезгаданого органу дозволяє зробити висновок про забезпечення співробітництва виключно органів виконавчої влади у сфері кібербезпеки України. Разом з тим, потрібна така організація, яка б змогла забезпечити координацію не тільки представників державного апарату, а й недержавних суб'єктів забезпечення інформаційної складової національної безпеки. Взаємодія

державного та громадського управління є однією з найважливіших умов соціально-економічного розвитку, державного будівництва в системі кібербезпеки особистості, суспільства, держави.

Наступним важливим аспектом, пов'язаним з формуванням і забезпеченням реалізації державної політики кібербезпеки є віднесення забезпечення кібербезпеки до найважливішої функції держави [72], що має передбачати, насамперед, формування відповідними державними органами політики і правові механізми її реалізації у сфері кібербезпеки. Важлива роль у цьому напрямку діяльності належить державним органам, які відповідно до наданих повноважень у сферах своєї відповідальності повинні здійснювати організаційне, нормативно-правове, методичне, науково-технологічне, матеріально-технічне та фінансове забезпечення реалізації державної політики кібербезпеки.

Актуальне значення, з урахуванням сучасного стану кібербезпеки України, набуває: координація діяльності всіх суб'єктів, які виконують певні повноваження у цій сфері; застосування на загальнодержавному рівні засобів і заходів державного впливу, спрямованих на ефективне та якісне виконання законів, інших нормативно-правових актів з питань кібербезпеки.

«Забезпечення кібербезпеки як справи всього українського народу» випливає з конституційної правової норми: «Носієм суверенітету і єдиним джерелом влади в Україні є народ. Народ здійснює владу безпосередньо і через органи державної влади та органи місцевого самоврядування» [72].

Отже, держава, яка забезпечує формування та реалізацію державної політики кібербезпеки, повинна реалізовувати політичну волю народу, принаймні його більшості. З

цією метою держава створює необхідну правову основу та організаційну структуру суб'єктів, на які покладено відповідні функції.

З цією метою створено Міністерство інформаційної політики України. Юрія Стеця призначено на посаду міністра інформаційної політики. Юрій Стець вважає, що Міністерство інформаційної політики повинно стати авторитетним та ефективним інструментом для вирішення наступних завдань:

- розробки та реалізації єдиної програми кібербезпеки, включно із забезпеченням населення достовірною інформацією з першоджерел;
- просування України в світі, формування іміджевих інструментів для цього;
- активного протистояння інформаційній агресії Росії;
- запобігання зовнішнього впливу на внутрішній інформаційний простір України;
- залучення інвестицій для створення національного інформаційного продукту;
- надання РНБОУ, президенту, Кабінету міністрів повної та якісної інформації для ухвалення ефективних рішень щодо безпеки країни;
- формування кадрового резерву для розвитку сфери комунікацій, імплементації відповідних міжнародних рішень та стандартів [162].

Згідно Положення про Міністерство інформаційної політики України, міністерство є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України. Міністерство інформаційної політики України входить до системи органів виконавчої влади і є головним органом у системі централь-

них органів виконавчої влади із формування стратегії інформаційної політики держави та забезпечення її дотримання у сферах просвітницької діяльності, створення інформаційної продукції, сприяння розвитку засобів масової комунікації, формування і використання національних інформаційних ресурсів, створення умов для розвитку інформаційного суспільства, а також у сфері здійснення державного нагляду (контролю) за діяльністю засобів масової комунікації та поширенням суспільно важливої інформації, незалежно від їх форми власності, в тому числі в питаннях, що стосуються національної безпеки.

Основними завданнями Міністерства інформаційної політики України є: забезпечення формування державної політики щодо діяльності засобів масової комунікації, формування стратегії інформаційної політики держави та забезпечення її дотримання, реалізація державної політики у сферах поширення інформації, просвітницької діяльності і використання національних інформаційних ресурсів, створення умов для розвитку інформаційного суспільства, а також у сфері здійснення державного нагляду (контролю) за діяльністю засобів масової комунікації незалежно від їх підпорядкування і форми власності [133].

На виконання Програми діяльності Уряду та Коаліційної угоди, укладеної депутатськими фракціями Верховної Ради України та учасниками коаліції при Міністерстві інформаційної політики України створено Експертну раду (ЕРМІП). Головною метою діяльності ЕРМІП стало напрацювання трьох взаємодоповнюючих документів: проекту Закону про Концепцію кібербезпеки, Доктрини інформаційної політики України та Державної програми розвитку інформаційного простору України. Зазначається, що метою

створення такої Експертної ради є публічне обговорення та розробка Концепції кібербезпеки України, а також співпраця з громадськими організаціями з питань, що стосуються розвитку інформаційного простору.

Експертна рада при міністерстві інформаційної політики представила проект Концепції кібербезпеки України. У документ також закладено конкретні механізми реалізації завдань із забезпечення кібербезпеки держави та додаткові режими громадського контролю за цією діяльністю.

Зазначається, що наступним етапом роботи Експертної ради при міністерстві інформаційної політики стане направлення проекту Концепції кібербезпеки для експертної оцінки фахівцями із ОБСЄ та інших міжнародних організацій.

Необхідно акцентувати, що навіть короткий аналіз вітчизняних та зарубіжних нормативно-правових актів дозволяє зробити висновок про актуалізацію шляхів вдосконалення кібербезпеки та упорядкування інформаційних відносин у всіх сферах життєдіяльності суспільства і функціонування державних і недержавних установ. Так, нестабільна політична ситуація в Україні активізує розробку, впровадження та реалізацію заходів, спрямованих на забезпечення кібербезпеки.

Тільки системне, комплексне і цілеспрямоване виконання покладених заходів всіма суб'єктами сприятиме підвищенню ефективності реалізації державної політики у сфері кібербезпеки України.

На основі проведеного аналізу досліджуваних напрямків державної політики щодо забезпечення кібербезпеки України, здійснення комплексного підходу до вирішення проблем кібербезпеки, формування та реалізація державної політики у цій сфері має базуватися на усвідомленні за-

гроз і небезпек. Їх джерела мають бути якісною підставою для адміністративно-правового визначення повноважень і функцій системи організаційного забезпечення кібербезпеки та регулювання відносин у цій сфері діяльності.

З метою визначення наукового, інформаційно-технічного, правового, економічного та організаційного механізмів реалізації єдиної політики щодо формування та розвитку системи забезпечення кібербезпеки, необхідно прийняти Закон «Про кібербезпеку».

У сучасних умовах саме системний підхід щодо кібербезпеки має бути визначальним напрямом державної політики, від якого буде залежати існування суверенної і незалежної держави, її національна безпека, соціально-економічний розвиток та відповідне місце у світовому співтоваристві.

Отже, кібербезпека є однією з основних складових національної безпеки країни. Її забезпечення з використанням якісно сформульованої національної інформаційної політики значно сприяло б досягненню успіху у виконанні завдань в політичній, воєнно-політичній, військовій, економічній, соціальній та інших сферах державної діяльності. Зокрема, впровадження вдалої інформаційної політики може істотно впливати на зниження соціальної напруги та розв'язання зовнішньополітичних й військових конфліктів.

1.3. Космічна фрактальність як важливий критерій кібербезпеки

На сучасному етапі розвитку правової держави освоєння космічного простору обумовлює необхідність комплексного вирішення складних правових, технічних, технологічних, економічних, організаційних питань. Одним із таких є актуальні питання кібербезпеки як фрактальності

космічного об'єкта в міжнародному праві, що на міждисциплінарному рівні захищає особу, державу та суспільство від будь-яких загроз. Саме в результаті досягнень синергетики як неврівноваженості та нелінійності розвитку сучасного соціуму фрактальність є нерегулярною подібністю малих частин у якісній структурі космічної природи (атому, молекули, клітини). У цьому розумінні фрактальною є і природа людської особистості, її правової ідентичності, зокрема резонуючої людської «клітини» із Всесвітом. Такий фрактальний об'єкт може бути представлений у космічному праві з огляду ціннісної матриці як ідентичність, що становить постійний аерокосмічний моніторинг, переважно у спецпідрозділах силових структур.

Актуальним питанням, пов'язаним із міжнародним космічним правом присвячені праці таких видатних вітчизняних та зарубіжних вчених, як: Ю. Шемшученко, О. Пірадова, Ю. Колосов, В. Кузніцов, О. Зотова та інші. В той же час, питання щодо розуміння кібербезпеки як фрактальності космічного об'єкта потребує системного та детального дослідження через відсутність єдиного підходу до її усвідомлення, а й отже залишаються актуальними і потребують подальшого наукового дослідження.

В сучасному законодавстві України відсутнє визначення поняття «фрактальність космічного об'єкта», оскільки в Законі України «Про космічну діяльність» міститься лише дефініція поняття об'єктів космічної діяльності (прилади та обладнання). Відповідно до Закону є матеріальні предмети штучного походження, що проектуються, виготовляються та експлуатуються як у космічному просторі (космічний сегмент, космічна інфраструктура), так і на поверхні Землі (наземний сегмент, наземна інфраструктура) з метою дослі-

дження та використання космічного простору (Закон України «Про космічну діяльність»).

Правовий зміст поняття «фрактальність космічного об'єкта»

В міжнародному космічному праві також немає єдиного підходу до визначення цього поняття, хоча термін «фрактал» доволі часто вживається серед наукової спільноти. Саме ця обставина, безперечно, актуалізує проблему визначення правового змісту поняття «космічна фрактальність».

Системного наукового обґрунтування стосовно терміну «космічна фрактальність» не було здійснено на міжнародно-правовому рівні, проте в певних наукових колах обговорюються ці питання. Серед таких спроб можна назвати міжнародну Конвенцію про міжнародну відповідальність за шкоду, завдану космічними об'єктами (1971 р.) [71] та Конвенцію про реєстрацію об'єктів, що запускають у космічний простір (1974 р.), відповідно до яких під космічними фракталами варто розуміти ментально-ціннісні складові частини космічного об'єкта, а також засоби його доставки в космічний простір. Таким чином, вказані конвенції не дають повної відповіді стосовно визначення «космічна фрактальність». Таке визначення вироблено концепцією міжнародного космічного права і зводиться до того, що ментальні (ідеологічна свідомість, мова, правова культура) фрактали як феноменологія технічних пристроїв, створених людиною, призначені для «атомізованого» використання в космічному просторі, оскільки сама людина і є «небесним тілом», що фракталами мікро-макрокосмосу, створює штучні супутники Землі, автоматичні і пілотовані кораблі та станції, ракети-носії тощо. Передусім, Конвенція 1962 року про створення Європейської організації з розробки

ракет-носіїв, у ст. 19 якої космічний об'єкт визначений як «апарат, призначений для виведення на орбіту супутника Землі або іншого небесного тіла, або для польоту по іншій траєкторії в космічному просторі» [105, с. 25]. В 1971 році на Всесвітній адміністративній конференції радіозв'язку космічний об'єкт був ототожнений з космічним кораблем і визначений як «створений людиною засіб пересування. Призначений для запуску за межі основної частини земної атмосфери» [68, с. 234].

У сучасних правових джерелах існують два основних підходи до визначення космічного об'єкта, основаного фрактальною ментальністю: функціональний і просторовий. Прихильники функціонального підходу звертають увагу на технічні характеристики космічних апаратів і на їх суттєві відмінності у цьому відношенні від повітряних суден, які використовують при польоті властивості повітря та ентропійних процесів у балістиці польоту. При цьому, на наш погляд, не враховуються в системі кібербезпеки належною мірою перспективи створення аерокосмічних об'єктів, здатних автономно злітати і підійматись у космос з поверхні землі та здійснювати посадку аналогічно повітряним судам.

Також варто визначати в методологічному аналізі кібербезпеки як космічної фрактальності просторовий підхід, що здійснює навігаційну діяльність відповідного космічного об'єкта.

З метою позначення осіб, які здійснюють космічні польоти і перебувають на борту космічних об'єктів або на небесних тілах, в угодах з міжнародного космічного права використовуються різні терміни: «космонавти», «екіпаж», «персонал», «представники», «особи на борту космічного об'єкта». Це, однак, не означає, що міжнародне космічне

право встановлює відмінності у правовому режимі осіб, які здійснюють космічні польоти, в залежності від виконування ними функцій або будь-яких інших ознак. Незалежно від того, є такі особи військовими чи цивільними, управляють вони космічним кораблем, безпілотним літальним пристроєм у вигляді «дрону» або виконують науково-дослідницькі функції, а також незалежно від їх національної належності, усі вони, з точки зору міжнародного космічного права мають однаковий статус космонавтів. На відміну від положень морського і повітряного права, в яких визначається відмінність між екіпажем і пасажирами судна, в космічному праві такої відмінності на даний час не існує. Проте в майбутньому, за умов здійснення регулярних космічних подорожей прогнозовано, що може з'явитися необхідність у виробленні і встановленні особливого правового режиму пасажирів космічних кораблів.

Адже космічний пристрій, зокрема штучний супутник Землі, використання якого регулюється нормами національного права. лише за певних умов (запуску в космічний простір або спорудження відповідного об'єкта у ньому) стає об'єктом міжнародного космічного права. Саме з моменту запуску космічного об'єкта або створення такого об'єкта в космічному просторі, включаючи небесні тіла, виникають пов'язані з ним міжнародно-правові відносини. які тривають до приземлення космічного об'єкта на території держави, яка його запустила, або згорання при входженні в щільні шари атмосфери [187, с. 201].

Згідно Конвенції 1975 року про реєстрацію об'єктів, що запускаються в космічний простір, держави направляють на ім'я Генерального секретаря ООН інформацію не лише про запущені космічні об'єкти, а й про об'єкти, які, будучи

виведеними на орбіти навколо Землі, більше не перебувають на цих орбітах. Надання такої інформації означає підтвердження факту припинення міжнародних правовідносин, пов'язаних з польотом конкретного космічного об'єкта.

Для застосування норм міжнародного космічного права важливе практичне значення має питання про те. чи відносяться до космічних об'єктів і тим самим чи підпадають під сферу дії Конвенції про реєстрацію об'єктів, що запускаються в космічний простір 1975 року, а також інших міжнародних угод по космосу літальні технічні пристрої (апарати), які. будучи виведені на навколоземну орбіту і не здійснили повного витка (так званий частково орбітальний політ), повертаються на Землю. На думку окремих фахівців у галузі космічного права положення міжнародних угод по космосу поширюються лише на такі літальні технічні пристрої (апарати), які здійснили повний виток по навколоземній орбіті. Саме так цими фахівцями сприймається, зокрема, норма п. 1 ст. II Конвенції 1975 року, в якій міститься зобов'язання реєстрації космічного об'єкта, що запускається на орбіту «навколо Землі або далі в космічний простір». У цьому відношенні частково орбітальний політ порівнюється з суборбітальними польотами міжконтинентальних балістичних ракет (МБР), на які не поширюється дія положень Конвенції 1975 року про реєстрацію об'єктів, що запускаються в космічний простір, а також інші міжнародні угоди по космосу.

У свою чергу, для такого порівняння, на наш погляд, як в юридичному, так і в технічному відношеннях немає достатніх правових підстав, оскільки стосовно часткового орбітального польоту космічного об'єкта наявність на його борту ядерної зброї стало б порушенням положень Дого-

вору 1967 року про заборону розміщувати в космосі ядерну зброю.

Кіберубезпечення як нерозповсюдження зброї масового знищення космічним об'єктом

З огляду кіберубезпечення як нерозповсюдження зброї масового знищення фрактальність космічного об'єкта дозволяє здійснювати орбітальний політ згідно міжнародних угод по космосу. Це сьогодні виклиає нагальну потребу в її актуалізації, оскільки в такому різновиді космічного об'єкту як міжконтинентальна балістична ракета основним видом зброї масового знищення є ядерна зброя. Така зброя основана на використанні енергії, що фрактально виділяється (розщеплюється) при ланцюгових реакціях ділення важких ядр відповідних ізотопів урану і плутонію або при термоядерних реакціях синтезу легких ядр ізотопів водню (дейтерію тритію) в більш важкі, наприклад ядра ізотопів гелію.

В цьому контексті правове рішення України остаточно позбутися ядерної зброї пов'язувалось із принциповістю положень про без'ядерний статус та миролюбне спрямування зовнішньої політики держави в галузі космосу було зафіксовано на той час у таких основоположних документах, як Декларація про державний суверенітет, Акт про незалежність України, «Основні напрями зовнішньої політики».

Крім того, варто зосередити увагу, що у конвенції 1975 року про реєстрацію об'єктів, що запускаються в космічний простір слідом за Договором 1967 року про принципи діяльності держав з дослідження і використання космічного простору, включаючи Місяць та інші небесні тіла (ст. VII і VIII) та Конвенцією 1972 року про міжнародну відповідальність за шкоду, завдану космічними об'єктами (ст. 1). міс-

титься положення про космічні об'єкти та їх «конструктивні елементи».

У розумінні «конструктивні елементи» космічного об'єкта в міжнародно-правових угодах по космосу необхідно зазначити телеметричну апаратуру як аерокосмічний зв'язок , енергетичне живлення, а також інше електронне обладнання для ефективного функціонування означеного об'єкта. Разом із тим, у Конвенції 1975 року, так само як і в Конвенції 1972 року, до змісту поняття космічного об'єкта включено «засіб його доставки і його частини».

За умов створення Мінародної космічної станції перед державами-учасниками постала дилема: вважати міжнародну космічну станцію космічним об'єктом, а її складові «конструктивними елементами» цього об'єкта або розглядати її як сукупність різних космічних об'єктів. що підлягають окремій реєстрації. Питання було розв'язане в Угоді про міжнародну космічну станцію. Підписаній у Вашингтоні 29 січня 1998 року урядом Канади, урядами 11 держав — членів Європейського космічного агентства, урядами Японії, Росії та США [58, с. 23]. Згідно зі ст. 5 цієї Угоди кожен партнер «реєструє в якості космічних об'єктів належні їм орбітальні елементи... ».

Фрактально виражені питання гуманності про «конструктивні елементи» космічних об'єктів або частини засобів їх доставки безпосередньо пов'язане з проблемою визначення юридичної природи так званого космічного сміття. Сьогодні в спеціальній літературі існує два підходи в цьому питанні, оскільки одні автори вважають, що таке сміття повинно класифікуватись як космічний об'єкт або його частина. Адже космічний об'єкт, який вийшов із ладу або з-під контролю, а також розпався в результаті вибуху на уламки,

не повинен розглядатися в якості космічного об'єкта або його частин. Тому будь-які збитки, завдані таким космічним сміттям, виявляться поза сферою дії Конвенції 1972 року про міжнародну відповідальність за шкоду, заподіяну космічним об'єктом.

При цьому, на думку значної кількості правознавців (С. Горов. Б. Ченг, Е. Жукова) космічне сміття повинно охоплюватися поняттям космічних об'єктів та їх частин.

Визначення правових режимів фрактальної діяльності космічних об'єктів

В системі міжнародного космічного права питання щодо визначення змісту поняття «космічне право» є дискусійним за змістом. Тому необхідно підкреслити, що у ході обговорення цього питання в науково-технічному підрозділі Комітету ООН по космосу в 1997 році було запропоновано визначення поняття космічне сміття. У цьому зв'язку. основна увага акцентувалась на не функціонуючі штучні космічні об'єкти, включаючи їх фрагменти і частини, нездатні відновити свою діяльність. А також про те, що можливість здійснити ідентифікацію його власника не має бути принциповою [68, с. 74].

Також викликало дискусію про правову природу щодо появи транспортних космічних апаратів багаторазового використання типу «Спейс Шатл», оскільки квінтесенцією результатів цієї дискусії стала узгоджена позиція з означених питань. Однак, на погляд окремих правових дослідників, при входженні в щільні шари атмосфери космічні човники повинні розглядатися в якості повітряних літальних апаратів, оскільки на цьому етапі польоту використовується реакція повітря. З метою недопущення розбіжностей у даному питанні, керівництво Національного аерокосміч-

ного агентства США (НАСА) виступило з офіційним роз'ясненням, що спуск з космічної орбіти на Землю «Спейс Шаттл» суттєво нічим не відрізняється від спуску звичайного космічного корабля і в цьому відношенні «Спейс Шатл» на всіх етапах польоту повинен розглядатися в якості космічного об'єкта. Відповідно, правовий режим даного об'єкта під час спуску і посадки визначається нормами міжнародного космічного права.

Класифікація космічних об'єктів

За означених обставин космічні об'єкти можна класифікувати за різними критеріальними напрямками. Це залежить від наявності чи відсутності екіпажу, що поділяють космічні об'єкти на дві основні групи: автоматичні і пілотовані. За територіальним виміром як місцем діяльності такі космічні об'єкти поділяються на навколоземні орбітальні та міжпланетні. У чинному міжнародному космічному праві, на відміну від міжнародного повітряного або морського права. космічні об'єкти військового призначення не виокремлюються в особливу правову категорію. У цьому виявляється специфічна особливість міжнародного космічного права порівняно з міжнародним морським і повітряним правом. У якому, відповідно, військові кораблі і військові літаки користуються особливим правовим режимом, відмінним від торгових судів і цивільної авіації.

У цьому відношенні не викликає сумнівів, що найбільш прозоро розмежування автоматичних («дронів») і пілотованих космічних об'єктів, на наш погляд, проведено в Угоді 1968 року про рятування космонавтів, повернення космонавтів і повернення об'єктів, запущених у космічний простір. Особливістю пілотованих космічних об'єктів є ментальна специфіка їх міжнародно-правового статусу залежно від

цільового призначення і місця діяльності. Тому уявляється можливим розрізняти три різновиди таких об'єктів: космічні кораблі, заселені орбітальні станції, заселені станції на небесних тілах.

Правове становлення жінки у космічній галузі як фрактальне забезпечення кібербезпеки

Сучасний розвиток космонавтики спонукає до рішучих дій гендерно-правові аспекти, оскільки сучасна жінка не може стояти осторонь глобальних проблем людства та світового розвитку правової думки. Тому сьогодні не виникає жодних зайвих питань чи емоцій, коли зустрічається жінка-підприємець, жінка-науковець чи жінка-космонавт.

В історії розвитку дослідження космічного простору можна умовно виділити чотири етапи вирішення фрактально правових проблем виходу в космічний простір, здійснення польоту людини в Космос, надання правової можливості довготривалого космічного польоту, вихід людини у відкритий Космос. Проте сьогодні можна виділити ще один етап — правове становлення жінки у космічній галузі як фрактальне забезпечення кібербезпеки. Цей етап можна характеризувати тривалістю та неоднорідністю. На перших порах «жінка як концепція для космічних досліджень не існувала» [65, с. 33]. Проте з часом прийнято правове рішення щодо проведення психологічного експерименту зі змішаним екіпажем «Замкнутий простір».

В ході експерименту було встановлено підвищення конфліктності, в результаті чого екіпажі змішаного типу були визнані не перспективними. Першим правовим проривом можна вважати політ першої жінки-космонавта, яка пройшла повний курс підготовки для польотів на кораблях типу «Восток», Валентини Володимирівни Терешкової. 16–

19 червня 1963 року на космічному кораблі «Восток-6» з тривалістю польоту 2 доби 22 години та 50 хвилин [65, с. 37]. Оскільки вона перенесла політ досить важко, і це, мабуть, стало однією з причин того, що наступний політ жінки в Космос відбувся лише через 19 років.

За таких умов багаторазово наголошувалося на неспроможності та ірраціональної обтяжувальності жінки на тлі складних екстремальних умов космічного польоту, на що заперечували жінки-космонавти. Аналізуючи причини провалу експерименту «Замкнутий простір» було виявлено, що конфліктність на борту імітованого космічного судна виникла в силу належної кваліфікації жінки, що певною мірою «зачіпала чоловічу гідність командира екіпажу» [65, с. 48].

Таким чином, сьогодні в космічній галузі були відкриті нові можливості, технології, горизонти, зокрема в США вже 25 відсотків астронавтів становлять жінки. Саме на сучасному етапі розвитку космонавтики можна озвучувати три фрактально виражені види космічних об'єктів: пілотовані кораблі, заселені орбітальні станції. заселені станції на небесних тілах. До конструктивних елементів космічних об'єктів варто віднести такі важливі пристрої як: медично-телеметричні, що дозволяють якісно контролювати стан серцево-судинної системи космонавтів у процесі довготривалих космічних польотів. При цьому необхідно вважати космічними об'єктами поруч із неземними об'єктами інфраструктури також і об'єкти наземної інфраструктури як одне ціле в теорії фрактальності. Саме така фрактальність космічного об'єкта, виходячи із гуманних намірів природознавства, є кіберубезпеченням у системі міжнародного права.

Контрольні запитання

1. Визначіть поняття «кібербезпека».
2. Охарактеризуйте сутність забезпечення кібербезпеки.
3. Які існують життєво важливі інтереси особи, держави та суспільства в електронній сфері?

Теми рефератів

1. Принципи та функції забезпечення кібербезпеки.
2. Методи забезпечення кібербезпеки.
3. Забезпечення кібербезпеки України.

РОЗДІЛ 2. МЕТОДОЛОГІЧНИЙ АНАЛІЗ КІБЕРБЕЗПЕКИ

2.1. Методи вивчення кібербезпеки

Забезпечення кібербезпеки в рекламних правовідносинах

Одним з головних пріоритетів в Україні є побудова орієнтованого на потреби та інтереси людей безпечного інформаційного суспільства, мета якого — створення, накопичення й примноження інформації та знань, вільний доступ, користування і обмін ними. Постійно зростаюча роль інформаційної сфери на сучасному етапі характеризує розвиток суспільства. Сформувалась залежність національної безпеки від забезпечення кібербезпеки, яка зростатиме пропорційно розвиткові інформаційних систем та інформаційних технологій. Адже інформація є важливим і необхідним підґрунтям для інтенсивного розвитку економіки; сфери, в яких використовуються сучасні інформаційні технології, стають все більш прибутковими.

Закон України «Про рекламу» від 03.07.1996 р. у редакції Закону від 28.12.2015 р. — основний чинний нормативно-правовий акт, що регулює рекламну діяльність. Із його прийняттям було фактично сформовано правову основу регулювання реклами в Україні. У цьому нормативному акті об'єднано норми різних галузей права, включаючи державне, адміністративне, цивільне право. Комплексний характер цього Закону пояснюється тим, що рекламна діяльність має багатоаспектний характер і тому є об'єктом комплексного правового регулювання.

Закон України «Про рекламу» розкриває основні засади рекламної діяльності в Україні, регулює відносини, що

виникають у процесі виробництва, розповсюдження та споживання реклами.

Відповідно до законодавчого визначення, реклама — це інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформувати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару.

Із цього визначення можна зробити висновок, що реклама є одним із видів інформації, тобто відомостей про осіб, предмети, факти, події, явища. Однак рекламою є не будь-яка інформація, а лише та, що має певні ознаки:

- інформація про осіб і продукцію. Слід враховувати, що поняття «особа» вживається в цьому Законі для позначення фізичної особи, в тому числі фізичної особи-підприємця, юридичної особи будь-якої форми власності, представництва нерезидента в Україні, а «товар» для позначення будь-якого предмета господарського обігу, в тому числі продукції, роботи, послуги, цінних паперів, об'єктів права інтелектуальної власності;
- інформація, що розповсюджується у будь-якій формі та будь-яким способом. Реклама може розповсюджуватися в будь-якій формі — письмовій, усній, у вигляді будь-яких зображень тощо, незалежно від засобу розповсюдження (засобу, що використовується для доведення реклами до її споживача);
- розповсюдження інформації здійснюється з метою сформувати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару.

Рекламна діяльність і реклама як складові частини інформаційних правовідносин потребують надійної кібербезпеки.

Питаннями адміністративно-правового забезпечення інформаційних відносин в галузі реклами займаються вітчизняні фахівці, серед яких слід відзначити Б.А. Кормичă, І.Б. Тацишина, П.П. Остапишина та інших.

Сьогоднішні реалії такі, що пересічна людина зазнає маніпулятивного впливу не баченого досі обсягу інформації різними каналами. Це ідеологія, іміджмейкінг, передвиборчі кампанії, паблик рилейшенез (publik relations), реклама, соціально-культурне проектування, що є відповідними інструментами маніпуляції свідомістю [87, с. 126].

У правовому змісті правовідносини безпеки інформаційних відносин в галузі реклами полягають в організації нормального (безпечного) функціонування рекламної діяльності і його учасників (рекламодавця, виробника реклами, розповсюджувача реклами, споживача реклами) [166, с. 90].

Вбачається специфіка інформаційних відносин в галузі реклами як об'єкта безпеки. Так, ст. 41 Конституції України визначає право кожного володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності. Статтею 54 Конституції України встановлюється: «Громадянам гарантується свобода літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності». Зазначені права є інформаційними за своїм об'єктом, але економічними або соціальними за своїм змістом.

З виникненням ринкових відносин в Україні значно зросла роль реклами та рекламної діяльності, які займають набагато більше місця в житті кожної людини. В даний момент реклама є провідним джерелом інформації про той

чи інший товар і, відповідно, може як принести користь, так і завдати шкоди правам і законним інтересам споживачів і виробників товарів та послуг.

У сучасних умовах сфера створення і розповсюдження реклами нерозривно пов'язана з використанням об'єктів авторського права і суміжних прав. Дедалі частіше крім учасників рекламної діяльності, а саме рекламодавця, виробника і розповсюджувача реклами, як суб'єктів правовідносин, що виникають у зв'язку з рекламою, виступають автори. При цьому як автор може виступати й безпосередньо сам виробник реклами. Закон України «Про рекламу», закріплюючи визначення поняття «виробник реклами», не розглядає його як автора та не регулює відносини, які виникають у сфері використання об'єктів авторського права в рекламній діяльності, у зв'язку із чим участь автора у відносинах, що виникають з реклами, регулюються законодавством про авторське право і суміжні права [174, с. 87].

Сучасний розвиток новітніх технологій сприяє широкому відтворенню і використанню об'єктів авторського права. Так, будь-яке фото можна без суттєвої шкоди для якості в лічені хвилини перетворити на комп'ютерний файл за допомогою сканера та використовувати при оформленні рекламного плакату для біг-бордів чи розміщенні його в журналах. Однак для того, щоб таке використання було законним, необхідна наявність дозволу власника авторських прав на фотографію або інший твір. Крім того, якщо при виробництві реклами буде створено самостійний об'єкт авторського права, автором буде виробник реклами [64, с. 8].

За загальним правилом автору належать як майнові, так і немайнові права. І якщо немайнові права пов'язані з особою автора та не можуть відчужуватись, то майнові права

можуть передаватись третім особам за згодою автора. Одним із майнових прав, які належать автору, є виключне право дозволяти використання твору третім особам будь-яким або всіма відомими способами на підставі авторського договору. Авторські договори про передачу прав на використання об'єктів можна поділити на дві основні категорії: авторські договори про передачу виключного права на використання твору та авторські договори про передачу невиключного права на використання твору. Відмінність між договорами полягає в тому, що при передачі виключних прав на використання твору за автором залишається право на використання цього твору лише в частині прав, що не передаються, тоді як при передачі невиключних прав за автором зберігається право на використання твору і на передачу невиключного права на використання твору іншим особам. Відповідно для того, щоб використовувати чужі твори в рекламі, необхідно укласти авторський договір із власником виняткових майнових прав щодо них. Авторські договори на передачу майнових прав можуть укладатись рекламним агентством, безпосередньо виробником реклами або замовником реклами, якщо він надає матеріали для виготовлення реклами. При цьому важливе значення має закріплення повного переліку прав, які передаються, оскільки відповідно до п. 8 ст. 33 Закону України «Про авторське право і суміжні права» майнові права, не зазначені в авторському договорі як передані суб'єктом авторського права, вважаються такими, що не передані, і зберігаються за автором. Тому, якщо при створенні реклами в неї включаються фотографії, музика, малюнки або інші твори, створені не самим рекламовиробником, то варто враховувати, що їх бездоговірне використання буде правопорушенням.

Слід враховувати, що, якщо виробником реклами виступають декілька осіб, наприклад, художники, дизайнери, композитори, декоратори, то усі вони визнаються співавторами. Авторське право на твір, створений у співавторстві, належить усім співавторам, незалежно від того, чи утворює такий твір одне нерозривне ціле або складається із частин, кожна з яких має самостійне значення.

Практика реклами свідчить, що більшість реклами створюється спеціалізованими юридичними особами, які мають у штаті фахівців, які спроможні творчо працювати та мають необхідні знання для створення реклами певного виду. Отже, з погляду авторського права суб'єктами цих відносин будуть: замовник, виробник реклами та автор. Як правило, замовник звертається до виробника реклами та між ними укладається цивільно-правовий договір (здебільшого, договір підряду), предметом якого є створення певної рекламної продукції. Виробник реклами для виконання своїх обов'язків за договором із замовником може звернутися до власного спеціаліста або, як це найчастіше буває, до групи спеціалістів, кожний з яких виконує певні функції, спрямовані на загальний результат, який (які) має (ють) з ним трудові відносини, або долучає до цього стороннього фахівця на підставі субпідрядних договорів або строкових трудових договорів [34].

Відносини, які виникають між виробником реклами — автором та рекламним агентством, можуть бути оформлені шляхом укладання трудового контракту. Однак, як зазначає В. Трофименко, трудова угода між працівником і власником підприємства, організації має форму наказу про прийняття на роботу, в якому, окрім безпосереднього наказу керівника прийняти громадянина на роботу, не містить

іншої інформації. Тому найбільш вдалим варіантом є визначення службового завдання на створення кожного екземпляра твору [173, с. 44].

Слід зазначити, що правовий статус автора, який має трудові відносини з рекламним агентством, відрізняється від статусу автора, який самостійно створює об'єкти, не маючи трудових та договірних відносин з іншими особами, обсягом авторських прав, яких вони набувають. Відповідно до ст. 16 Закону України «Про авторське право і суміжні права» авторське особисте немайнове право на службовий твір належить його автору. Виключне майнове право на службовий твір належить роботодавцю, якщо інше не передбачено трудовим договором (контрактом) та (або) цивільно-правовим договором між автором та роботодавцем.

У зв'язку з тим, що немайнові права автора є невідчужуваними, однією з проблем, яка може виникнути на практиці, є висунення автором вимоги зазначити його як автора в рекламі. Здебільшого така вимога буде невигідною для замовника, адже він хоче, щоб реклама повністю ідентифікувалась лише з його продукцією та найменуванням/іменем, покращувала лише його ділову репутацію тощо, а також це спричинюватиме додаткові витрати, пов'язані зі збільшення обсягу реклами та розсіюванням уваги споживача реклами. До того ж, відмова в задоволенні цієї вимоги може призвести до подання автором позову та стягнення відповідних коштів із замовника. Тому, щоб уникнути можливих спорів, пропонується внести до договору пункт про те, що твір автора використовуватиметься анонімом [96, с. 8].

Важливим є питання використання в рекламі творів, створених третіми особами раніше.

При створенні рекламного матеріалу часто використовується не весь авторський твір, а якась його частина. Наприклад, один кадр із всіма улюбленого фільму, один рядок з відомого твору тощо. Рекламовиробник часто помилково вважає, що, використовуючи такий матеріал в своїй діяльності, він не порушує чиїхось прав. Проте це не зовсім так [165, с. 63]. Відповідно ст. 9 Закону України «Про авторське право і суміжні права» частина твору, яка може використовуватися самостійно, у тому числі й оригінальна назва твору, розглядається як твір і охороняється відповідно до цього Закону [136]. Звідси можна зробити висновок: при використанні авторського твору в будь-якому об'ємі необхідно врегулювати відносини з автором цього твору на договірній основі.

Для того, щоб використовувати чужі твори в рекламі, необхідно укласти авторський договір із власником виняткових майнових прав у відношенні них. Тому якщо при виробництві реклами в неї включаються фотографії, музика, малюнки або інші твори, створені не самим рекламовиробником, то варто враховувати, що їхнє бездоговірне використання швидше за все буде правопорушенням. При цьому закон вимагає чіткої і прямої вказівки в авторському договорі всіх прав, що передаються.

Перед заключенням авторського договору варто упевнитися, чи не минув термін дії авторських прав на твір, що збираються використовувати. Термін дії майнових авторських прав за загальним правилом дорівнює періодові життя автора і 70 років після його смерті.

Оскільки рекламодавець використовує у своїй рекламі твір, то він буде нести відповідальність у випадку порушення авторських прав у більшому ступені, ніж рекламовироб-

ник, що одержав винагороду за створену рекламу. Тому при замовленні на виробництво рекламного твору рекламодавцеві рекомендується перекласти свою частку відповідальності на рекламовиробника, що у такому випадку навряд чи стане запозичати чужі твори при виконанні замовлення [26].

Іноді спори виникають щодо використання твору, автор якого помер. В цьому випадку потрібно заключати договір на використання твору або його частини уже зі спадкоємцями. Порушення цього правила може загрожувати рекламовиробникові великими неприємностями у вигляді незапланованої виплати авторської винагороди або участі в якості відповідача в суді за позовом про незаконне використання результату інтелектуальної діяльності. Прикладом може слугувати доволі широка практика.

Багато хто пам'ятає рекламу пива «Старый мельник», де використано музику І. Дунаєвського. Бюджет ролика був серйозний, і ціна помилки відповідно висока. Проте помилка була допущена. З одним із спадкоємців композитора був підписаний договір про використання мелодії, був виплачений гонорар, і питання вважалося вирішеним. Однак творці ролика не врахували, що у І. Дунаєвського чотири нащадки. Один із синів композитора виявив своє невдоволення у зв'язку з відсутністю укладеного із ним окремого договору, виник конфлікт, який загрожував судом. Справа в тому, що спадкоємці мали спільні права на твори І. Дунаєвського, і спадкоємець, з яким було підписано угоду, мав лише 25 відсотків прав. Справа до суду не дійшла, але закінчилася досить серйозною компенсацією, яка не була закладена в бюджет [24].

Авторові належить особисте право на недоторканність свого твору. Після смерті автора захист цього права без-

строково можуть здійснювати його спадкоємці. Тому варто утримуватися від серйозного перекручування в рекламі твору, особливо такого, котре може завдати шкоди честі і гідності автора.

В якості учасників рекламного процесу виступають рекламодавець, рекламовиробник і рекламорозповсюджувач. Закон «Про рекламу» визначає відповідальність кожного учасника рекламного процесу.

Рекламодавець відповідає за порушення законодавства про рекламу в частині змісту інформації, що представляє для створення реклами. При цьому необхідно довести, що порушення законодавства відбулося не з вини рекламовиробника або рекламорозповсюджувача. Відповідальність рекламовиробника виникає, якщо ним допущене порушення рекламного законодавства в частині оформлення, виробництва й підготовки реклами.

Розповсюджувач реклами відповідає за порушення законодавства про рекламу в частині, що стосується часу, місця й засобів розміщення реклами.

Відповідно до Закону «Про рекламу» контроль за дотриманням законодавства України про рекламу здійснюють у межах своєї компетенції:

- Державна інспекція України з питань захисту прав споживачів — щодо захисту прав споживачів;
- Антимонопольний комітет України — щодо дотримання законодавства про захист економічної конкуренції;
- Національна рада України з питань телебачення і радіомовлення — щодо телерадіоорганізацій усіх форм власності.
- Міністерство фінансів України — щодо реклами державних цінних паперів;

- Національна комісія з цінних паперів та фондового ринку — щодо реклами на фондовому ринку;
- Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України — щодо спорудження житлового будинку.

Таким чином, виходячи з вищевикладеної позиції законодавця та її аналізу, можна сформулювати наступні правила використання охоронюваних авторським правом творів. По-перше, слід дізнатися хто є автором охоронюваного твору. По-друге, знайти його координати та зв'язатися з ним або його спадкоємцями чи правонаступниками. По-третє, отримати дозвіл від автора або інших суб'єктів, яким належать авторські права на твір, на предмет використання твору або його уривку у рекламі за відповідний гонорар. По-четверте, укласти із цим автором або іншими суб'єктами авторського права на твір авторський договір у письмовій формі. По-п'яте, використати цей твір тільки у відповідності із умовами укладеного авторського договору.

Рекламна інформація виступає головним продуктом і основою функціонування рекламної індустрії. Забезпечення кібербезпеки в рекламних правовідносинах є необхідністю сьогодення. Порушення прав суб'єктів рекламних правовідносин змінили пріоритети розвитку рекламної діяльності в бік постійного державного контролю за цим видом діяльності внаслідок специфіки правового регулювання об'єкта дослідження. Забезпечення безпосередньо кібербезпеки людини, суспільства, юридичних осіб ґрунтується на створенні ефективно діючих правових механізмів, за допомогою яких перелічені суб'єкти мали б можливість визначити і забезпечити необхідний рівень власної безпеки.

Стосовно об'єкта дослідження існують певні наукові напрацювання вітчизняних і закордонних вчених. Але, враховуючи швидкі темпи розвитку і глобалізацію інформаційних відносин та процесів, це потребує більш ретельного дослідження. Вимоги сьогодення до інформаційного продукту — реклами — спонукає до подальшого розвитку інформаційних відносин та її безпеки в майбутньому.

Політична сутність формування кібербезпеки у галузі реклами стосується відповідних елементів політичної структури держави та суспільства: структур підготовки та прийняття політичних рішень, структур управління місцевої та регіональної влади, структур виборчих систем, інформаційно-телекомунікаційних урядових систем спеціального призначення.

Для економічної сфери сутність формування кібербезпеки у галузі реклами полягає у загальноекономічному аналізі та прогнозуванні економічного розвитку через вплив рекламного продукту на потенційних партнерів та споживачів на ринку товарів, робіт, послуг; порядку та структурі прийняття оптимальних рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, інфраструктури банківських мереж та систем, системи управління в критично важливих для функціонування держави структурах (енергетика, транспортні комунікації, телекомунікаційні та інформаційні мережі).

Досвід інформаційно розвинутих країн свідчить, що економічні переваги ґрунтуються в сучасному світі на прогресивній інформаційній експансії, в тому числі і рекламної інформації, і саме ті країни, які найбільш рушійні у напрямку інформаційної цивілізації, будуть переважати у сві-

товій господарській системі та в міжнародній конкуренції з технологічно відсталими країнами і регіонами [92, с. 24].

Суспільна сфера сутності формування кібербезпеки у галузі реклами виступає найбільш вразливою для інформаційних впливів, оскільки включає системи формування громадської думки, структури засобів масової комунікації, інформаційно-організаційні структури політичних партій, громадських рухів, національно-культурних та релігійних інституцій, структури забезпечення основних прав і свобод, плюралізму і незалежності виявлення поглядів, вільного обміну ідеями та інформацією.

У правовому змісті сутність безпеки інформаційних відносин у галузі реклами полягає в забезпеченні функціонування рекламної діяльності і її учасників (рекламодавця, виробника реклами, розповсюджувача реклами, споживача реклами) через прийняття уповноваженими органами державної влади комплексу нормативно-правових актів, які б врегульовували даний сегмент національної кібербезпеки. За словами П.П. Остапишина: «Кібербезпека в галузі реклами становить частину двох систем національної безпеки та інформаційного суспільства, які не зможуть бути цілісними без своїх складових» [121, с. 370].

Забезпечення безпеки інформаційних відносин у галузі реклами повинно здійснюватись на основі наступних принципів: верховенства права; пріоритетності прав і свобод людини і громадянина; своєчасності заходів захисту національних інтересів реальним і потенційним загрозам; чіткого розмежування повноважень та взаємодії органів державної влади у забезпеченні безпеки інформаційних відносин у галузі реклами; використання в інтересах України міждержавних систем та механізмів міжнародної колективної кібербезпеки.

Об'єктом безпеки інформаційних відносин у галузі реклами є рекламна інформація і рекламна діяльність в інформаційному просторі України, котра повинна здійснюватись на засадах непорушності прав та свобод людини і громадянина (право на достовірну інформацію); духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей суспільства; конституційного ладу, суверенітету, територіальної цілісності і недоторканості держави.

Таким чином, державна політика щодо безпеки інформаційних відносин у галузі реклами реалізується через діяльність відповідних суб'єктів — уповноважених державних органів влади, зокрема Президента України, Верховної Ради України, Ради національної безпеки і оборони України, Служби безпеки України, Міністерства інформаційної політики та інших центральних органів виконавчої влади, місцевих державних адміністрацій та органів місцевого самоврядування і інших.

Освіта, наука та виховання як ціннісні рецептори адміністративно-правового забезпечення кібербезпеки

Система освіти як важливий соціальний інститут в умовах глобалізації цивілізаційних процесів виступає стратегічним фактором і умовою виживання людства [123, с. 57].

Комплексність підходів до кібербезпеки та пов'язаних з нею проблем зумовлює обов'язкове виділення особливої діяльності, що закладає інтелектуальні підвалини успішного національного інформаційного розвитку. Високий рівень інформаційно-правової культури та професійної підготовки фахівців із забезпечення кібербезпеки займає одне з фундаментальних місць у системі гарантій кібербезпеки. В умовах реформування системи вищої освіти в Україні орга-

нізація такої підготовки є складним завданням, виконанню якого сприятиме створення консолідованими зусиллями системи цільової підготовки та перепідготовки фахівців у різних галузях забезпечення кібербезпеки.

Зокрема, до результатів такої діяльності можна віднести створення напряму підготовки фахівців з вищою освітою – 125 «Кібербезпека» [139]. Підтвердженням намірів України приєднатися до спільної боротьби з цим небезпечним явищем є ратифікація у 2005 році Європейської Конвенції про кіберзлочинність [70]. Важливість всебічних наукових досліджень у нових сферах життєдіяльності держави і суспільства не викликає сумнівів. На сучасному етапі активного входження інформаційних відносин до сфери правового регулювання особливої актуальності набувають правові дослідження. З цього приводу слушною є думка А.І. Марущака, який наголошує на доречності застосування класичних напрямів досліджень юридичної науки до проблем, пов'язаних з кібербезпекою, а саме:

- науково-теоретичне обґрунтування доцільності правового регулювання суспільних відносин, що виникають з приводу кібербезпеки особи, держави, суспільства;
- визначення основних понять та категорій, які застосовуватимуться для унормування відповідних суспільних процесів;
- наукові розробки щодо повноважень суб'єктів суспільних інформаційно-безпекових відносин, форм і методів їх реалізації;
- дослідження питань юридичної відповідальності за правопорушення у сфері кібербезпеки [97, с. 37].

Інформаційно-просвітницька діяльність є втіленням такого засобу реалізації державної влади як переконання і

загалом полягає у підвищенні рівня всіх складових інформаційної культури суспільства, і особливо інформаційно-правової культури. Крім того, важливою складовою цієї діяльності є надання суспільству об'єктивної та всебічної інформації щодо чинників, які зумовлюють основні напрями державної політики з метою формування консолідованої суспільної думки щодо них.

Сьогодні інституціоналізація з боку науки значною мірою розгорнулася саме в інформаційних технологіях. З огляду на цю інформаційну фазу інституціоналізація, зокрема вищої освіти, готує професійні кадри. Виконує функцію забезпечення належного інтелектуального рівня сучасного виробництва. При цьому, збереження та розвиток інтелектуального потенціалу країни, створення сприятливих економічних, правових і соціально-політичних умов, необхідних для розвитку науки і підготовки наукових кадрів, якісний рівень пріоритетних завдань державної політики, дозволяють духовно відродити Україну, перетворити її в єдину інтелектуальну європейську державу на засадах національної та соціальної злагоди, державності та народності як запоруки мудрості [88, с. 38].

Виходячи з наведеного, можна сказати, що основою формування інформаційного суспільства повинні бути: інформатизація всієї системи загальної і фахової освіти; підвищення ролі кваліфікації, професіоналізму і здібностей до творчості як найважливіших характеристик людського потенціалу, а також формування і розвиток індустрії інформаційних та комунікаційних послуг, в тому числі домашньої комп'ютеризації, орієнтованої на масового споживача.

Тихомиров О.О. класифікує забезпечення кібербезпеки за напрямами пізнавального процесу:

- професійна освіта;
- наукові дослідження;
- інформаційно-просвітницька діяльність [170, с. 94].

Й.У. Мастяниця підкреслює, що в процесі переходу від індустріального до інформаційного суспільства майже в усіх сферах соціальної практики ліквідуються обмеження щодо накопичення і використання його головної продуктивної сили — інформаційних ресурсів, що основу соціальної динаміки в інформаційному суспільстві становлять не традиційні матеріали, а інформаційні, інтелектуальні ресурси — знання, наука, організаційно-управлінські фактори, інтелектуальні здібності людей, їхня ініціатива і творчість [100, с. 12].

Щодо необхідності розвитку інтелектуальних ресурсів суспільства наголошують й інші українські вчені. Неодмінною умовою для того, щоб людство справилося з нинішніми проблемами, є розвиток людських ресурсів в широкому розумінні. Реально найефективнішими конструктивними можливостями розвитку людини володіє система освіти, а особливо вища освіта. Саме вища освіта як стратегічний ресурс людства, базовий елемент національної безпеки країни, один із критеріїв людського розвитку суспільства, підвалину економічного зростання, ефективний механізм становлення творчої, духовно багатої особистості [153, с. 2].

Вітчизняний науковець М. Курко стверджує, що «Майбутнє суспільства залежить від того, наскільки якісно вища освіта виконує свої функції. Саме вона готує фахівців, які визначатимуть долю держави, її безпеку, незалежність і добробут через 10–15 років [83, с. 13].

Як наголошує П. Давидов: «У сучасних умовах освіта не може залишатися у стані внутрішньої замкнутості та само-

достатності. Саме у добу глобалізації та цивілізаційних конфліктів стає зрозумілим, що освіта є не приватною справою, не результатом особистих уподобань, а соціальною технологією виробництва людини, її здібностей та вмінь» [35, с. 97].

Американський футуролог Е. Тоффлер у своїй роботі «Метаморфози влади» зазначає: «Контроль над знаннями — ось сутність майбутньої всесвітньої битви за владу в усіх інститутах людства» [171, с. 43].

В Україні виховання повинно розвиватися у двох напрямках: знання та повага до всіх існуючих культурних систем і володіння особистою культурою. Виховання — це частина освітнього процесу. Освіта розглядається як цілеспрямований процес виховання і навчання особистості в інтересах суспільства і держави. Якість освіти багато в чому визначається якістю виховання, яке повинно бути спрямоване на забезпечення процесу соціалізації особистості і формування творчо розвиненої особистості.

Майбутнє українського суспільства значною мірою залежить від здатності управляти інформацією та засобами спілкування. До причин, які зумовлюють необхідність інформаційного забезпечення національної системи освіти, слід віднести:

- підвищене насичення суспільства інформацією і зростання споживання ЗМІ;
- ідеологічне значення ЗМІ та можливість їхнього впливу на свідомість людини;
- поява явища управління інформацією в різних установах (урядові структури, політичні події, громадські об'єднання);
- активне втручання ЗМІ в демократичні процеси (вибори, парламентські слухання);

– активізація на національному та міжнародному рівнях процесу приватизації інформаційних технологій.

Виходячи з вищезазначеного, одним з найважливіших завдань інформаційного забезпечення національної системи освіти є застерегти молоду людину на рівні загальноосвітньої школи та вузу від різноманітних форм медіа-впливу або медіа-маніпулювання. Йдеться про дезінформацію, яка є свідомо помилковою інформацією, що надається для більш ефективного ведення бойових дій, перевірки на витік інформації і напрямок її витоку, а також сам процес маніпулювання інформацією, введення кого-небудь в оману шляхом надання неповної або повної, але вже не потрібної інформації, а також спотворення її частини. Метою такого впливу є прийняття об'єктом дезінфомації рішення, вигідного для маніпулятора [155, с. 30]. Існують такі види дезінформації: уведення в оману конкретної особи або групи осіб; маніпулювання вчинками (однієї людини або групи осіб); створення громадської думки щодо якоїсь проблеми або об'єкта. Уведення в оману — це надання неправдивої інформації. Маніпулювання — спосіб впливу, спрямований безпосередньо на зміну напряму активності людей. Для більш ефективного маніпулювання громадською думкою дезінформація може поширюватися одночасно через друковані та електронні ЗМІ, телебачення, мережу Інтернет, чутки. Провідну роль у поширенні такого роду «інформації» відіграють ЗМІ, що формують суспільну думку і смаки споживачів. При цьому, варто розпізнавати наміри такого маніпулятивного впливу: зловмисні чи доброчинні.

Разом з тим, такий різновид освіти покликаний сприяти розвитку здатності особистості засвоювати максимум інформації на підставі власного розуміння джерела інфор-

мації. Зазначені програми орієнтують на вивчення масмедіа впродовж усього життя, що передбачає усвідомлення ЗМІ кожним громадянином як культурної цінності, яку треба захищати, розвивати, критикувати. В Україні ідея поєднання ЗМІ та гуманітарної освіти останнім часом комплексно реалізується в експериментальному навчальному курсі «Громадянської освіти», ініційованому Міністерством освіти і науки України. На сьогодні вже існує цілісний навчальний комплекс поширення даної системи знань на рівні 9-го, 10-го та 11-го класів середньої загальноосвітньої школи.

Громадянська освіта є частиною синтезованого досвіду розвинених країн світу й, за визначенням фахівців, означає систему виховання і навчання, яка спрямована на створення умов для формування глибоко усвідомленої громадянської позиції та відповідальності особи. Вона, зокрема, передбачає: набуття молодою людиною досвіду суспільно-корисної діяльності; орієнтацію на безперервну освіту з метою постійного підтримання власної компетентності; стимулювання прагнення особистості приносити користь своєму суспільству. В національному варіанті громадянської освіти щодо вивчення ЗМІ передбачено опанування наступних сегментів:

1) інформація та її місце в суспільстві;

2) організація діяльності засобів масової інформації;

3) функції засобів масової інформації в сучасному суспільстві;

4) вплив ЗМІ на політичне життя;

5) взаємодія громадян і ЗМІ в процесі розвитку громадянського суспільства [42, с. 89].

Інформаційно-психологічна безпека особи

Інформаційно-психологічна безпека особи та суспільства є складовою частиною кібербезпеки України і займає

особливе місце в державній політиці під час її забезпечення. Це зумовлено специфікою загроз і їхніх джерел, особливим характером принципів і завдань державної політики у даній сфері. Сьогодні війни можна вести і без застосування військової сили, тобто психологічним та інформаційно-психологічним способом. У зв'язку з цим постає проблема створення інформаційно-психологічної безпеки особистості, суспільства та держави.

На думку вчених, саме психологічна складова системи національної безпеки виражається сукупністю індивідуально-психологічних, інформаційно-психологічних, соціально-психологічних, морально-психологічних та інших чинників, які здійснюють відповідний вплив на соціальну психіку кожного громадянина, формуючи певні світогляд, індивідуальну і суспільну свідомість, прагнення, поведінку, що в сукупності зумовлює певний психічний стан окремих соціальних груп та соціально-психологічний стан суспільства загалом.

Індивідуально-психологічна складова відображає психологію окремої особистості — громадянина, її готовність до суспільно корисної діяльності, ставлення до влади, співвідношення власного і суспільного, а також психологічне здоров'я особи.

Інформаційно-психологічна складова характеризує вплив інформації на індивідуальну психіку кожного громадянина й соціальну психіку спільнот і виражається в тому, що будь-яка інформація — це психічне явище, яке позитивно, нейтрально або негативно впливає на індивідуальну психіку окремих громадян і соціальну психіку суспільства загалом.

Соціально-психологічна складова виявляється в характері спілкування і взаємодії різних соціальних груп, а також

таких явищах, як наявність роботи чи безробіття, справедливість чи несправедливість тощо.

Морально-психологічна складова містить моральні засади функціонування суспільства як мотивацію поведінки й діяльності його членів, різних соціальних груп, зокрема політичних партій і блоків. Нині думка суспільства стала одним з суттєвих чинників, що впливає на процеси прийняття рішень на різних рівнях соціального й державного управління [37, с. 159].

Р.А. Калюжний та В.О. Шамрай до об'єктів кібербезпеки відносять: свідомість, психіку людей або різноманітні інформаційні системи, які становлять інформаційну інфраструктуру держави. До соціальних об'єктів кібербезпеки — особистість, колектив, суспільство та держава — її конституційний лад [62, с. 38].

В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник під інформаційно-психологічною безпекою особи вбачають стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) підсвідомість людини, що призводить до неадекватного сприйняття нею дійсності [60, с. 116].

Андрєєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. інформаційно-психологічний вплив розуміють як цілеспрямоване виробництво та розповсюдження спеціальної інформації, що надає безпосередній вплив на функціонування і розвиток інформаційно-психологічного середовища суспільства, психіку і поведінку населення України. Психологічне та пропагандистський вплив є різновидом інформаційно-психологічного впливу [14, с. 38].

Говорячи про інформаційні впливи (вплив визначається як дія, спрямована на об'єкт з метою домогтися тієї чи

іншої мети), слід враховувати, що в психології під впливом розуміється цілеспрямоване перенесення руху та інформації від одного учасника взаємодії до іншого. Вплив може бути безпосереднім (контактний) і опосередкований (дистанційний, за допомогою чого-небудь).

При веденні інформаційної боротьби об'єктами впливу можуть бути: психіка людей, інформаційно-технічні системи різного масштабу і призначення, система формування, розповсюдження та використання інформаційних ресурсів, система формування суспільної свідомості (за допомогою пропаганди та засобів масової інформації), система формування і функціонування громадської думки, система прийняття рішень [14, с. 37].

Умовно об'єкти впливу можна розділити на технічні та соціальні. У ролі технічних об'єктів можуть виступати системи управління та зв'язку, фінансово-економічної діяльності держави тощо. До соціальних об'єктів можна віднести окремих індивідів, групи, суспільство, держава, світове співтовариство. Основними соціальними елементами суспільства є групи і окремі індивіди.

Об'єктами небезпечного інформаційного впливу і, отже, кібербезпеки можуть бути: свідомість, підсвідомість, психіка людей, інформаційно-технічні системи різного масштабу та призначення.

Українські дослідники О.П. Дзьобань та О.В. Ставицька пропонують об'єднати під назвою «соціальна безпека» головні складові національної безпеки як системного феномена безпеку особистості, безпеку суспільства і безпеку держави [39, с. 71].

Суб'єктами кібербезпеки варто вважати ті органи і структури, що займаються її забезпеченням.

Виділяють такі інформаційно-психологічні впливи: психогенний, нейролінгвістичний, психоаналітичний, психотропний та психотронний [60, с. 134].

Небезпечні інформаційні впливи доцільно поділити на два види [134, с. 7]. Перший пов'язаний із втратою цінної інформації, що знижує чи підвищує ефективність діяльності противника, конкурента. Якщо об'єктом такого впливу є свідомість людей, то йдеться про розголошення державних таємниць, вербування агентів, спеціальні заходи і засоби для підслуховування. Безпеку від інформаційного впливу даного виду забезпечують органи цензури, контррозвідки й інші суб'єкти кібербезпеки.

Другий вид інформаційного впливу пов'язаний із впровадженням негативної інформації, що може не тільки призвести до наступних інформаційно-психологічних небезпек:

- Спроби узурпації влади через оволодіння інформаційними ресурсами;
- Маніпулювання суспільною свідомістю з боку неконтрольованих засобів масової інформації;
- Розподіл суспільства на поінформованих і непоінформованих;
- Психічні розлади.

Під негативним інформаційно-психологічним впливом необхідно розуміти дії, що призводять:

- до розмивання почуття гордості за свою державу, до підриву переконаності в необхідності виконувати свій конституційний обов'язок щодо захисту Батьківщини;
- до зниження морально-психологічного стану, створення обстановки невпевненості стосовно власного майбутнього та перспектив розвитку держави;

- до суперечок у суспільстві через політичні, релігійні, етнічні, службові й інші чинники, протистояння між такими групами і серед військовослужбовців;
- до неадекватного сприйняття наявної загрози національній безпеці, реальних планів і намірів ймовірного супротивника;
- до створення викривленої картини бойових дій, бойової обстановки [48, с. 2–9].

Основні джерела інформаційно-психологічного впливу:

- держава, органи влади й управління та інші державні структури й установи (зокрема й іноземні);
- суспільство (різні громадські, політичні, економічні та інші організації (зокрема й зарубіжні);
- різноманітні соціальні групи (формальні та неформальні, стійкі й випадкові, великі та малі, за місцем проживання, навчання, служби, проведення дозвілля тощо);
- певні особи (керівники держави, політичні лідери, командири і начальники, представники різних соціальних груп).

Серед основних засобів інформаційно-психологічного впливу виокремлюють:

- ЗМІ (преса, радіо, телебачення, інформаційні системи, Інтернет);
- літературу (художня, науково-технічна, суспільно-політична, спеціальна);
- мистецтво (різні напрями, так званої, масової культури);
- освіту (система дошкільної, середньої, середньо-спеціальної та вищої освіти, а також система, так званої, альтернативної освіти);
- виховання (різноманітні форми виховання в системі освіти, громадських організацій — формальних і неформальних, система організації соціальної роботи);

– особисте спілкування [38, с. 21–22].

Сучасні цифрові технології формування теле-, радіо-, відео-, аудіо-, продукції є могутнім інструментом для прихованого інформаційного впливу на великі маси людей. Подібний вплив призводить до зниження соціальної активності людей, маніпуляції їхньою свідомістю. Окрім того, інформаційні впливи здатні спровокувати розвиток фізіологічних і органічних порушень у функціонуванні організму, а також загострення чи виникнення психосоматичних захворювань [127, с. 53].

Преса, телебачення, радіо, Інтернет та інші канали можуть виступати засобами пропагандистсько-психологічного впливу на свідомість, підсвідомість внаслідок чого нав'язується особистості, суспільству, державі бажана система цінностей, поглядів, інтересів, рішень у життєво важливих сферах.

Важлива особливість інформаційно-психологічного впливу на індивідуальну свідомість полягає в тому, що людина може не помічати його і не усвідомлювати як загрозу. Поведінкою особи керує її мозок (свідомість, мислення). Усе, що спонукає людину до діяльності, має проходити через її мислення. Отже, інформаційно-психологічні впливи з метою зміни поведінки особистості в бажаному напрямку має домогтися відповідної зміни в її свідомості.

Однією з характерних тенденцій, яка склалася в сучасних умовах не тільки в Україні, але й у світі, є випереджальний розвиток форм, способів, технологій і методик впливу на свідомість (підсвідомість), і психічний стан людини порівняно з організацією протидії негативним, деструктивним психологічним впливам, інформаційно-психологічним захистом особистості й суспільства загалом.

У теперішній час все актуального значення набувають інформаційні взаємодії. Це викликано глобальним поширенням дії засобів масової інформації, таких як телебачення, радіо. Широке використання комп'ютерів, поширення комп'ютерної мережі Інтернет, значний обсяг електронних носіїв інформації, що використовують комп'ютери як відтворюючі пристрої, поширення комп'ютерних ігор та інших сучасних інформаційних засобів, вносить значну частку у формування інформаційного середовища, яке активно впливає на людину.

Проблема інформаційно-психологічної безпеки особистості, її психологічної захищеності й способів формування психологічного захисту в умовах глобалізацій них змін постає як теоретичною, так і практичною проблемою. У сучасному інформаційному суспільстві з'явився могутній засіб формування спеціальних впливів, які реалізуються за допомогою засобів масової інформації. Людина, що живе в штучному інформаційному полі, одержує найсвіжішу інформацію з усіх кінців планети, але тільки ту, яка надається їй пресою, радіопередачами, з екранів телевізорів. У такому випадку, знаходячись у відірваному від реальності світі, людина може йти навіть проти своїх власних інтересів. Така людина стає об'єктом зі вразливою свідомістю.

Інформація, як множина аналітично оброблених даних, стає не лише засобом прийняття певних рішень, а й метою соціальних процесів, глобальним важелем формування та впливу на свідомість людини [84, с. 443].

Цілеспрямовані інформаційні кампанії в друкованих виданнях, на телебаченні, в Інтернеті дають змогу впливати на населення шляхом застосування наступних спеціальних інформаційних факторів. Вони спрямовані на дезорганіза-

цію діяльності людини, вплив на свідомість таким чином, аби керувати людиною і змусити її діяти проти своєї волі, своїх інтересів. Інформація, передана за допомогою сучасних технічних засобів, дозволяє формувати поведінку багатьох людей.

Друковані засоби впливу є доступними, різноманітними, завдяки чому здатні масово впливати на аудиторію.

8 вересня 2016 року Кабінет Міністрів України схвалив проект закону «Про внесення змін до деяких законів України щодо обмеження доступу на український ринок іноземної друкованої продукції антиукраїнського змісту». Метою документу є протидія інформаційній агресії Російської Федерації та дотримання вимог законодавства України щодо заборони пропаганди ксенофобії, тероризму та сепаратизму. Зокрема, законопроектом передбачається заборонити використання друкованих засобів масової інформації та видавничої продукції для закликів до захоплення влади, насильницької зміни конституційного ладу або територіальної цілісності України; пропаганди війни, насильства та жорстокості; розпалювання расової, національної, релігійної ворожнечі; пропаганди комуністичного та / або націонал-соціалістичного (нацистського) тоталітарних режимів та їхньої символіки; популяризації або пропаганди органів держави-агресора та їхніх окремих дій, що створюють позитивний образ працівників держави-агресора, працівників радянських органів державної безпеки, виправдовують чи визнають правомірною окупацію території України.

Після вступу у дію закону буде запроваджено процедуру видачі дозвільного документу на ввезення видавничої продукції, що походить з держави-агресора чи тимчасово окупованої території України. Дозволу не потребуватиме

лише видавнича продукція, що ввозиться громадянами в ручній поклажі або супроводженому багажі загальною кількістю, що не перевищує 10 примірників. Критерії оцінки видавничої продукції, яка дозволена до розповсюдження на території України, розроблятимуться експертною радою та затверджуватимуться уповноваженим органом. Відповідні зміни пропонується внести до трьох законів України: «Про друковані засоби масової інформації (пресу) в Україні», «Про видавничу справу» та «Про перелік документів дозвільного характеру у сфері господарської діяльності» [61].

Вплив через радіозасоби дозволяє охоплювати масові аудиторії шляхом передачі в ефір спеціальних радіопрограм. Жоден інший засіб масової інформації не може конкурувати з радіо за широтою охоплення аудиторії.

Засобами телебачення вплив здійснюється шляхом передачі в ефір телепрограм. Телебачення — одна з найбільш ефективних форм інформаційно-психологічних впливів. Воно перетворилося в засіб, що ефективно захопив розум мільярдів людей на Землі.

4 червня 2015 року набрав чинності закон «Про внесення змін до деяких законів щодо захисту інформаційного телерадіопростору України», який передбачає, зокрема, введення санкцій проти українських телеканалів, що показують заборонені російські фільми та серіали.

Закон забороняє:

- розповсюдження і демонстрування в Україні фільмів, що містять популяризацію або пропаганду органів держави-агресора (Російської Федерації) та їхніх окремих дій, що створюють позитивний образ працівників держави-агресора, працівників радянських органів державної безпеки, виправдовують чи визнають правомірною

окупацію території України, вироблених після 1 серпня 1991 року;

- трансляцію (демонстрування шляхом показу каналами мовлення) будь-яких фільмів, вироблених фізичними та юридичними особами держави-агресора (Російської Федерації) після 1 січня 2014 року;
- трансляцію телепередач, виготовлених після 1 серпня 1991 року, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що виправдовують чи визнають правомірною окупацію території України;
- трансляцію аудіовізуальних творів (фільмів, телепередач, крім інформаційних та інформаційно-аналітичних телепередач), одним із учасників яких є особа, внесена до Переліку осіб, які створюють загрозу національній безпеці, оприлюдненого на веб-сайті Міністерства культури України (цей перелік складається на підставі звернень Ради національної безпеки й оборони, Служби безпеки України та Національної ради з питань телебачення і радіомовлення). При цьому учасником аудіовізуального твору вважається фізична особа, яка брала участь у його створенні під власним ім'ям (псевдонімом) або як виконавець будь-якої ролі, виконавець музичного твору, що використовується в аудіовізуальному творі, автор сценарію та / або текстів чи діалогів, режисер-постановник, продюсер.

Закон встановлює критерії визначення аудіовізуальних творів, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій:

- серед позитивних героїв фільму є співробітники (у тому числі колишні або позаштатні) органів держави-агресора, радянських органів безпеки;

- сюжет фільму безпосередньо або опосередковано пов'язаний з діяльністю органів держави-агресора, радянських органів безпеки, і ця діяльність представлена у фільмі як позитивна;
- у сюжеті фільму безпосередньо або опосередковано заперечується або ставиться під сумнів територіальна цілісність України, виправдовується або подається в позитивному світлі окупація території України, акти агресії з боку інших держав, розв'язування війни, пропагується винятковість, зверхність або неповноцінність осіб за ознаками їх релігійних переконань, належності до певної нації або раси, статі, майнового стану, соціального походження [112].

Але телебачення може викликати і позитивні ефекти. Телевізійні зображення можуть створювати певні психологічні ефекти, зокрема, формувати гарний настрій, підвищувати імунітет організму, навіть незалежно від змісту зображення [127, с. 48]. При формуванні телевізійних програм досить часто використовуються різного роду світлові спалахи. Їхній вплив має психофізіологічну природу, — регулюючи параметри світлового і звукового сигналу, можна домогтися певного психофізіологічного ефекту, цілеспрямовано формувати спеціальні інформаційні впливи.

Підбираючи кольорову гаму телевізійних передач, комп'ютерних ігор, інтернетівських сайтів, можна програмувати ефект впливу зображень на людину.

Інтернет — це глобальна інформаційно-комп'ютерна мережа, організована на громадських засадах і самофінансована сукупність вузлів різних рівнів. Через свою масовість, доступність, швидкість розповсюдження, Інтернет породжує наступні загрози: несанкціоноване отримання інфор-

мації з обмеженим доступом, вплив на функціонування комп'ютерів та мереж, розповсюдження інформації з метою інформаційно-психологічного впливу. Інтернет також є консцієнтальною зброєю для масового споживача, що викликає небезпеку для здоров'я підлітків.

Консцієнтальна зброя використовується при веденні консцієнтальних війн, які націлені на підкорення свідомості людей, що проживають на певній території. У випадку використання цієї зброї ми маємо справу з таким видом панування, яке на відміну від інших видів панування (фінансово-економічного, політичного, мілітаристського тощо) має на меті саме керування свідомістю. Управління свідомістю досягається за допомогою цілого ряду факторів та засобів, найважливішим з яких є використання мультимедійних технологій, тобто Інтернету [87, с. 142].

Суспільну думку можна формувати і навіть управляти нею. Для цього потрібно використати деякий важіль впливу. На сьогоднішній день подібних важелів існує багато, але основні з них — ЗМІ, компетентні та авторитетні особи, PR і реклама. Найпотужніший вплив на суспільну думку чинить реклама. Вона орієнтована на підсвідомість людини: її емоції і почуття.

Реклама здійснює одразу подвійний вплив: на рівні рекламованого об'єкту і на рівні ситуативної моделі поведінки, котра засвоюється підсвідомо [46, с. 184]. Вплив телереклами пов'язаний з постійним впливом на психіку і напрямом думок глядача. Людина не встигає переробляти масив пропонованих даних. Однакова інформація, що потрапляє в голову кожного, змушує усіх думати і діяти за єдиною схемою. Створюються певні образи, які сприймаються людиною і цілими соціальними групами, особисті думки замі-

нюються нав'язаними. Подібний механізм є єдиним як для комерційної реклами, так і для політичної реклами або пропаганди. Г. Шиллер зазначав, що реклама, здебільшого, не демонструє споживчі якості товару, а нав'язує певне уявлення про стиль життя, потреби в цьому товарі для підтвердження певного соціального статусу [184, с. 72]. Для поліпшення сприйняття реклами її творці намагаються сформувати в глядача гарний емоційний фон. Такий прийом дає можливість підвищити рівень запам'ятовування пропонованої інформації. 45 % інформації про емоції передаються зоровими сигналами, а 17,6 % — слуховими. Використовуючи комбінацію зорових і слухових впливів, можна підсилити позитивний емоційний фон сприйняття реклами [8, с. 162]. Мета більшості рекламних роликів — продати рекламований товар максимальному числу покупців, при чому інтереси останніх не враховуються.

Отже, як реклама, так і розважальна індустрія, маніпулюють свідомістю людей, створюючи і нав'язуючи вигаданий стиль життя, що може мати негативні наслідки для суспільства.

Ще одна із загроз інформаційній безпеці України, на якій слід зупинити свою увагу, є маніпулювання суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або неупередженої інформації.

Сучасний український філософ П.М. Лісовський під маніпуляцією розуміє «...певні способи соціального впливу на людину, керування нею за допомогою засобів масової інформації, економічних, політичних, соціальних та інших засобів з метою нав'язування відповідних ідей, цінностей, форм поведінки тощо. Причому цей вплив (як особливий стан, в якому поведінка одного суб'єкта змінюється діями

іншого) досить часто є латентним (прихованим) для того, на кого він спрямований [87, с. 10].

В інформаційному аспекті маніпулятивний вплив є особливим видом інформаційного впливу, при якому інформація виступає як засіб примушення особистості до здійснення вчинків, які є невластивими або неприйнятними для неї.

В Оксфордському тлумачному словнику англійської мови слово маніпуляція трактується як поводження із об'єктами зі спеціальним наміром, особливою метою, як ручне управління, ручні дії. У переносному значенні Оксфордський словник визначає маніпуляцію як акт впливу на людей або управління ними зі зневажливим контекстом, як приховане управління чи обробка [177].

У загальному випадку маніпуляція може призвести до таких наслідків руйнування людської свідомості:

- некритичне сприйняття інформації та подій, що відбуваються;
- неадекватне розуміння ситуації;
- байдуже сприйняття подій;
- викривлення уявлень про події;
- маніакальне споживання інформації;
- страх перед інформацією (інфофобія) тощо.

Небезпека реалізації інформаційних загроз значно зростає через застосування різноманітних методів, методик і прийомів маніпулятивного інформаційно-психологічного впливу з урахуванням їх дії на суспільну та індивідуальну свідомість.

Під негативними технологіями маніпуляції суспільною свідомістю будемо розуміти можливі деформації системи масового інформування і поширення дезінформації, які

ведуть до потенційних порушень суспільної стабільності, нанесення шкоди здоров'ю і життю громадим, унаслідок пропаганди чи агітації, що збуджують соціальну, расову, національну чи релігійну ненависть і ворожнечу. Ці впливи, усвідомлювані чи неусвідомлювані, як показує життя, можуть призводити й у дійсності призводять до серйозних порушень психічного і фізичною здоров'я громадян, розмиванню природних і культурно заданих норм поводження, до росту ризикованих соціальних і особистісних ситуацій.

2.2. Концептуальна модель квантової філософії в контексті кібербезпеки

Сучасний розвиток інформаційних технологій, що використовує в критеріальній основі кожна особа, держава та в цілому соціум, значною мірою сприяє зміцненню глобального іміджу в постсучасності. При цьому, метою глобального іміджу є забезпечення ефективності та збалансованої діяльності світової політики як на державному рівні, так і у громадському житті з подальшим використанням ціннісно-смислових пріоритетів у життєвих імперативах.

Як свідчить вітчизняна практика, основною причиною, що розкриває, зокрема розвиток іміджу держави, є відсутність законодавчо врегульованих механізмів забезпечення відповідних інформаційних обмінів. Саме такі комунікативні зв'язки здійснювали б якість адміністративно-правових рішень у системі іміджу державної політики. Адже модернізація державної політики в Україні прогнозує «створення дієвих комунікативних підрозділів замість діючих відділів із взаємодії з громадськістю, яких на Заході давно вже не існує: громадяни — платники податків, вважають недоцільним витрачати спільні кошти на власну рекламу» [2, с. 18]. З

огляду на це, в Україні поки що відсутній системний інформативний характер стосовно убезпечення громадськості та налагодженні поліфункціональних оперативних зв'язків із засобами масової інформації як система превентивних заходів енергетичної безпеки. Тому, в сучасних умовах інтеграції з усім світом набувають іміджу ті країни, в яких поруч із зростанням економічного потенціалу та якості життя, належне місце посідає духовний капітал мудрості її особи. При цьому, моральна свідомість, в якій наріжним каменем є гідність, відіграє консолідуючу роль у сучасному інформаційному соціумі як психоаналітична складова енергетичної безпеки.

Так, наприклад, у Німеччині через мережу Інтернет приймаються прохання від студентів про надання їм фінансової допомоги. «Впровадження служби планування поїздок призвело до 15-відсоткової економії всіх транспортних витрат і до 50-відсоткової економії адміністративних витрат» [185, с. 463].

У свою чергу, в Естонії функціонує інтернет-портал «сьогодні вирішую я», за допомогою якого громадянин республіки може взяти участь в управлінні державою — висловити свою думку про поточні процеси у країні, запропонувати поправки до законопроектів тощо. Цей портал також дозволяє користувачу голосувати [185, с. 465].

Мотиваційні передумови глобального іміджу

Визначальну роль у процесі глобального іміджу як світового впливу відіграє мотиваційні передумови, що створюють сукупну матрицю рушійних сил, які спонукають людину (людей, людство) до виконання відповідних дій. З огляду філософії людини мотивація — це діалектичний процес необхідного усвідомлення вибору того чи іншого

типу діяльності в результаті всебічного впливу зовнішніх (стимули) і внутрішніх (мотиви) факторів.

З огляду глобального іміджу мотивація визначається як функція управління (керівництво, контроль), завдання якої — створити у підлеглих (впливових людей) стимули до життєвого світу з повноцінною віддачею з метою задоволення потреб та інтересів. Таке мотиваційне ядро сьогодні надзвичайно важливе для країн ЄС та Близького Сходу.

Виходячи із сучасного глобального природоенергетичного комплексу, газова труба, що прокладається через турецький простір, є однією із мотиваційних сил для глобального іміджу. Тому постає нагальне питання, хто ж буде серед країн ЄС та Близького Сходу лідерам «газової труби»? Чому так оперативно Президент Франції Макрон провів переговори з В. Путіним та П. Порошенком? При цьому, саме економічні, політичні, військові мотивації як цільова активність становлять стратегічну панораму в системі глобального іміджу як єдиного діалектично взаємообумовленого соціального організму.

З цього приводу варто акцентувати увагу на те, що Девід Макклелланд виокремлює три основні мотиви досягнення — прагнення домогтись найкращого вирішення складних проблем; мотиви афіліації — потреба в налагодженні шляхетних стосунків з оточуючими; мотиви влади — прагнення впливати на поведінку інших людей. Існують оптимальні співвідношення для тієї або іншої діяльності, проте висока мотивація досягнення у більшості випадків є бажаною і навіть необхідною [20, с. 218].

В 1961 році у своїй праці «Суспільство досягнення» Д. Макклелланд висунув припущення стосовно мотивації, що є досягненням економічного процвітання. На наш по-

гляд, визначивши ступінь виразності відповідного мотиву в суспільстві, можна з вірогідністю передбачати тенденцію капіталу мудрості народів світу. У цій площині на межі соціальних та вітчизняних потреб знаходиться клас «гібридних потреб» — етнічні потреби як потреба «гібридної війни» на Сході України, «оскільки «без потреби слідувати нормам, прийнятим в даному суспільстві, існування соціальних потреб було б неможливим» [156, с. 87].

Місце України у природноенергетичному світовому ресурсі

Сьогодні в надрах України виявлено близько 20 тис. родовищ і проявів 117 видів корисних копалин, з яких 8231 родовищ 97 видів корисних копалин має промислове значення і враховано Державним балансом запасів. Мінерально-сировинні ресурси України значною мірою зумовлюють державний поділ праці. Адже Україна за потенційною вартістю підтверджених видобувних запасів корисних копалин, у надрах займає 12 місце у світі (2,2 % потенційної вартості світових запасів). При цьому, необхідні розвідані родовища, що мають промислове значення, можна розподілити залежно від їх розмірів, якості корисних копалин, екологічних, економічних та інших умов їх промислового використання. Із загальної кількості розвіданих родовищ, що знаходяться в експлуатації, потужні становлять 9,6 %, середні — 27,7 %, малі — 67,6 %. Щорічно видобувається з потужних родовищ понад 51 % мінеральної сировини, 24 — з середніх і лише 25 % — з малих родовищ [160, с. 165].

Разом з тим, визначаючи у світовому процесі необхідно досягти міжнародного консенсусу, на основі якого постає демократична держава саме якість адміністративно-право-

вого забезпечення принципу демократії виступає одним з найважливіших об'єктивних показників успішності міжнародної інтеграції серед країн світу, в тому числі подальшої інтеграції України до ЄС.

Суттєвим моментом забезпечення паливно-енергетичного комплексу України є енергозбереження, модернізація та його реструктуризація, залучення інвестицій тощо. Принагідно зазначити, що нафта з Перської затоки у Європу йде через Суецький канал, так і навколо Африки. Це складає відповідно 11 800 км та 32 000 км до нафтового комплексу в Ротердамі. Шлях доставки нафти через територію Туреччини та України у 2–3 рази коротший. При цьому необхідно враховувати можливість переробки значних обсягів нафти на вітчизняних нафтопереробних підприємствах. Так, відстань транспортування нафти з Кіркука (Іран) до Кременчуцького нафтопереробного підприємства складає 2 930 км, тоді як існуючий шлях постачання нафти з Росії нафтопроводами дорівнює 4 000 км.

У цьому напрямку повинні здійснюватись цільові форми фінансово-економічних механізмів у рамках законодавчих аспектів:

1) податкової політики — шляхом звільнення від оподаткування, податкових знижок, диференційованих податкових ставок, введення пільгових податків та зборів;

2) амортизаційної політики — шляхом установлення скорочених термінів амортизації нової техніки, що підвищує надійність енергопостачання та енерговикористання;

3) страхової політики — шляхом створення та підтримки страхових компаній, які страхують від ризиків стосовно постачання паливно-енергетичних ресурсів, зокрема порушення стабільного енергопостачання;

4) інвестиційна політика — шляхом залучення та заохочення додаткових інвестицій, у тому числі приватних та іноземних, для фінансування проектів, спрямованих на підвищення енергетичної безпеки України.

На сучасному етапі геополітичного та економічного розвитку з огляду нафтогазовидобування та використання існують об'єктивні внутрішні та зовнішні причини загроз, зокрема енергетичній безпеці Україні, серед яких визначальними є:

- недостатня ресурсна забезпеченість власного нафтогазовидобутку через істотне відставання геологорозвідувального виробництва від вимог і потреб розвитку галузі;
- обмеженість джерел надходження нафти і газу в Україну;
- зниження ступеню надійності та технічної безпеки експлуатації нафто- та газопровідної системи. При цьому їх незавантаженість, потужності та низькі темпи реконструкції з метою забезпечення глибини переробки нафти до 75 %;
- успадкованість структури споживання паливно-енергетичної здобутку, яка значною мірою зорієнтована на природний газ і нафту;
- надмірна обтяжливість економіки держави енергетичними виробництвами, що таким чином виснажує природне багатство Землі;
- відсутність пристосованого до ринкових умов і створеного на цивілізованих засадах ринку енергоносіїв [66, с. 57].

Для цього потрібно здійснити диверсифікацію джерел постачання нафти і газу в Україну з Азербайджану, Казахстану, Іраку, Ірану, Сірії, Об'єднаних Арабських Еміратів, Кувейту, Алжиру, Лівії, Нігерії, Тунісу, країн басейну Північного моря (Голландії, Норвегії).

Таким чином, глобальний імідж у сучасному світовому процесі будується на інформаційно-аналітичній підтримці відвернення кризових явищ, що передбачає, в свою чергу, в паливно-енергетичному ресурсі створення методології оцінки ризику як феноменальних рецепцій мудрості особи, держави, суспільства. Це, насамперед, створення систем космічного моделювання та моніторингу методами дисперсії та ентропії, а також формування систем попередження та запобігання загрозам (ризикам).

Міжнародні питання ризиків в енергетичній безпеці

У сучасну епоху глобалізаційних змін актуального значення набувають міжнародні відносини, оскільки світ ризику стрімко еволюціонує. За цих умов важливим постає необхідне усвідомлення саме критеріальної системи оцінювання світових ризиків, що ефективно забезпечує здоров'я та добробут людства (людей, людини) від будь-яких негативних впливів (катаклізмів, катастроф, терактів тощо), а також надає упевненості в майбутньому.

При цьому мають бути різноманітні критеріальні показники рівнів імовірних процесів впливу на свідомість окремої особи, народу, етносу, нації тощо.

У цьому напрямку необхідно розробити методологічні аспекти, в яких мають бути на практиці методики і чіткі рекомендації, пропозиції щодо технологічного (інструментального) характеру визначення (ступеня) ризику.

У свою чергу, за політики-географічним характером світові ризики залежать від ментальної репрезентації в сучасних умовах мультикультуралізму, а саме: свідомості, мови, етносу тощо, в якому символічний капітал культури відіграє провідну роль, що залежить від мудрих рішень окремої особи, народу та суспільства.

Безперечно, що також вплив метеополя на поведінку особи, держави та суспільства має неабиякий характер, оскільки людина за природою сутністно — це відкрита (прозора, явна) космічна інформаційна система, яка має постійно убезпечувати себе від будь-яких загроз з метою вияву ступеню вірогідності відповідних ризиків та їх ідентифікувати (категоризувати, угрупувати, систематизувати).

В контексті викладеного варто зазначити, що міжнародна політична реакція на ризик сприяє зниженню числа повторюваності несподіванок, а також якості убезпечення особи, держави та суспільства від будь-яких загроз (негативного впливу). Для цього потрібно розробити концептуальні дії щодо превентивних заходів у системі ризикових процесів, а саме: системно аналізувати, виявляючи несподівані події і використовувати дисперсійний та ентропійні методи математичного моделювання в теорії випадкових функцій і надавати критеріальну оцінку ефективності в неймовірних діях, формувати феномен імперативу модернізації страху.

Імператив модернізації страху

Сучасні нанотехнології хоч і дозволяють людству повною мірою полегшувати життя саме на фізичному рівні. Проте інформаційний простір для критичного мислення таких людей має обмежений характер, що когнітивно прискорює ризикові процеси в людському організмі і у підсвідомих актах мозку накопичується ентропійна енергія страху. Таким чином, не генерується інноваційна матриця добротворчого потенціалу окремого суб'єкта, що визначає параметри оптимального розподілу людського капіталу.

Адже в сучасних умовах світових інформаційних війн феномен імперативу модернізації страху має нагальне значення, оскільки постає гостра проблема нерозповсюдження

зброї масового знищення. У цьому сенсі, невід'ємну роль відіграє такий чинник як розподілення світових енергозберігаючих ресурсів у вигляді природної сировини. Саме з цією метою США активно застосовують економічні санкції проти Росії, Північної Кореї, Ірану тощо.

Особливості математичних методів у ризикових процесах

У цьому сенсі є спроба обґрунтування доцільності використання математичних методів для аналізу ризикових процесів у міжнародній системі та глобальному розвитку. Адже використання математичного інструментарію передбачає аналіз чисельних еквівалентних складових ризикових процесів у міжнародних питаннях. При відсутності таких компонентів, вони вводяться штучно методом експертних оцінок чи парним порівнянням.

Для аналізу основних ознак глобальних ризиків варто використовувати такі міжнародні інституції як: «Навчально-науковий інститут міжнародних відносин та соціальних наук Міжрегіональної академії управління персоналом» та «Міжнародну кадрову академію», що досліджують особливості превентивних процесів у країнах світу.

При цьому слід використовувати наступні критерії оцінювання:

- ментально-ціннісні орієнтири. Розглядається демократичний характер і надійність державної системи, незалежності, ефективності адміністративно-правового забезпечення, а також демократичний контроль над військовими, правоохоронними формуваннями та спецслужбами;
- освітянський процес, у якому вивчається розвиток освітньої системи та участі осіб серед числа вітчизняних та іноземних студентів;

– інформаційне суспільство. Оцінюється духовний капітал особи, держави, в якому знання є рушійною інтелектуальною силою;
– корупція (спекуляція). Досліджується громадська думка стосовно корумпованості влади, бізнес-інтереси провідних політиків країн, якість антикорупційних ініціатив.

Використовуючи базу оцінок і рейтингів країн, зокрема Німеччини, Чехії, Польщі тощо, можна визначити загальні тенденції протікання превентивних процесів у будь-яких країнах світу. Враховуючи циклічність в координатах людиноцентризму та людинокосмізму, а також впливу метеополя на свідомість як експертних оцінок, варто обрати метод тренд-соціокомунікативного моделювання, що основується на «рядах Фур'є». Цей «ряд Фур'є» є способом здійснення довільної складної функції сумою простіших. У загальному випадку кількість таких функцій може бути нескінченною, що враховується при розрахунку, оскільки вищою стає кінцева точність представлення даної функції. В більшості випадків якістю найпростіших використовуються тригонометричні функції синуса і косинуса. Саме в цьому випадку ряд Фур'є називається тригонометричним, а обчислення такого ряду вважається розкладом на гармоніки.

При цьому, ряд значень, узятих за часовий період, називається числовим рядом, що складається з наступних складових:

- тренду, що вказує на загальний тип змін в історичних даних;
- метеоколивань навколо тренду, що виникають на регулярній природній основі (кліматичних умовах та географічному середовищі);

- циклічних коливань у вигляді пасіонарності та біфуркацій як відповідних фаз зі стандартним циклом ділової активності;
- випадкових коливань в ентропійній системі. Це непередбачені випадково-закономірні коливання, що є присутніми у більшості реальних часових рядів.

– Аналіз таких коливань можна використовувати для обчислення ймовірних помилок і оцінки надійності застосування моделі прогнозування.
– Таким чином, універсальна форма запису часового ряду має вигляд:

$$Y(t) = T(t) + S(t) + C(t) + \xi(t),$$

в якому:
$T(t)$ — тренд (довгостроковий вектор розвитку);
$S(t)$ — сезонна компонента (вплив метеополя);
$C(t)$ — циклічна компонента;
$\xi(t)$ — ентропійна компонента (випадкові коливання).

Динамічні ряди описують зміни часових даних. У більшості випадків аналіз таких моделей зводиться до виділення детермінованої і випадкової складової в системі ентропії. При аналізі детермінованої складової виділяють наступні компоненти:

– тренд (t_r);
– метеоскладову (S);
– циклічну складову (С)

$$d = t_r + S + C$$

У трендовій моделі знаходять математичний вираз, в якому значяться необхідні характеристики. Якщо коефіцієнт детермінації більший за |0,5|, то додається лінія тренду та визначається форма рівняння. Якщо коефіцієнт детермі-

нації менший за |0,5|, то проводиться згладжування вихідного ряду. Після згладжування за допомогою пакету додається лінія тренду та визначається форма рівняння. Вибирається найпростіша форма рівняння тренду (іноді за рахунок погіршення коефіцієнту детермінації). Якщо спостерігається лінійна залежність, тоді або залишається знайдена форма рівняння тренду, або проводиться лінеаризація та регресійний аналіз.

Із вихідного ряду видаляється тренд і залишаються лише метеоколивання, вивчають їх і підбирають математичний закон їх зміни.

Прогнозується поведінка особи та окремої держави як результативна ознака за узагальненим рівнянням, що складається з трендової, циклічної та ентропійної складових.

Циклічна компонента вивчається тільки для рядів, які не мають тренду. Тому у дослідженні, при аналізі циклічної компоненти було видалено тренд за формулою:

$$Z(t) = Y(t) - t_r$$

Після видалення тренду необхідно перейти від абсолютного часу до штучного.

Доцільним є заданий час перевести у радіанну міру за формулою:

$$t^* = \frac{2\pi}{N} t.$$

Оскільки недоліком авторегресії є вплив метеополя на свідомість людини (людей, людства) як вияву космогенних факторів, то за формулою Беселя знаходяться коефіцієнти b_k, a_k, a_0, при обмеженні по кількості гармонік — N_2.

$$a_0 = \frac{1}{N} \sum_{i}^{n} = 1 Z_t$$

$$a_k = \frac{2}{N}\sum_i^n = 1Z_t^* \cos 1Ct \text{ [30, с. 752].}$$

Таким чином, побудова стратегічної панорами в іміджелогії країнознавства супроводжується застосуванням системно інтуїтивної та раціональної компонент феноменальної свідомості, а також прийомів математичного моделювання. При цьому повинна зберігатись логіко-семантична структура такої феноменальної свідомості як суттєвої потреби людини в соціумі

Перспективи бачення нового космічного порядку в філософії країнознавства: кібербезпечні виміри

Одним із основних пріоритетів глобалізованого світу є процес створення кібербезпеки та впровадження її в свідомість кожної особи, держави та соціуму. Виходячи із нестабільності соціального розвитку, варто визначити, що інформологія — це системно-діяльнісне явище, спрямоване на оволодіння інформаційно-інтелектуальним ресурсом у лексико-семантичному полі розширеної свідомості.

У цьому сенсі кібербезпека як структура основи інформології містить у собі розробку і реалізацією інноваційних технологій, систем акумуляції і передачі даних, що забезпечують вичерпне та своєчасне використання інформації та знань з метою убезпечення від будь-яких загроз у різних сферах діяльності людини (людей, людства). Іншими словами, кібербезпека означає — створити ефективно діючі умови для вирішення особистих і суспільних проблем. Адже сьогодні інформологія виступає як важливий інноваційний феномен, що перебуває в процесі глобалізації. Це, в свою чергу, надає можливість кібербезпеці як соціотехнічному пріоритету світу виділити чотири основні пріоритетні напрямки: електронізацію, комп'ютерізацію, медіатизацію та інтелектуалізацію. Також це є критеріальним операто-

ром ентропії (невизначеності досвіду з кінцевим числом можливих результатів) у теорії випадкових функцій.

При цьому, електронізація є широкою можливістю насичення людинорозмірних систем відповідною технікою у космічній інформаційній системі, що облегшує доступ до певної інформації і, таким чином, кібер-убезпечує діяльність людини. Адже сьогодні без комп'ютера сам процес інформології уявляється немислимим.

В силу означеного глобальна й мобільна комп'ютерізація веде до наступної стадії розвитку кібербезпеки — це медіатизація, що є процесом комунікативних взаємодій людей і географічних регіонів на основі убезпечення новітніми інформаційними технологіями.

Крім того, інтелектуалізація як людський ресурс кібербезпеки породжує проблему не управління інформацією, а проблему інформаційного управління системами різного рівня складності. Саме формування нового космічного порядку, в якому має місце трансформація знань в інформаційні ресурси з огляду врахування рівня розвитку всіх сегментів інформології, сприяє вирішенню насущних завдань.

За цих умов і складається новий космічний порядок у системі кібербезпеки, в якому здійснюється модернізація пріоритетів світової політики на базі нових технологій та інформаційної структури.

Відображення модернізації в постучасності визначається здатністю до постіндустріальних трансформацій на основі діалектичного поєднання локального й універсального, зміцненням соціально-політичних і культурних особливостей, збереженням суверенітету, національної самобутності.

Разом з тим не можна не визнати, що сучасне становище ускладнюється нерозумінням того, що причина всіх

криз (небезпек, загроз) криється в духовно-моральному паралічі суспільства, людини. При цьому вирішальний конфлікт на початку XXI полягає в суперечностях соціуму промислової цивілізації й соціуму, культури.

Роль кібербезпеки саме є у системі знань набуває на етапі постіндустріального розвитку соціуму фундаментального значення. Оскільки на цьому етапі система знань надає можливість творити гуманне творіння, в якому найважливішою новою якістю в кібербезпеці постала здатність вчитись навчатись. Адже сучасна інформаційна техніка та технології спрощують доступ до знань, забезпечують її вільну циркуляцію як вияв екзистенціального імперативу інноваційної людини.

Якщо припустити, що формування соціальної природи людини з відповідним типом знань завершується на індустріальному етапі розвитку суспільства, структурними одиницями якого є національної держави, то сьогодні відбувається активне творення віртуальної або «кібер»-орієнтованої природи людини, націленої на майбутнє вже в масштабах глобального планетарію.

Внаслідок цього процесу відбуваються грандіозні трансформації, зокрема, формується радикальне відчуження знання від субстанційної природи, яка народжує і народженої як Природи природного світу. При цьому, варто означити вчення французького дослідника Жана Бодріяра про симулякри, зокрема, симулякри другого та третього рівня («виробництво» та «симуляція» відповідно) [22, с. 177].

«Не можна не помітити: сьогодні відбувається нічим не прикрите тяжіння до віртуального та пов'язаних з ним технологій. І якщо віртуальне дійсно означає зникнення реальності, то воно, мабуть, і є поки що негативно усвідомленим,

але сміливим специфічним вибором самого людства. Людство вирішило клонувати власну тілесність та власне майно в іншому, відмінному від попереднього всесвіті, воно, по суті, вважалося зникнути як людський рід, щоб закарбувати себе в роді штучному, значно більш життєздатному та ефективному... Поле віртуального — це ніщо інше, як область, де різноманітні предмети вимірюються однією й тією самою мірою, якою є подвійність, комбінація нуля та одиниці» [22, с. 154].

Отже, інтернаціоналізація як інфоглобалізація є фактором міжнародної інтеграції економічних, політичних і соціальних систем країн у світовий контекст та основним ретранслятором глобальних цінностей, підходів та технологій на рівні тієї чи іншої держави.

2.3. Комерційна торгівля в інтернет-ресурсах

На сучасному етапі інформаційного розвитку особи, держави та суспільства Інтернет стрімко ввійшов у життєвий світ і почав змінювати реальність людини. Саме ця стрімкість та масштабність змін, що внесли у суспільство сучасні інформаційні технології є актуальним з огляду правового поля як занепокоєння юристів і людської спільноти в цілому. Адже нові інформаційні технології породжують певні явища, зокрема комерційну торгівлю в Інтернет-мережах, які нерідко знищують основні ціннісно-смислові критерії людського життя, а саме: честь, гідність, мораль, довіру, а також правову культуру. В силу розширення системи масового інформування, зростання кількості комунікативних потоків, прискорення інформативного обміну відбулись зміни уявлень окремої особи, держави та суспільства про реальну дійсність. Отже, Інтернет, який орієнтується

на зростання можливості здійснення комунікації, є тим медіумом, що перетворює систему соціальних інститутів у своєрідну віртуальну реальність та неможливість людині достовірно оцінювати відповідну інформацію.

Сучасні мережі Інтернет використовують комерційний прийом фабрикації фактів лише при наданні недоступної інформації. Відбір подій реальності є одним із головних прийомів програмування мислення — контролю над інформаційним раціоном людини. Це відмова від цілісного, різнобічного надання інформації. Характерною ознакою прийому є приховування (замовчування) інформації і створення таким чином віртуальної реальності. Відповідним чином використовуються в Інтернеті також прийом напівправди, коли з метою забезпечити довіру користувачів об'єктивно та ретельно висвітлюють конкретні меншовартісні деталі і водночас замовчують важливіші факти, або ж створюють загальну інтерпретацію подій.

Реклама як джерело фінансування Інтернет-компаній

В означеному дослідженні однією із провідних форм комерційної торгівлі в Інтернет-мережах є реклама. При цьому, основним джерелом фінансування Інтернет-компаній є рекламні оголошення, які розташовуються залежно від рейтингу відвідування певного сайту. Як правило, Інтернет-компанії беруть плату із замовників, які рекламують свої образи через його мережу. Суть реклами полягає в пропонуванні широкому колу потенційних споживачів певного товару (послуги), який або тільки з'являється на ринку і намагається «заявити про себе», або ж намагається розширити коло своїх споживачів шляхом «просування бренду». Проте це абсолютно неможливо без використання об'єктів авторського права, оскільки разом із торговельною

маркою, фірмовим найменуванням чи географічним позначенням це формує оригінальність, неповторність та творчий характер як обличчя товару (послуги) Інтернет-компанії, що сприяє лояльність споживача тощо.

Згідно Закону України «Про рекламу», реклама — це інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформувати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких осіб товару. Для того, щоб створити якісну рекламу, необхідно прикласти певні творчі зусилля. Ці зусилля приводять до того, що реклама стає творчим добутком, вираженим у якій-небудь об'єктивній формі, а значить — об'єктом авторського права.

За цієї причини, відносини, що виникають у зв'язку зі створенням і використанням творів, регулюються Законом України «Про авторське право і суміжні права». у даному випадку можна виділити два основних питання: питання захисту авторських прав на рекламу і питання використання в рекламі творів третіх осіб.

Відповідно до зазначеного Закону авторське право поширюється на твори науки, літератури і мистецтва, що є результатом творчої діяльності, незалежно від призначених намірів твору, а також від способу його ознака результату, що виражається в оригінальності твору. Саме тому в рекламі, як і в будь-якому творі, авторським правом не охороняються ідеї, методи, способи, концепції, факти, а також інші неоригінальні елементи, що можуть з'явитися при рівнобіжній творчості.

Слід зазначити, що інформація в комерційній торгівлі Інтернет-мережах не є об'єктом авторського права, оскільки рекламне повідомлення не виражене в оригінальній формі,

а лише повідомляє про гідні наміри товару, то воно не охороняється авторським правом.

Проте, згідно тієї ж ст. 13 Закону не вважаються рекламою:

- оприлюднення, виголошення у програмі, передачі імені, найменування спонсора, об'єктів права інтелектуальної власності;
- трансляція соціальної реклами за умов безкоштовного розповсюдження трансмедією;
- анонси власних програм, передач телерадіоорганізації.

У ст. 4 Закону України «Про рекламу» йдеться про використання у рекламі об'єктів авторського права і (або) суміжних прав, що здійснюється відповідно до вимог законодавства України про авторське право і суміжні права (Закон України «Про авторське право і суміжні права» від 23.12.1993 № 3792-XII).

При цьому варто акцентувати увагу на тому, що реклама у будь-якій формі є об'єктом авторського права особи, яка її створила. Цей висновок випливає з аналізу ст. 8 Закону України «Про авторське право і суміжні права», згідно з якою охороні за цим Законом підлягають всі твори, зазначені у ч. 1 цієї статті, як оприлюднені, так і не оприлюднені, як завершені, так і не завершені, незалежно від їх призначення, жанру, обсягу, мети (освіта, інформація, Реклама, пропаганда, розваги тощо).

Таким чином, можна дійти висновку, що реклама після отримання об'єктивної форми (рекламного ролику, салогана, музичної фрази тощо), стає об'єктом авторського права за умови результату творчої праці фізичної особи (згідно із ст. 1 Закону України «Про авторське право» автор — фізична особа, яка своєю творчою працею створила твір), яка міс-

тить у собі нове та оригінальне. Це дає підстави вважати, що реклама за умови наявності у відповідного об'єкта реклами таких ознак, підпадає під дією Закону України «Про авторське право». Іншими словами, в автора існує єдиний обов'язок — довести, що його реклама — це оригінальний результат творчої праці порівняно з існуючими.

У цьому сенсі варто наголосити, що виникнення авторського права і виникнення реклами в даному випадку не є тотожними. Як відомо, авторське право виникає з моменту створення твору. У визначенні поняття реклами нової редакції Закону використовується дієслово завершеного виду «розповсюджена» замість «яка розповсюджується», а отже інформація про особу чи товар буде вважатись належною рекламою в силу її достовірного донесення до споживача.

Крім того, з метою створення нового рекламного продукту рекламодавці укладають відповідні угоди з приватними компаніями, що спеціалізуються на даному виді послуг — рекламними агентствами (виробник реклами). Згідно законодавства зазначається, що особисті немайнові права автора є невідчужуваними, за винятками встановленими законом (наприклад, у випадку смерті автора означені права переходять до спадкоємців або правонаступників). Отже, майнові права укладаються у виключному праві на використання твору в будь-якій формі і будь-яким способом. Тому ніхто не може використовувати рекламний твір або його частину, будь-то рекламний ролик, фото, малюнок, образ або який-небудь інший об'єкт без дозволу правовласника.

Серед об'єктів інтелектуальної власності можна виділити об'єкти, що представляються в рекламі (товарні знаки, фірмові найменування, об'єкти патентних прав), або вико-

ристовуються при її виготовленні (твори науки, літератури і мистецтва).

Безперечно, саме рекламодавець є правовласником у відношенні товарного знаку, зареєстрованого у встановленому порядку. Однак в рекламі незаконно використовується товарний знак, що належить іншій особі. Найчастіше це відбувається тоді, коли рекламодавець не знає про наявність у третьої особи прав на представлене в рекламі позначення. При цьому, порушенням прав власника товарного знаку визнається будь-яке несанкціоноване ним введення в господарський оборот товару, позначеного точно таким же або подібним з ним до ступеня змішання позначенням, або самого позначення у відношенні однорідних із зазначеними у свідоцтві товарами.

Закон України «Про рекламу» не допускає і несумлінну рекламу. Що вводить споживачів в оману щодо рекламованого товару за допомогою імітації (копіювання або наслідування) загального проекту, тексту, рекламних формул, зображень, музичних або звукових ефектів, використовуваних у рекламі інших товарів. Тому, в деяких випадках використання позначень (звукових, образотворчих тощо), що уже використовуються в рекламі іншими, не допускається.

Порушенням Закону України «Про рекламу» є також недостовірна реклама, в якій присутні відомості, що не відповідають дійсності, зокрема, у відношенні товарного знаку. Наприклад, виробник не вправі вказувати в рекламі за допомогою попереджувального маркірування (букви «R» у кружку) або іншим способом на те, що знак зареєстрований, якщо в дійсності не внесений до Державного реєстру товарних знаків.

У зв'язку з вищесказаним можна порадити виробникам використовувати тільки свої позначення і піклуватися про

їхню охорону. Закон України «Про товарні знаки» надає потужні можливості для захисту законних інтересів у сфері реклами, оскільки як товарні знаки можуть виступати і реєструватися не тільки логотипи, назви, етикетки, але і рекламні салогани, звукові позначення. Це дозволяє виробникам ефективно просувати свій товар на ринок, використовуючи в рекламі товару оригінальні позначення. Що є об'єктами виключних прав. Наприклад, як товарний знак для кави був зареєстрований фрагмент твору П.І. Чайковського.

У рекламованих товарах часто втілюються об'єкти патентних прав: винаходи, корисні моделі, а також їхніх складових частин, промислові зразки. В Інтернет-мережній рекламі вбачаються лікарські препарати, медичні пристрої, що запатентовані як промисловий зразок.

Згідно до патентних законів патентовласникові належить виключне право на використання охоронюваних патентом винаходи, промислові зразки, корисні моделі.

Сама реклама продукту, що містить захищений патентним законодавством об'єкт, може порушенням виключних прав патентовласника, якщо здійснюється без його дозволу. Дозвіл оформляється укладанням ліцензійного договору. якщо сторони вважають цю умову істотною. Практика реклами свідчить, що більшість реклами виробляється спеціалізованими юридичними особами, котрі здатні творчо працювати та мають необхідні знання для створення реклами певного виду.

Контроль якості та безпеки лікарської продукції

Контроль за обігом лікарських засобів у рекламних Інтернет-мережах є важливою потребою адміністративно-правового регулювання в сфері охорони здоров'я, оскільки значна частина лік випускаються з порушенням діючих

норм, є підробками, або такими, ефективність яких не відповідає заявленим виробниками показникам. З цією метою має діяти на належному рівні державна служба України щодо лікарських засобів. Основними завданнями держслужби України є:

- внесення пропозицій стосовно формування державної політики у сферах контролю якості та безпеки лікарських засобів, медичних виробів, а також ліцензування господарської діяльності з питань виробництва лікарських засобів. імпорту лікарських засобів, оптової та роздрібної торгівлі лікарськими засобами;
- реалізація державної політики у сфері державного контролю якості та безпеки лікарських засобів, оптової та роздрібної торгівлі лікарськими засобами [140].

Крім того, поруч з трьома вище зазначеними об'єктами контролю у рекламних Інтернет-мережах необхідно виділити і протидію ВІЛ-інфекції / СНІДу та інших соціально небезпечних захворювань. Така правомірна діяльність спрямовується і координується Кабінетом Міністрів України через Віце-прем'єр-міністра України — Міністра охорони здоров'я України.

Міжнародно-правові гарантії прав людини в Україні

Правова проблема повноти і гарантованості людини потребує в сучасному інформаційному світі глобального значення. Тому, зокрема щодо комерційної торгівлі в сучасних інтернет-мережах, світова спільнота намагається створити єдині правила соціальної та правової захищеності громадян, уніфікувати, прийняти єдині стандарти і процедури, які б сприяли визнанню гідності та честі.

У цьому сенсі важливого значення в забезпеченні прав і свободи людини набувають міжнародно-правові гарантії,

що передбачені міжнародними угодами, конвенціями, деклараціями та іншими міжнародними документами. Також у науковій літературі подано таку класифікацію міжнародно-правових гарантій як: ратифікація пакті і конвенцій про права людини, міжнародно-правовий контроль, міжнародно-правові санкції, міжнародно-правовий судовий захист прав людини, координація сумісних зусиль держав, міжнародно-правові наради і зустрічі з прав людини [115, с. 455].

На нашу думку, міжнародні нормативно-правові гарантії прав людини — це всебічна координована система, в якій міжнародно-правові акти містять правила та норми діяльності, формулюють права та обов'язки відповідних суб'єктів. Такими актами варто вважати конвенції, пакти, угоди, договори тощо, а також міжнародні документи, які не подають норм, правил поведінки (зокрема, декларації, заяви, меморандуми).

Крім того, згідно зі ст. 21, громадяни будь-якої сторони — учасниці договору на території будь-якої іншої сторони не обкладаються іншими зборами, податками, митом або нарахуваннями будь-якого роду [44, с. 57]

Оскільки сьогодні весь світ переходить на цифровий вид економіки, то саме концептуальне впровадження інтерактивних форм підприємницької діяльності через інтернет-мережі є раціональним інтересом, на що, в першу чергу, мають цілеспрямувати свою ефективну діяльність митні служби. Проте, невизначеним постає актуальне питання криптовалюти як правової ентропії, що становить електронний вид в колообігу грошової одиниці в сучасному інформаційному соціумі.

Відповідно до цього варто додати, що правова держава делегує фактично функції правотворчості численним гос-

подарюючим суб'єктом. Тому услід за формуванням геоекономічної і геофінансової світових популяцій формується новітня модель світової правової системи, що опосередковує цей процес. Саме за цих умов трансграничні фінансові потоки буквально захлеснули світ. При цьому виправдання традиційних правових моделей породжує застій у мисленні окремих правових суб'єктів, що спеціалізуються в економіці, фінансах, промисловій політиці тощо.

Отже, в сучасних умовах комерційних інтернет-мереж проблема правового регулювання мають чітко позначати три яруси: національне право. міжнародне право і глобалізоване право з особливим характером взаємодії між ними.

ООН як орган світової виконавчої влади в мережевому суспільстві

Сучасне мережеве суспільство — це сукупна матриця нових медіа, яка стверджує, що нові методи комунікацій у світі цифрових технологій дозволяють певним групам осіб збиратися разом online і ділитися думками, інформацією, продавати і обмінювати товари і інформацію. також дозволяє значній кількості людей мати право голосу у своєму співтоваристві і у світі в цілому. Найважливіша структурна особливість нових медіа — інтеграція телекомунікаційних технологій. Отже, мережеве суспільство може бути визначене як соціальне формування з інфраструктурою соціальних мереж і медіа мереж, що активує їх основний спосіб організації на усіх рівнях (на особистому рівні, груповому, колективному і громадському).

У зв'язку з цим необхідно зазначити, що на сучасному етапі інформаційного розвитку особи, держави та суспільства органами світової виконавчої влади є така потужна міжнародна установа як Організація Об'єднаних Націй

(ООН), у структурі якої створена і почала функціонувати низка виконавчих структур, на кшталт Ради безпеки ООН, ЮНІСЕФ, у європейському контексті до них слід віднести ОБСЄ, Військово-політичний союз НАТО та інші установи.

Саме Центр ООН з прав людини. Комісія ООН з прав людини, Верховний Комісар ООН з прав людини, Комітет із ліквідації расової дискримінації, Комітет проти тортур, Комітет з прав людини, Комітет з економічних та культурних прав, Міжнародний арбітраж, Міжнародний арбітраж, міжнародний суд ООН, Європейський суд з прав людини тощо є міжнародними органами зі спостереження, контролю за дотриманням прав людини (комісії, комітети) та із захисту цих прав (суди).

У зв'язку з цим слід підкреслити, що в Україні визнається пріоритет міжнародного над національним. Адже ст. 9 Конституції України визнає, що чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України. Проте, це конституційне не має механізму реалізації. Жоден судовий орган не прийме позову від громадянина країни з посиланням на міжнародний договір, положення якого порушуються у правозастосовній практиці, оскільки міжнародний механізм захисту прав людини досить розгалужений.

2.4. Контррозвідувальна діяльність у вирішенні правових інтересів сучасної України

Сьогодні надзвичайно актуальною є концептуальна модель контррозвідувальної діяльності у вирішенні правових інтересів України, оскільки контррозвідувальна система слугує феноменальною основою для переходу на принци-

пово новий, ефективно діючий правовий захист інтересів України. Потреба та необхідність обраної теми обумовлена формуванням незалежних (автономних) структурних організацій, підрозділів та відповідних служб (керівних центрів, відділів, секторів тощо) на правових засадах структурно-функціональної методології. Це забезпечує нові правові механізми управління і планування як якість ефективного прогнозування та превентивного реагування на зміни суспільних обставин на рівні окремої особи, держави та суспільства, а також виконання нових завдань за рахунок інтелектуального перерозподілу наявних правових сил. Відповідно до цього контррозвідувальна діяльність передбачає: якісне формування організаційно-штатних структур у правовому полі персоналу на основі аналізу реальної обстановки; перекваліфікацію працівників; проведення комплексу заходів із психологічної перебудови та адаптації персоналу до нових реалій і умов працездатності; перегляд і приведення у відповідність до сучасних правових вимог, форм і методів атестації працівників.

Оскільки означена тематика в правовій державі досить складна і не потребує в широкому обсязі оприлюднення, а обмеженого характеру, то варто апелювати до публікацій таких сучасних дослідників та аналітиків як: З. Бжезинського, В. Бриля, З. Гом'єн, Б. Кларка, П. Лісовського, В. Остроухова, К. Шрідхара, О. Фармагея, С. Гордієнка тощо.

При цьому, особливої ваги набуває аналіз проблем вищої освіти — В. Андрущенко, Л. Губерський, В. Кремінь, М. Курко, М. Згуровський, І. Стеценко, О. Рябека тощо, що певною мірою торкаються означеної теми.

У сучасних умовах інформаційного суспільства контррозвідувальна діяльність є одним з важливих напрямків ро-

боти спеціалізованих служб, органів та різних форм організацій. Саме компетентний підхід контррозвідки, форми та засоби її діяльності закріплюються рішеннями керівництва, що в цілому ефективно як надійний юридичний захист створює правову базу.

Інтерес як правове коріння контррозвідувальної діяльності

У цьому аспекті варто зазначити поняття «інтерес», що рухає суспільство вперед. Як наголошує дослідник А.Г. Здравомислов: «інтерес» є вихідний момент окремого явища, окремої події, певної послідовності подій, основа ідеології, важливий стимул розвитку наукового пізнання [56, с. 178]. За таких умов в українській науковій думці знайшов поширення мотиваційний підхід до поняття «інтересів», який має досить універсальне поняття та різнобарвний зміст як «спонуки людської діяльності, зумовлені об'єктивними потребами. Мотиви безпосередньо передують конкретній поведінці людини і фактично пов'язані з нею» [129, с. 244]. Адже мотиви передбачають не лише задоволення тієї чи іншої потреби, а й вибір засобів для цього, оскільки виявляються у конкретних вчинках і поведінці людей як здійснення певної мети.

В системі контррозвідувальної діяльності необхідно озвучити специфіку саме закону інтересу, що полягає в його класифікації на інтереси розвитку, функціонування і гальмування. Інтереси розвитку пов'язані саме з тим, що коренями всякого розвитку є протиріччя. Взаємопритяжіння і взаємовідштовхування, взаємопроникнення і взаємовиключення альтернативних протилежних шляхів, форм, методів і засобів розв'язання протиріч між умовами, цілями, ідеалами і умовами існування правових суб'єктів веде до

удосконалення системи суспільних зв'язків і правових відносин, її оновленню.

Але не треба забувати про органічну цілісність процесів розвитку, функціонування і гальмування, що простежуються в життєдіяльності як окремих осіб, так і класів, націй, народів. Не можна випускати із виду відносну самостійність правових процесів розвитку, функціонування і гальмування.

Іншими справами, закони інтересу як фундаментальної основи контррозвідувальної діяльності належить особливе місце в системі законів суспільного розвитку, оскільки нічого не відбувається без інтересу у зрушенні розвитку продуктивних сил, зокрема у правових відносинах державної політики, ідеології тощо.

У свою чергу, запровадження концептуальної моделі контррозвідувальної діяльності спрямовано на оптимізацію структурних підрозділів контррозвідки і системи її діяльності. Означена концептуальна модель базується на положеннях Конституції України, законів України та інших нормативно-правових актів у сфері національної безпеки, міжнародних договорів, згода на обов'язковість яких надана Верховною Радою, а також нормативних документах України.

Структурна організація контррозвідувальної діяльності

Контррозвідувальна діяльність є особливим видом діяльності, підпорядкованим вирішенню завдань забезпечення безпеки, оскільки спрямована на адекватну (юридично надійну) протидію реальним та потенційним загрозам безпеці, що виникають внаслідок розвідуванню підривної діяльності спеціальних служб іноземних держав (розвідки, контррозвідки), недержавних розвідувальних і контррозві-

дувальних структур, організацій та окремих осіб проти України у формах агентурної, технічної розвідки і розвідки з використанням легальних можливостей по території України і за її межами, об'єктами зацікавленості яких є інформація з грифами обмеження, що належать Україні) та безпосередньому підриву (терор, диверсія, шкідництво).

Крім того, структурний зміст контррозвідувальної діяльності полягає в попередженні, виявленні та припиненні розвідувально-підривної діяльності іноземних держав з використанням спеціальних сил і засобів, форм і методів, які сприяють вирішенню національних інтересів України, своєчасному прийняттю заходів, адекватних характеру та масштабам загроз цим інтересам, що основані на принципах правової демократичної держави, оперативної та ідеологічної доцільності у відповідності з чинним законодавством.

У концептуальній конструкції контррозвідувальної системи відповідно до визначених напрямів варто закласти такі критеріальні елементи як: конституційні, соціально-політичні, основні, спеціальні, оперативно-тактичні та організаційні. При цьому акцентуємо увагу на структурну організацію, яка визначається:

1. Діяльністю органу, яка спрямована на досягнення результату, визначеного його головним функціональним завданням.

2. Структура органу відповідає характеру його діяльності і будується з урахуванням направленості на конкретні об'єкти.

3. Елементи цієї структури можуть об'єднуватися для створення підрозділів за принципом подібності об'єктів діяльності та методів і засобів, які при цьому використовуються.

4. Підпорядкованість і взаємодія елементів у контррозвідувальній системі забезпечується як результат діяльності кожного з них, що є керуючою інформацією для структурних елементів наступного рівня ієрархії (знизу — вгору і навпаки).

Отже, структурна організація контррозвідувальної діяльності як вияв методологічної основи є системою ідей, поглядів, цілеспрямувань на діяльність контррозвідки з метою убезпечення особистості, держави та суспільства від протиправної діяльності спеціальних служб іноземних держав, окремих організацій, груп та осіб, що пов'язані з ними в електронній сфері життєдіяльності суспільства. Така здатність системи контррозвідки як суспільних відносин є забезпеченням оптимального функціонування її інститутів у суспільстві країни і за його межами у вирішенні життєво важливих інтересів.

Основні критерії оцінювання контррозвідувальної діяльності

1. Адекватність реагування на будь-які загрози;

2. Конституційність;

3. Захист пріоритетних інтересів, посягання на які може призвести до значної матеріальної чи політичної шкоди;

4. Легальні можливості, спрямовані на одержання відомостей з грифами обмеження на об'єктах;

5. Освіта, наука та виховання як формула академічної мудрості в протидії корупційним маніпуляціям;

6. Аерокосмічні канали зв'язку;

7. Правова дисперсія та ентропія;

8. Ментально-ціннісні орієнтири;

9. Компетенція. Безперечно, саме розподіл компетенції як важливого критеріального конструкту в системі контррозвідки здійснюється на підставі їх ментально-професійної

спеціалізації в силу екстралінгвістичних здібностей певних осіб, груп, класів, етносів, спільнот;

10. Дипломатія як шляхетність переговорів;

11. Мудрість як якість переосмислення життєво важливих інтересів;

12. Конфіденційність інформації;

13. Ризики у системі превентивних заходів, що визначаються низкою засобів і методів захисту інформації та ймовірністю завдання шкоди і розмірами можливої шкоди, яка наноситься ресурсам інформаційної системи;

14. Фрактальність як правова безпека інформації.

Термін «фрактальність» використовується із сучасного природознавства, в якому фракталами йменуються такі утворення, що при зміні масштабу їх розгляду повністю відтворюють свою структуру як якість правового суб'єкта людини. Іншими словами, для національної безпеки фрактальність складає особистісну ідентичність, що є правомірним на ексклюзивність, оригінальність, специфічність. При цьому, засновник теорії фракталів Б. Мандельброт запропонував теоретичне обґрунтування закону Ціпера, якщо «порівнювати мову тексту з кодуванням, що може бути використано для визначення стратегії правової поведінки» особи, держави та суспільства [107, с. 112].

Механізми реалізації системи контррозвідки

Концептуальна модель контррозвідувальної діяльності реалізується на основі послідовного впровадження в діяльність кожного співробітника контррозвідувального підрозділу визначених основних положень і засад, пріоритетних напрямків та завдань щодо забезпечення національної безпеки України відповідно до правових інтересів сучасних життєвих реалій. Це здійснюється за такими методиками:

1. Проводиться аналіз загроз і ризиків інформації конкретного компонента інтелектуальної системи з використанням адаптивних засобів оперативної інформації.

2. Необхідність об'єктивно-орієнтованого підходу в моделі захисту інформації, яка полягає в побудові образу системи, оцінюючи її загальний стан, уразливість або рівень захищеності інформації в ній. Такий підхід використовує об'єктну декомпозицію, коли поведінка системи описується в термінах взаємодії об'єктів. При цьому, основним інструментом боротьби зі складністю в об'єктно-орієнтованому підході є інкапсуляція — це приховування реалізації об'єктів (їх внутрішньої структури і деталей реалізації методів) з наданням зовні тільки певних інтерфейсів.

3. Правовий захист конфіденційної інформації в Україні. Слід зазначити, що рівень захищеності інформації, зокрема конфіденційної інформації, визначається рівнем демократії в суспільстві, дотриманням міжнародних стандартів прав людини та основних свобод. Одним з основних видів захисту інформації в державі є правовий захист. Так, відповідно до статті 30 Закону України «Про інформацію» від 2 жовтня 1992 р. конфіденційна інформація — це відомості, які знаходяться у володінні, користуванні та розпорядженні окремих фізичних або юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Що стосується держави, то види конфіденційної інформації, її склад визначаються законами або внутрішніми регуляторними актами, що видаються відповідними державними органами. Головна спрямованість таких актів — це захист, збереження, недоступність інформації, що визначається як державна таємниця або інформація з обмеженим дос-

тупом. Можна сказати, що держави та її органів застосовується принцип «дозволено лише те, що зазначено в законі».

Так, відповідно до статті 30, частини 2 Закону України «Про інформацію» громадяни, юридичні особи, які володіють інформацією професійною, діловою, виробничою, банківською, комерційною та іншого характеру, одержаною на власні кошти, не порушує передбачені законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційності та встановлюють для неї систему (способи) захисту [53, с. 338].

У цьому зв'язку варто проаналізувати зміст інструкції щодо порядку зберігання й використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, яка є власністю держави (затверджена Постановою Кабінету Міністрів України № 1892 від 27 листопада 1998 р.) У даному регуляторному акті термін «конфіденційна інформація, що є власністю держави» не розтлумачений, але на підставі цього акту Кабінет Міністрів надав право державним органам визначати Перелік конфіденційної інформації, що є власністю держави, на який надається гриф обмеження доступу «для службового користування».

Адже варто означити, що такі переліки не потребують реєстрації в Міністерстві юстиції України, а, отже, не підлягають обов'язковій публікації.

Проте, враховуючи ту обставину, що переліки охоплюють широку сферу щодо обмеження доступу до інформації, на їх підставі практично можна обмежити конституційне право громадян України на отримання інформації всупереч діючій статті 34, частині 3 Конституції України, в якій йдеться про обмеження інформаційних прав громадян України лише на підставі Закону.

У цьому зв'язку відповідно до статті 37 Закону України «Про інформацію» [53, с. 413] не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містять у собі: інформацію, визнану у встановленому порядку державною таємницею; конфіденційну інформацію; інформацію про оперативну та слідчу роботу органів прокуратури, МВС. СБУ, роботу органів дізнання та суду у тих випадках, коли її розголошення може зашкодити оперативним заходам, розслідуванню чи дізнанню. Установа, до якої направлено запит, може надавати для ознайомлення документ, що містить відповідну інформацію, яка не підлягає розголошенню на підставі нормативного акту іншої державної установи, а та державна установа, яка розглядає запит, не має права вирішувати питання щодо її розсекречування і інформацію фінансових установ, підготовлену для контрольно-фінансових відомств.

З огляду на існуючі міжнародні стандарти прав людини, закріплені в нормах міжнародного та європейського права, такий підхід значно обмежує права громадян України на отримання всебічної, правдивої, неупередженої інформації, а також породжує протиріччя між конституційними та галузевими нормами права України, яке потребує негайного усунення.

4. Національний вимір загрози транснаціональної злочинності. Національний вимір загрози транснаціональної злочинності пов'язаний із природою організованої злочинності, що здатна порушувати державні кордони. Хоча в сучасних умовах глобалізації кордони стають прозорішими. Проте наявність і регулювання кордонів залишаються одними з невід'ємних атрибутів державності. Протиріччя між державою та кримінальними організаціями в цій

царині складають основу конфлікту між правом держави на здійснення функцій охорони та моніторингу своєї території та правом групи осіб на охорону та задоволення інтересів своїх членів, що можуть не збігатись з інтересами держави [109, с. 25].

За цих умов основним практичним напрямком наукових пошуків у дослідженні проблем транснаціональної злочинності може стати аналіз ролі організованої злочинності в контексті міжнародних відносин. Науковим підходом у практичній площині, що максимально віддзеркалює міжнародний характер явища, має стати системний підхід.

Цей підхід розглядає організовану злочинність в якості складного системного явища, в основі якого знаходиться соціально-політичний і економічний конфлікт, а його транснаціональний вимір характеризується розвитком процесів глобалізації та природним продовженням зв'язків, що виникають внаслідок транснаціонального промислового виробництва.

Таким чином, діяльність органів контррозвідки провадиться як на стратегічному, так і тактичному рівнях. При цьому, види, форми, методи, сили і засоби системи контррозвідувальної діяльності спеціальних служб іноземних держав тощо; попередженням і припиненням протиправної діяльності спеціальних служб іноземних держав тощо. Форми системи контррозвідки визначаються за: цільовим призначенням; силами і засобами, що використовуються; характером здійснення; територією, на якій проводяться превентивні заходи, та рівнем ухвалення рішення про проведення означених заходів. Саме на базі системного методу діяльність контррозвідувальних підрозділів міністерств, відомств та підприємств із захисту інформаційних ресурсів в

майбутньому надає гарантію їх збереження від заволодіння ними будь-якого противника.

Контрольні запитання

1. Форми та види кіберпротиборства.
2. Завдання кібервійн.
3. Об'єкти деструктивного інформаційного впливу та форми кібервійн.

Теми рефератів

1. Сутність медіа кампаній стосовно кіберпротиборства.
2. Цілі кібервійни на світовому ринку озброєнь.
3. Методи кіберборотьби, які застосовуються на світовому ринку озброєнь.

РОЗДІЛ 3. ЗДОРОВ'Я ЛЮДИНИ ТА ГРОМАДЯНИНА В СФЕРІ КІБЕРБЕЗПЕКИ

3.1. Здоров'я людини та громадянина у адміністративно-правовому полі: український погляд

У сучасних умовах кіберпростору, коли надзвичайно поширені алергічні захворювання, здоров'я людини та громадянина є особливо актуальною. При цьому застосування засобів лише традиційної медицини, викликає у значної кількості громадян різного роду ускладнення фізичного і психічного характеру. Тому при зростанні цін на лікувальні засоби певна частина населення світу все частіше звертається до народної та нетрадиційної медицини. Адже всесвітня Організація Охорони Здоров'я як одна з провідних інституцій ООН звертається до лікування засобами народної та нетрадиційної медицини, що констатує численні надбання медичного знання людства. Отже, Україна належить до країн, в яких нетрадиційна медицина легально співіснує з офіційною. Про це свідчить, зокрема, ст. 74 закону України «Основи законодавства України про охорону здоров'я», згідно якого особам без спеціальної освіти дозволяється діяльність у галузі народної та нетрадиційної медицини.

Центральним органом, що здійснює управління народною та нетрадиційною медициною в Україні, є Міністерство охорони здоров'я, яким утворено Центр управління діяльністю в галузі народної і нетрадиційної медицини. У складі МОЗу створений Комітет з народної і нетрадиційної медицини відповідно до Указу Президента України від 31 липня 1998 р. «Про додаткові заходи щодо врегулювання

діяльності у сфері народної і нетрадиційної медицини». Означений Комітет має право видавати особам без спеціальної освіти дозвіл на медичну діяльність у галузі народної та нетрадиційної медицини. Цей Комітет також є головною установою Міністерства з проведення експертизи, атестації осіб, які мають спеціальні дозволи, займаються медичною діяльністю в зазначеній галузі за ліцензіями МОЗ України.

Частина повноважень у цій сфері делегована Українській асоціації народної медицини, яка, зокрема, здійснює експертизу цілительських здібностей осіб, котрі виявили бажання займатися медичною діяльністю в галузі народної та нетрадиційної медицини.

Медичне право в сфері господарювання

Саме підприємницька діяльність як дух господарювання з медичної практики підлягає ліцензуванню. Суб'єктам цієї діяльності як суб'єктам господарювання варто зареєструватися в установленому законом порядку, а для здійснення своєї діяльності незалежно від їх організаційно-правової форми та форми власності необхідно отримувати ліцензію з метою медичної нетрадиційної практики. Це має провадження зазначеного в ньому виду діяльності з медичної практики протягом визначеного терміну та за умови виконання ним Ліцензійних умов.

Ліцензійні умови регламентуються ст. 8 Закону України «Про ліцензування певних видів господарської діяльності», Постановою Кабінету Міністрів України від 14 листопада 2000 року № 1698 «Про затвердження переліку органів ліцензування» та спільним наказом МОЗ України і Державного комітету України з питань регуляторної політики та підприємництва від 16 лютого 2001 року № 38/63 «Про затвердження Ліцензійних умов провадження господарської

діяльності з переробки донорської крові та її компонентів, виготовлення з них препаратів, господарської діяльності з медичної практики та проведення дезінфекційних, дезінсекційних, дератизаційних робіт. При цьому знання і дотримання вимог чинного законодавства щодо умов провадження медичної практики в галузі народної та нетрадиційної медицини стає все більш важливим, оскільки підвищує правовий захист суб'єкта підприємницької діяльності на територіальному ринку медичних послуг.

У сучасних умовах ринку праці діяльність фахівців з питань народної медицини в Україні регламентоване низкою нормативно-правових актів, які в основному представляють відомчі акти, що передбачають, зокрема порядок звітування про затвердження плану у 2007 році головних позаштатних спеціалістів з народної і нетрадиційної медицини; встановлюють систему управління у цій галузі; встановлюють порядок ліцензування тощо.

Законодавчо встановлено:

- механізми регулювання здійснення медичної практики у галузі народної і нетрадиційної медицини;
- контроль за здійсненням незаконної медичної діяльності у галузі народної і нетрадиційної медицини;
- порядок і випадки надання спеціальних дозволів для здійснення такої діяльності;
- систему атестації та експертизи в галузі народної і нетрадиційної медицини, зокрема експертизи цілительських здібностей осіб, які виявили бажання займатись медичною діяльністю в галузі народної і нетрадиційної медицини, в також переатестації осіб, яким було видано ліцензії на здійснення медичної практики в сфері народної та нетрадиційної медицини.

З урахуванням вище означеного Комісія по видачі спеціальних дозволів з народної і нетрадиційної медицини при вирішенні питання про надання спеціальних дозволів розглядати заяви осіб, які бажають здійснювати медичну практику в галузі народної та нетрадиційної медицини, за такими методами, як: ароматерапія, біоенергоінформотерапія, іридодіагностика, мануальна терапія, точковий масаж, Су-Джок, терапія неінвазивна (для осіб зі спеціальною медичною освітою), фітотерапія.

Контроль та рекомендації діяльності у сфері народної та нетрадиційної медицини

У свою чергу, Кабінетом Міністрів України за зазначеним приписом Президента України було створено спеціальний орган — Комітет з питань народної і нетрадиційної медицини у структурі Міністерства охорони здоров'я України.

Міністерству інформації України, Державному комітету України у справах релігій було дано доручення про посилення контролю за використанням засобів масової інформації особами, які практикують у сфері народної та нетрадиційної медицини, проповідниками новітніх релігійних течій з метою недопущення поширення ними інформації, що негативно впливає на здоров'я громадян та перешкоджає додержанню загальновизнаних норм етики і моралі.

Крім того, Генеральній Прокуратурі України було запропоновано посилити нагляд за додержанням законодавства особами, які займаються медичною практикою у сфері народної та нетрадиційної медицини. Це посилило вимоги до ліцензування.

У своїй роботі цілитель та лікар, під контролем якого перший з них здійснює медичну діяльність (або в умовах лікувального закладу), керується законодавством про охо-

рону здоров'я, нормативно-правовими актами МОЗ України, а також зазначеним Положенням, в якому визначені права та обов'язки цілителя та лікаря.

Зокрема, цілитель, який здійснює таку діяльність, зобов'язаний:

- займатися медичною практикою за умови наявності спеціального дозволу (ліцензії) МОЗ України під контролем лікаря або в умовах лікувального закладу;
- здійснювати медичну практику, передбачену спеціальним дозволом (ліцензією) МОЗ України в обсязі та порядку, встановлених законодавством;
- узгоджувати свої дії щодо надання консультативної та лікувальної допомоги пацієнтам із лікарем-спеціалістом;
- вести облікову документацію (журнал обліку діагностично-лікувальних сеансів, процедур), в якому варто зазначати паспортні дані пацієнтів, обсяг лікувальних процедур, моніторинг за динамікою стану здоров'я та висновок щодо ефективності наданого лікування.

Лікар, який контролює медичну діяльність цілителя в галузі народної та нетрадиційної медицини, має право:

- припинити або заборонити потреби застосування методів народної та нетрадиційної медицини, які цілитель використовує при лікуванні хворого;
- вносити пропозиції щодо змін в організації роботи цілителя.

Законодавство України встановлює відповідальність цілителя і лікаря, під контролем якого перший здійснює медичну діяльність у галузі народної та нетрадиційної медицини.

Так, цілитель та контролюючий його діяльність лікар у встановленому законодавством порядку несуть відповідальність за:

– дії, які призвели до шкідливих наслідків для здоров'я пацієнта;
– достовірність облікових та звітних даних;
– порушення чинного законодавства щодо надання медичної допомоги та порядок здійснення підприємницької діяльності.

Спекулятивні маніпуляції в транс-медіа щодо народної та нетрадиційної медицини

Надзвичайно можливими є рекомендації представникам Національної ради України з питань телебачення і радіомовлення щодо дотримання телерадіоорганізаціями України вимог чинного законодавства до висвітлення проблем народної та нетрадиційної медицини, затверджені на підставі ст. 24 Закону України «Про рекламу». Адже відомо, що в гонитві за грошима наприкінці 60-х на початку 90-х років ЗМІ «розкручували» екстрасенсів, психотерапевтів, цілителів, сприяли проведенню масових сеансів лікування, які мали, як вже зазначалося, для багатьох негативні наслідки.

У Рекомендаціях зазначено, що у теле- і радіопрограмних телерадіоорганізацій України значно поширилося висвітлення лікувальної практики у сфері народної та нетрадиційної медицини з грубим порушенням чинного законодавства.

Регламентується чинним законодавством і висвітлення у ЗМІ медичної практики у цій сфері. Зокрема, пунктом 24 Закону України «Про рекламу» передбачено: «Реклама щодо інших видів підприємницької діяльності, які відповідно до законодавства України потребують спеціального дозволу, повинна мати посилання на номер чинної ліцензії і найменування органу, який її видав».

Значна кількість вітчизняних телеорганізацій ці вимоги ігнорують. Звичним явищем стало широко рекламувати і

висвітлювати медичну практику осіб, котрі порушують чинне законодавство України в галузі народної та нетрадиційної медицини. Героями транс медіа, що пропонуються масовій аудиторії, стають «цілителі», котрі не мають ні спеціальної медичної освіти, ні документів МОЗ України (ліцензії, спеціальні дозволи), що надавали б їм право на здійснення лікувальної діяльності в цій сфері. Дії багатьох із них уже завдали значної шкоди здоров'ю громадян, що становлять певну потенційну загрозу. Проте, тележурналісти нерідко надають псевдо цілителям ореол сенсаційності та фальшивої всемогутності, обертаючи своїх слухачів і глядачів на «заручників шарлатанів». Саме цим загрозливим явищем занепокоєні управлінці вітчизняної сфери охорони здоров'я та медичні фахівці. Зокрема, МОЗ України неодноразово звертався до Національної ради України з питань транс-медіа та запобігання корупції з вимогою негайно припинити беззаконня в зазначеній сфері. Тому, на наш погляд, одних рекомендацій недостатньо, оскільки мають бути передбачені жорсткі санкції за порушення представниками ЗМІ вимог законодавства в розглянутій частині. Зважаючи на важливість деонтологічних (морально-етичних) аспектів діяльності у сфері народної та нетрадиційної медицини і на те, що згідно зі ст. 92 Конституції України всі правовідносини, пов'язані із забезпеченням, гарантуванням та реалізацією прав і свобод людини, регулюються виключно законами. Оскільки говориться про захист першорядних для людини прав — на здоров'я та життя, то регулювання зазначених біотичних правовідносин доцільно перенести зі сфери регулювання підзаконними (відомчими документами у площину нормативно-правового акту вищої юридичної сили. Крім того, пропонується кодифікувати законодав-

ство у сфері охорони здоров'я, прийнявши Кодекс законів про охорону здоров'я, одну з частин якого варто присвятити питанням народної та нетрадиційної медицини.

Страхування медичних ризиків

За сучасної фінансово-економічної ситуації в Україні розвиток страхування відповідальності за шкоду, заподіяну життю та здоров'ю людини, її генетичній, біологічній, психічній цілісності усього суспільства, може стати реальним механізмом забезпечення біологічної безпеки суспільства, ринковим механізмом на господарських суб'єктів у сфері охорони здоров'я. З метою запобігання тотального геноциду націй у світовому процесі як людського генофонду, збереження його цілісності необхідно здійснювати адміністративно-правовий захист біологічної безпеки, зокрема в сфері інтелектуального бізнесу та інноваційної економіки. Тому в сучасних умовах підвищеного ризику суспільство має розробити відповідний захисний механізм для боротьби з ризиком.

Серед різних методів керування ризиком виділяється страхування, що як складова фінансової системи сприяє стабілізації економіки. Для України це особливо необхідно, оскільки саме інноваційний підхід до реформування економіки пов'язаний зі значними труднощами як соціально-економічного, так і культурно-екологічного та політичного характерів.

Передумовою виникнення страхових відносин у біобезпеці є ризик як соціальне конструктивне явище негативного і позитивного впливу. Зміст такого ризику і його міра ймовірності визначають ентропійні межі страхового захисту.

Про ризик йдеться лише тоді. коли є відхилення між запланованими і реальними (фактичними) результатами.

Така девіація (відхилення) може бути або позитивним, або негативним. Негативне відхилення означає несприятливий результат. Позитивне відхилення виникає тоді, коли фактичний результат виявляється вагомішим, ніж очікувалося. Можливість негативного відхилення в межах внутрішньої позитивної енергетики людини та громадянина (так званої «аури, ціннісної парадигми, світоглядних орієнтирів) від запланованого фактичного результату, і називається ризиком як ентропійної системи (невизначеності). Ймовірність позитивного відхилення при вихідних заданих параметрах на одну очікувану подію визначається як шанс. У цьому сенсі можна виокремити ризик втрати (збитку) або шанс на позитивний результат (прибуток), в яких збиток виражається у негативному, а прибуток — у позитивному відхиленні між плановими (очікуваними) і реальними (фактичними) результатами. Саме багатогранність форм прояву ризику, частота і шкідливість наслідків прояву, заходам страхування.

Адже ризик — це така сукупність явищ (подій, фактів тощо) з настанням яких відбуваються виплати з раніше утвореного централізованого страхового фонду в натурально-речовій або грошовій формі. Ризик пов'язаний із конкретним об'єктом, щодо якого визначаються чинники ризику. Аналіз одержаної інформації в комплексі з іншими заходами дозволяє суттєво знизити негативні наслідки здійснення (реалізації) ризику, який зумовлює ймовірність загибелі чи пошкодження (у майновому страхуванні) об'єкта, прийнятого на страхування.

Якщо ймовірність дорівнює нулю, можна стверджувати про неможливість настання прогнозованої події. Якщо показник ймовірності дорівнює одиниці, то подія гарантовано

відбудеться. Очевидно, що чим менша ймовірність біотичного ризику, тим легше й дешевше можна організувати страхування цього ризику.

Потужна ймовірність ризику передбачає страховий захист за високою ціною, що ускладнює його здійснення (таким, наприклад, він може бути сьогодні для сфери обігу ГМО). Тією мірою, якою оцінено ймовірність настання можливої події, може бути об'єктивно визначено розмір ризику, наприклад, при застосуванні продуктів та товарів із ГМО цей розмір може бути надзвичайно високим.

При цьому, страхування і розмір ризику діалектично взаємопов'язані. Вирівнювання ризику, його розподіл становлять сукупність прийомів страхової організації, за допомогою яких на практиці організовується проведення страхування, добір відповідних технічних прийомів. Належна оцінка розміру ризику має неабияке значення в роботі страховиків, оскільки визначає величину необхідного страхового фонду, а значить, і можливості відшкодування збитків застрахованих як у звичайні, так і в особливо несприятливі роки.

Пропонується розробити проект закону про страхування біотичних ризиків. Такий закон дозволив би здійснювати біотичне страхування при здійсненні будь-яких експериментів, науково-дослідних робіт із залученням біооб'єктів, промислового виробництва, зокрема лікувальних препаратів, продуктів харчування, побутових препаратів з використанням біологічного матеріалу тощо. У законі доцільно розробити практико застосовний механізм та інструментарій управління біотичними ризиками з метою мінімізації негативних наслідків для навколишнього середовища і життєдіяльності людей; сформувати систему біотичного страхування як сукупність ефективних заходів оптимального пово-

дження з біологічними видами, людським організмом, для раціонального природокористування; розробити специфічну методику розрахунку страхових тарифів, визначити основні джерела накопичення страхових резервів та напрями їх використання; створити модель розвитку біотичного страхування як в сфері біології, медицини, так і інших сферах життєдіяльності суспільства.

У процесі розробки законопроекту має бути сформовано всебічну та повно аспектну систему біотичного страхування, створено блок-схему регулювання біотичного ризику для об'єктів підвищеної небезпеки. Тому варто створювати шляхи мінімізації біотичних ризиків: можливо, через обмеження деяких видів діяльності за участю біооб'єктів, зокрема в генній інженерії; заміну операцій з отримання стволових клітин від ембріонів на їх виробництво із інших біоматеріалів (зокрема, із шкіри, яка може регенеруватися); заміну органів-трансплантатів від сторонніх донорів н клоновані органи самого реципієнта тощо.

Потребують законодавчого врегулювання проблеми, пов'язані з клонування людини як біосоціоістоти. Це отримується із застосуванням генонанотехнологій. Законодавець має переглянути і оновити у бік посилення захисту прав людини правовий режим та правила проведення операцій з трансплантації органів та тканини. Крім того, важливим питанням розвитку системами біотичного страхування є визначення розміру тарифних ставок, які розраховуватимуться залежно від ціни екологічного ризику та інших витрат, необхідних для виконання зобов'язань за укладеним договором страхування. При розрахунку величини тарифу в системі біотичного страхування необхідно буде врахувати такі чинники: частоту виникнення генетичної, біологічної

аварії; кількість суб'єктів біотичної діяльності з підвищеним ступенем біотичної небезпеки (трансплантаційні центри, лабораторії, що здійснюють науково-дослідні експерименти з генетичними та біологічними матеріалами, підприємства генної інженерії, приватних компаній з виробництва лікарських препаратів із застосуванням ГМО, фетальних матеріалів, ембріональної тканини тощо); розміщення на певній території; максимальний збиток, який може бути спричинено людському середовищу, генофонду внаслідок виникнення страхового випадку.

3.2. Трансформація людини як генотехнологічна система клонування

На сучасному етапі інформаційного розвитку біотехнологій, появою та інтенсивним застосуванням генної інженерії та інноваційними відкриттями в медицині виникла актуальна потреба правового врегулювання. Адже сьогодні біотичне законодавство набуває такого активного розвитку в різних країнах світу, що вже існує досить значний масив міжнародно-правових актів. При цьому із правових інститутів у галузях цивільного, екологічного, медичного, адміністративного, кримінального права формується самостійна галузь біотичного права зі своїм предметом регулювання та своїми інститутами. У цій правовій сфері склалися і розвиваються такі правові інститути, як психічного здоров'я; пенітенціарної медицини; врегулювання взаємовідносин лікаря та пацієнта; правового врегулювання проблем, пов'язаних із евтаназією; сурогатного материнства; поводження з фетальними матеріалами; гуманного поводження з тваринами (зокрема, при використанні останніх, як об'єктів дослідження в наукових та медичних цілях) тощо [172, с. 212].

Масове запровадження в повсякденну практику нових біомедичних та психотехнологій постійно породжують біотичні проблеми, які вимагають актуального правового розв'язання, оскільки питання про етичність клонування людини нагально обговорюється вченими, лікарями і фахівцями з біоетики.

Як відомо, генотехнології входять а антропологію, просуваючись до можливості практичного маніпулювання генетичною програмою, геномом людини. Коли генетичні зміни перевищують певну критичну долю генетичного матеріалу людини, є підстава стверджувати, що людини перетворюється на іншу, відмінну від людини живу істоту. У цих істот немає сьогодні єдиного загальноприйнятого імені. Такі стратегії ведуть до можливості ще однієї екзотичної істоти — Клона, тобто точної генетичної копії іншого людського організму, оскільки Клон — генетично нормальна людська істота. При цьому Людина Мережі — Інтермен також є одним з проектів стану майбутньої людини. «Інтерменом можна назвати людину XXI-го століття, життя якої тісно пов'язане (зав'язане на) з Інтернетом. Особистість інтермена формується в Мережі і належить мережевим співтовариствам. Інтермен будує плани, виходячи лише з можливостей, що відкриваються Мережею, інтелектуально і емоційно прив'язаний до неї, залежить від процесів, що відбуваються в кіберпросторі, переживає захоплення і потрясіння у зв'язку з подіями, що відбуваються в Мережі, закохується і ненавидить через Мережу, шукає допомоги, підтримки через Мережу. Психологічно інтермен прив'язаний до процесів у Мережі, що мають до нього безпосереднє відношення, бо лише їх вважає справжніми, вартими його уваги та часу. На нашу думку, сутністю інтермена є його

здатність реалізовуватись у такій мен-маргінал (звичайний користувач інформацією), інтермен-хакер (користувач прихованою інформацією) і інтермен-креативщик (творець інноваційних інформаційних проектів) [59, с. 87].

Застосування біотехнологій з клонування

З одного боку, застосування біотехнологій з клонування дасть можливість розв'язати значну кількість медичних проблем. Так, за допомогою стовбурових клітин можна вилікувати хворобу Альцгеймера або травму спинного мозку, які не піддаються лікуванню іншим шляхом. З іншого боку, клонування людини вважається не прийнятим з етичного погляду.

У 2005 році Генеральна Асамблея ООН прийняла резолюцію, яка закликала законодавців усіх країн світу заборонити всі форми клонування людини. За цих умов під заборону потрапило не лише репродуктивне, але й терапевтичне клонування, тобто клонування ембріональних стовбурових клітин з метою отримання культур, які використовують для лікування різних захворювань.

В основу резолюції було покладено пропозицію США про повну заборону діяльності з клонування людини, людських органів, тканин і клітин. Це рішення схвалили значна кількість країн, проте питання про повну заборону на використання стовбурових клітин у медичній практиці стало причиною відповідних суперечок. У результаті, прийнятий значною кількістю голосів акт отримав лише рекомендаційний характер, хоча прибічники США розраховують на те, що Резолюція стане кроком до запровадження в майбутньому більш жорстких заходів щодо заборони клонування людини.

Крім того, країнам, що займали різні позиції щодо клонування, в цьому питанні так і не вдалося досягти компромісу, було прийнято Декларацію, яка стала актом компро-

місного характеру. За цих умов прихильники здійснення досліджень, пов'язаних з ембріоном, мотивували свою позицію прагненням врятувати людство від ряду тяжких хвороб. Так, на їх думку, використання клітин клонованих ембріонів дозволить вирішити значну кількість проблем сучасної медицини. Адже використання його як біологічного матеріалу, з якого будуть вилучати, наприклад, стовбурні клітини, інші «запчастини», неминуче призводить до загибелі ембріону, а це, на їх думку, можна кваліфікувати як убивство.

Попри те, що в багатьох країнах клонування заборонене, експерименти в цьому напрямі продовжуються. Виконується чимало наукових програм з генетики, терапевтичного клонування та відтворення. деякі з них мають позитивні результати. Так, зокрема, інтернаціональним колективом вчених із США, Німеччини, Великобританії було розшифровано генетичний код Х-хромосоми людини. Ця хромосома відповідає за розходження між статями: жінки мають дві Х-хромосоми, а чоловіки — одну Х та одну Y-хромосоми. Функції «дефектного» гена в одній жіночій Х-хромосомі бере на себе «нормальний» ген в іншій хромосомі. У чоловічому ж організмі ген-мутант нічим не компенсується. Мутація генів Х-хромосоми спричиняє приблизно 300 спадкових захворювань, від яких найчастіше страждають саме чоловіки, причому деякі з хвороб передаються підліткам по материнській лінії. Більшість цих хвороб важко лікуються або не виліковні зовсім. Серед таких хвороб гемофілія, олігофренія, аутизм та інші.

Ученим із Бристольського університету вдалося виростити хрящ, використовуючи стовбурові клітини хворих, здатні за певних умов перетворюватися на різні органи і тканини. Для дослідження їх вилучили з кісткового мозку

стегна у хворих, яким робили реконструктивні операції. Стовбурові клітини вирощували у спеціальному розчині, застосовуючи каркас із поліґліколевої кислоти, який має здатність розсмоктуватися. Цей полімер сьогодні застосовують переважно у виробництві шовного матеріалу для оперативних втручань. Нова геотехнологія в майбутньому дасть можливість виконувати операції з трансплантації нового хряща на місце старого, деформованого внаслідок захворювання на остеоартрит, одною з найбільш поширених захворювань суглобів, що спричиняє інвалідність. Так, за даними медичної статистики тільки у Великобританії від остеоартриту страждає понад два мільйони осіб.

За допомогою цієї геотехнології можна буде одночасно розв'язати декілька проблем, які можуть виникнути під час проведення трансплантації. По-перше, вдасться уникнути небезпеки відторгнення хряща, оскільки пацієнтові пересаджуватимуть власні стовбурові клітини. По-друге, будуть дотримані етичні норми, оскільки відпаде потреба у використанні клітин людських ембріонів. Такий вид клонування вбачається найбільш прийнятим і дійсно дозволяє вирішити біотичну проблему. Раціональним є уникнути прийняття на міжнародному рівні документу, який би запроваджував клонування тільки клітин від хворого (як це мало місце з вирощуванням згаданого хряща, для виготовлення для нього тих чи інших потрібних йому біологічних матеріалів, включаючи й органи для трансплантації). Це б дозволило:

- значно підвищити рівень приживлюваності органів і тканин;
- врятувати життя й здоров'я живим донорам, чиї органи незаконно вилучають і використовують з метою трансплантації;

- припинити заборонену міжнародними нормами торгівлю органами та тканинами, а також використання ембріонів як «біологічної сировини» для виготовлення препаратів, для трансплантаційної мети тощо;
- припинити функціонування злочинних трансплантаційних центрів.

Україна підписала та ратифікувала міжнародні акти, які забороняють репродуктивне клонування людини. Крім того, в нашій державі діє Закон «Про заборону репродуктивного клонування людини», яким заборонено створення особи, генетично ідентичної іншій живій або померлій людині, шляхом перенесення в позбавлену ядра жіночу статеву клітину ядра соматичної клітини людини, а також ввезення в Україну та вивезення з неї клонованих ембріонів людини.

Вважається, що українському законодавцеві варто прийняти ще закон, який би заборонив спекулятивні маніпуляції з ембріонами та використання їх для отримання стовбурових клітин. Одночасно необхідно вирішити на законодавчому рівні питання про здійснення клонування клітин хворого суб'єкта з метою вирощування для нього ж необхідних біологічних матеріалів, зокрема органів для трансплантації.

Варто звернути увагу на генетичні експерименти з вірусами, що також дали належні результати. Нове дослідження, результати якого опубліковано в часописі Nature, присвячене вивченню бактеріофагів — вірусів, що уражують бактерії. Вчені з Американського інституту алергійних та інфекційних захворювань виявили в бактеріофагах ген, який сприяє швидкій перебудові білків і прикріпленню їх до різних клітинних рецепторів.

Отже, на наш погляд, зазначені дослідження відкриває можливості для створення вакцин і ліків проти стійких бак-

терій, які дедалі більше непокоять громадськість. До несподіваних висновків стосовно розвитку злоякісного характеру онкопухлин дійшли британські вчені. Іншими словами, ген c-Jun контролює процеси розподілу клітин і вважається одним із найбільш «канцерогенних» у всьому геномі, що відіграє важливу роль у відтворенні нервових клітин після їх ушкодження.

Правова оцінка поводження з ембріоном людини

Із цього приводу прийнято ряд міжнародно-правових та європейських актів. Так, у Рекомендації № 934 (1982) з питань генної інженерії Парламентська Асамблея Ради Європи запропонувала ряд заходів із стосовно поводження з ембріонами. При цьому, також було прийнято спеціальні акти, серед яких — Рекомендація Парламентської Асамблеї «Про використання ембріонів та плодів людини з метою діагностики, терапії, наукових досліджень і промислового використання та торгівлі».

Міжнародні та європейські правові стандарти вимагають: за будь-яких обставин людські ембріони та плоди вимагають поводження, гідного людини. а також обмеження та здійснення суворого використання цих біологічних матеріалів і тканин за умов жорсткого і постійного контролю з боку компетентних державних органів. В силу означеного, правовий статус ембріона людини не визначено законами, тому український законодавець повинен розробити модельний закон про правовий статус ембріона, який можна було б запропонувати для європейських країн через відповідні служби Ради Європи.

Адже сьогодні за існуючих умов вжиття лише національних правових засобів не дасть ефективних наслідків, оскільки будь-яку діяльність у цій сфері може бути перене-

сено в іншу країну, в якій ці питання залишаються не врегульованими. При цьому Комітет міністрів Ради Європи стверджує:

- проаналізувати інформацію щодо торгівлі мертвими ембріонами та плодами та оприлюднення результатів аналізу;
- обмежити використання ембріонів людини, також отриманих із них тканин та біоматеріалів виключно терапевтичною сферою, якщо не має альтернативних засобів;
- прийняти нормативні акти, які inter alia визначили б умови, за яких допускається вилучення та використання тканин ембріона з терапевтичною і з метою діагностичною;
- заборонити будь-яке створення людських ембріонів шляхом штучного запліднення та проведення досліджень із живими чи мертвими ембріонами;
- заборонити всі дії, які може розглядатись як небажане використання або похідні методи від нього, включаючи:
- створення ідентичних людських істот шляхом клонування або будь-яким іншим методом з метою расового відбору;
- імплантацію ембріона людини самці тварини чи навпаки;
- злиття гамет людини з гаметами будь-якої тварини;
- створення ембріона зі сперми різних людей;
- поєднання ембріонів, яке може призвести до появи мутантів;
- ектогенез, або створення індивідуальної та самостійної людської істоти в лабораторних умовах;
- вибір статі шляхом генетичних маніпуляцій із нетерапевтичною метою;

- створення ідентичних близнюків;
- досліди на життєздатних людських ембріонах;
- експерименти на живих людських ембріонах, незалежно від того: життєздатні вони чи ні;
- утримання ембріона з будь-яких причин більше 14 днів після запліднення (за вирахуванням часу. необхідного для заморожування), а також ввести відповідні санкції для забезпечення застосування постанов, прийнятих відповідно до рекомендацій;
- створити національні регістри акредитації медичних центрів, яким надано право застосовувати такі методики, зокрема в наукових цілях;
- спростити та заохочувати створення національних полідисциплінарних комітетів і комісій з питань наукової діяльності (генетичних матеріалів ембріонів та плодів) з метою науковому керівництву та консультацій медичного і наукового характеру для останнього, а також з метою супроводу та контролю застосування таких методик і дозволу здійснення спеціальних проектів за відсутності конкретного закону чи постанови;
- продовжити вивчення проблем, пов'язаних із використанням тканин ембріонів та плодів у наукових цілях, та підготувати на основі положень відповідну Європейську конвенцію або будь-який інший юридичний документ, який був би відкритий також і для прийняття країнами, що не є учасницями Ради Європи.

Міжнародні стандарти щодо ембріонів встановлюють нижченаведені правила діагностики. Так, є неприпустимим будь-яке втручання у живий ембріон in vitro або in utero, або у плід у діагностичних цілях є неприпустимим, крім випадків, визначених національним законодавством,

особливо, коли це втручання здійснюється задля блага майбутньої дитини та забезпечення його розвитку. Допускається використання мертвих ембріонів та плоду в діагностичних цілях або з'ясування причин мимовільного переривання вагітності.

Міжнародними стандартами передбачено умови застосування ембріонів у терапевтичних цілях. Зокрема, неприпустимим є втручання в живий ембріон плоду, якщо тільки таке втручання не здійснюється заради блага майбутнього дитини, зокрема полегшення пологів, розвитку дитини тощо. При цьому, неприпустимою є штучна підтримка життя ембріонів або плодів з метою вилучення матеріалів для подальшого використання.

Страхова медицина як боротьба із корупційною маніпуляцію

Саме в сучасних ринкових умовах для суб'єктів медичної діяльності усіх рівнів відкрилися критеріально нові економічні та психологічні можливості застосування медичних навичок «дозування правди». Адже працівники сфери медичної допомоги, не отримавши при розвалі Радянського Союзу ані дивідендів від приватизації, ані адекватної економічної оцінки їх складної праці, змушені були виживати «хто як зможе».

Саме сьогодні простежується нова модифікована форма введення в оману пацієнтів, а саме: медичні працівники, отримуючи якість гонорари від фармацевтичних приватних товариств (компаній), виписують пацієнтам дорогі препарати, які мають дешевші аналогом, або ті, які загалом не потрібно вживати. З метою припинити подібні випадки, варто керуватися досвідом більш розвинених країн, в яких лікар виписує більш дорогий препарат пацієнту, чиї послу-

ги сплачуються страховою медициною і, яких можна притягнути до юридичної відповідальності.

Тому у нашій країні для того, щоби виключити подібні негативні випадки, необхідне системне запровадження страхової медицини, а перелік ліків, які доцільно виписувати пацієнтам у тому чи іншому випадку підтвердженого захворювання, повинен затверджувати компетентний державний орган. До того ж медичні працівники мають увійти до кола державних службовців, отримувати належну винагороду за свою працю пільги тощо, як це відбувається в Німеччині, отримати статус державних службовців, як це має місце на Кіпрі тощо.

У ст. 43 Конституції України визначено, що кожна людина має право заробляти на життя роботою, яку вона обирає або на яку добровільно погоджується. У ст. 48 того ж документа зазначається, що умови праці мають бути відповідними, безпечними і здоровими, а заробітна плата — не нижче визначеного законом прожиткового мінімуму.

В «Основах законодавства України про охорону здоров'я» зазначено, що з метою охорони здоров'я населення, організуються профілактичні медичні огляди неповнолітніх, вагітних жінок, працівників підприємств, установ та організацій зі шкідливими і небезпечними умовами праці, військовослужбовців та осіб, професійна чи інша діяльність яких пов'язана з обслуговуванням населення або підвищеною небезпекою для оточуючих.

Таким чином, крім правових норм необхідно вживати практико-застосованих заходів, а також здійснювати націоналізацію незаконно приватизованих після 1996 року закладів систем охорони здоров'я, повернувши їх у державну та комунальну власність, а також «реанімувати» систему

диспансеризації та профілактики оглядів як хворих, так і усіх, хто може бути віднесений до групи ризику.

3.3. Нейробіолінгвістика як вияв корупційних маніпуляцій свідомістю

У сучасних умовах інформаційних нанотехнологій актуального значення набуває нейробіолінгвістика як всебічно складна наука. Як відомо із біомедицини, у виробленні білка значну роль відіграють синтетичні бактерії, оскільки сам білок як складова продуктів харчування сприяє довголіттю людини. Згідно даним Міжнародної організації з питань продовольства та аграрної продукції при ООН значна кількість людства не отримує від продуктів харчування необхідної кількості білка, що викликає таку тяжку хворобу як квашіокор [176, с. 247]. У процесі харчування білки підлягають гідролізу до амінокислот, які і всмоктуються в кров. Одним із шляхів вироблення білка — це введення в рослинну їжу синтетичних амінокислот завдяки необхідним бактеріям. Поряд із цим вирощують нові сорти рослин, що містять гени, відповідальні за синтез недостатніх амінокислот, які певною мірою сприяють посиленню імунної системи людського організму, оскільки виконують функцію транслокації як ферментного носія.

При цьому згідно з міжнародними професійними стандартами будь-яке медичне втручання, в тому числі з метою досліджень нейробіомозку, має здійснюватись з дотриманням професійних норм і обов'язків, та відповідних правил професійної поведінки.

При такому здійсненні медичного втручання має застосовуватися встановлене міжнародними стандартами загальне правило про те, що таке втручання може здійснюватись

лише після того, як отримання добровільної згоди від заінтересованої особи. Тобто умова про інформовану згоду пацієнта має бути застосована без будь-яких застережень. При наявних умов така особа отримує заздалегідь належну інформацію про мету і характер втручання, а також про його наслідки та ризик, оскільки заінтересована особа вільна в будь-який момент відмовитись від своєї згоди.

Доцільно зосередити увагу також і на необхідності уніфікації термінології у цій сфері, оскільки у законодавстві передбачено численні терміни і не з'ясовано, чи однакові поняття вони позначають. Це, зокрема, клінічне випробування, медичні досліди, медико-біологічні досліди, медико-біологічні експерименти [172, с. 234].

Адже міжнародні стандарти передбачають і захист осіб, які страждають на психічні розлади. Особа, яка страждає на відповідний *психічний розлад*, згідно з міжнародними стандартами, може бути піддана без її згоди медичному втручанню, проте лише такому, що спрямоване на лікування цього розладу, і лише тоді, коли відсутність лікування може завдати серйозної шкоди її здоров'ю. При цьому має бути дотримано передбачені законом умови захисту, в тому числі процедуру нагляду, контролю та подання апеляцій. Саме таких осіб використовували в клініках різних країн світу для проведення медичних експериментів. Для упередження подібних дій вважається за потрібне передбачити в законі профілактичні заходи і належну систему зовнішнього нейробіолінгвістичного моніторингу, із залученням фахівців різних закладів та спеціальної моніторингової служби.

Якщо через надзвичайну ситуацію не може бути отримана інформована згода пацієнта, може негайно здійснюватись будь-яке втручання, що є необхідним для покра-

щення стану здоров'я заінтересованої особи, але не для експерименту.

У разі, якщо на момент медичного втручання пацієнт не в змозі висловити свою волю, однак є в установленому порядку оформлене розпорядження про можливість медичного втручання щодо цієї особи, то за наявності у медичного закладу чи працівника такого підтвердження враховуються висловлені раніше пацієнтом побажання стосовно нейробіолінгвістичного втручання. Проте міжнародні стандарти попереджають про обережне поводження при дослідах та експериментах із геномом людини. Окремо варто зазначити, що втручання з метою модифікації геному людини може здійснюватись лише в профілактичних, діагностичних або терапевтичних цілях, і лише за умови, що воно не спрямоване на зміну феномену нащадків. Забороняється будь-яка форма дискримінації щодо особи за ознакою її генетичної спадковості.

У національному законодавстві також слід передбачити проведення прогностичних тестів на наявність генетичного захворювання або генетичної здатності до певного захворювання лише в медичних цілях або для наукових медичних досліджень і за умови відповідної консультації спеціаліста-генетика.

Конвенція забороняє використання допоміжних медичних технологій для вибору статі дитини, яка має народитись, за винятком випадків, коли це робиться задля уникнення серйозних спадкових захворювань, пов'язаних зі статтю [69].

Отже, при визначенні відповідальності за шкоду, заподіяну особі при проведенні над нею дослідів або експерименту, слід виходити з того, що основним безпосереднім об'єктом злочину є в цих випадках життя або здоров'я

особи, а додатковим обов'язком об'єктом такого злочину має бути порядок проведення дослідів над людиною. Об'єктивна сторона такого злочину характеризуватиметься: діями у вигляді незаконного проведення нейробіолінгвістичного дослідження над людиною, що зможе призвести до непередбачуваних наслідків для життя і здоров'я людини. Контроль над цими питаннями мають здійснювати відповідні спецслужби.

З огляду на вимоги міжнародно-правових актів з нейробіомедичних питань, пов'язаних із виготовленням, виробництвом, реалізацією та обігом лікарських засобів, пріоритетом мають бути інтереси пацієнта, які полягають у забезпеченні доступних ліків з доведеною терапевтичною ефективністю та безпекою. Саме тому конкуренція фармацевтичних компаній має бути спрямована не у бік отримання значних прибутків за будь-яку ціну, а у бік забезпечення якості та доступності продукції як головний критерій сучасності.

Контроль здійснюється у двох напрямах. Так, при надходженні лікарських засобів будь-якого виробництва в обіг контроль їх якості здійснює, крім Державної інспекції з контролю якості лікарських засобів, ще й Державна служба. Саме ці органи відповідають за якість ліків, що надходять на ринок України протягом п'яти років після їх державної реєстрації. Відповідно до чинного законодавства при виявленні неякісної продукції органи державного контролю зобов'язані вилучити її з обігу. У разі виявлення бракованої продукції, яка може певним чином вплинути на здоров'я людини (для ін'єкційних форм — однієї серії, для інших лікарських форм, що безпосередньо не контактують із кров'ю — трьох серій), органи державного контролю зобо-

в'язані вжити заходів не тільки для вилучення цих ліків, а й для припинення дії реєстраційного посвідчення [172, с. 242].

Таким чином, варто створити національну моніторингову службу, яка б могла стати складовою європейської та світової моніторингової служби з метою контролю за застосуванням лікарських засобів та їх побічною дією, а також щодо морально-психічної адекватності та необхідних форм і ступеня девіантної поведінки у відношенні юридичних і фізичних осіб.

Контрольні запитання

1. Кібербезпека особи, держави та суспільства.
2. Джерела загроз кібербезпеці особи та суспільства.
3. Які зустрічаються категорії спеціальних впливів на населення?

Теми рефератів

1. Категорії спеціальних впливів на населення.
2. Чим обумовлюється потреба правового захисту інформаційної сфери в Україні?
3. Система правопорушень в кіберсфері.

РОЗДІЛ 4. КІБЕРБЕЗПЕКА ЯК ЗАПОРУКА УСПІХУ В ПРАКТИЧНОМУ РОЗВИТКУ УКРАЇНИ ТА ІНШИХ КРАЇН СВІТУ

4.1. Аерокосмогеологічна діяльність в Україні

На сучасному етапі інформаційного розвитку окремої особи, держави та суспільства нафтогазова промисловість України є складним багатогалузевим комплексом як прерогатива діяльності спецслужб, взаємопов'язаність та взаємозалежність якого вимагає чіткої скоординованості дій у кіберпросторі. Адже запаси нафти і газу в Україні повною мірою не забезпечують нагальних потреб держави як можливість зростання їх видобутку. Тому все це вимагає проведення широкомасштабних геологорозвідувальних робіт та впровадження такого актуального методу спостереження в кібербезпеці як аерокосмічного. Саме актуальна обумовленість параметрів сучасної геодинаміки в кіберпросторі щодо деформаційних та флюїдодинамічних процесів вимагає подальшого правового вдосконалення та обґрунтування критеріїв постановки й проведення комплексних досліджень. При цьому суттєва просторова нерівномірність розподілу геокінематичних і геодинамічних параметрів — їх АНлокалізація у вузьких зонах — вимагає розроблення принципів побудови аерокосмологічних спостережних мереж у залежності від ступеню гетерогенності середовища й просторово-часового масштабу об'єктів і явищ, що вивчаються.

Сучасні правові виявлення помітних прискорень сучасних рухів земної кори, які віддзеркалюють фрактальну нелінійність рухів у часі, залежить, в основному, від точності вимірювань, частоти й кіберпросторового масштабу аерокосмогеологічних мереж спостереження стосовно області, що деформується. Тому необхідно переходити до довгоперіодичних рядів спостережень, у тому числі режимних спостережень (моніторингу) з використанням високоточного приладного парку для правового вивчення часового спектра рухів, якими займалися такі дослідники як: Ю.М. Гавриленко, В.Г. Кузнєцова, А.А. Лукк, І.А. Нерсесов, А.С. Мазницький [91, с. 14].

Для правового виявлення й аналізу тенденцій палеодинаміки щодо особливостей і властивостей сучасної геодинаміки, а також для вивчення глобальних її особливостей, проводяться дослідження в рамках міжнародних проектів і національних програм. Міжнародно правове вивчення сучасних рухів і деформацій літосферних плит, внутрішньоплитних та між плитних зон, є важливою складовою частиною міжнародної програми «Літосфера», дослідження з якої координує Комісія з літосфери Міжнародного геодезичного і геофізичного союзу.

Основні засоби виконання аерокосмічно правових програм

Із середини 1960 років у США проводяться дослідження з геодинаміки космічними методами — геодинамічна програма NASA. При цьому основними засобами виконання програми є радіоінтерферометри та лазерні далековіддалемірні (радіодалекомірні) системи. Лазерні визначення відстані досягли в кіберсучасності точності, необхідної та достатньої для геодинамічних досліджень правомірного ха-

рактеру. Проведені співставлення результатів визначення базисних ліній, отриманих за допомогою лазерної локації ШСЗ (похибки складають 2–4 см) і радіоінтерферометрії (похибки складають 1–3 см), Kolenkicwicz R. [86, с. 73], підтверджують самодостатність методів космічної геодезії щодо дослідження сучасної геодинаміки земної кори. Із 1980 року на заході США вивчаються регіональні деформації на кордонах плит за допомогою системи довго базисної радіоінтерферометрії. Виконані вимірювання довжини ліній поперек простягання розлому Сан-Андреас мають точність біля 2 см, що дозволяє реально виявляти взаємні горизонтальні зміщення плит, якщо їх швидкість більше 5 см / рік. З отриманих результатів лазерних вимірювань до ШСЗ на 900-кілометровому базисі, виконаних у 1972 р. і повторених у 1974 і 1979–1983 рр. між пунктами Куінсі (Каліфорнія) і Сан-Дієго, швидкість стиснення склала 61–65 мм / рік із похибкою 10 мм / рік. Правова значущість цього експерименту мала підтвердити зміщення Північно-Американської та Тихоокеанської плит, яке було встановлено геодезичними методами вимірювань на коротких базисах через розломи в південній Каліфорнії. Саме лазерні дослідження за допомогою ШСЗ у 1979–1982 рр. дозволили визначити відносні рухи літосферних плит по пунктах спостережень на Гавайях і в Австралії. Результати кореспондуються з моделлю рухів Тихоокеанської та Американської літосферних плит (порядок рухів 1,8 до 4,8 см / рік).

Концептуальна основа національної стратегії у питаннях безпеки

З огляду на це у Хартії про особливе партнерство між Україною та Організацією Північноатлантичного договору зазначено, що незалежна, демократична та стабільна Украї-

на є одним із визначальних факторів забезпечення стабільності в Центрально-Східній Європі та континенті в цілому. У рамках правових критеріїв розвитку між Україною та НАТО визнано, що безпека всіх держав у регіоні ОБСЄ є неподільною, що жодна країна не здатна будувати свою безпеку за рахунок безпеки іншої країни.

У взаємовідносинах Україна — НАТО важливо забезпечити підтвердження відкритості альянсу для нових демократій Європи включно з Україною; недопущення розподілу Європи на сфери впливу і домінування; гарантії свободи вибору щодо приєднання до існуючих структур безпеки; підтвердження як умови для вступу країн — кандидатів в НАТО вирішення всіх територіальних та інших проблем з сусідами, у тому числі з Україною.

Згідно зі статтею 17 Конституції України «захист суверенітету і територіальної цілісності України, забезпечення її економічної та кібербезпеки є найважливішими функціями держави, справою всього Українського народу». Формування та реалізацію єдиної політики національної безпеки [32, с. 2].

Таким чином, національна безпека України є своєрідною тріадою безпеки у взаємовідносинах людини, держави та суспільства. Адже правова політика держави у сфері національної безпеки — це цілий комплекс різноманітних напрямків діяльності, спрямований на попередження чи ліквідацію можливих проявів небезпеки [73, с. 43]. В Основному Законі держави значна увага приділяється національній безпеці та її компонентам — безпеці державній, зокрема економічній, інформаційній, екологічній тощо. Створюючи систему національної безпеки, адаптовану до міжнародних вимог, Україна прагне брати активну участь в уні-

версалізації регіональних, європейської та глобальної систем безпеки на всіх стадіях цього процесу.

4.2. Міжнародні аспекти кібербезпеки в умовах глобалізації

За умов мобільного розвитку глобального інформаційного суспільства, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набуває проблема кібербезпеки. Кібербезпека не може бути гарантована без тісної співпраці з впливовими структурами безпеки регіонального, трансрегіонального та глобального рівня. Дбаючи про свою безпеку, кожна держава або група держав мають підтримувати розбудову дієвих механізмів стабільності, розцінюючи це як важливу складову власної національної безпеки.

Особливу актуальність кібербезпека набуває в умовах приєднання України до глобальної кіберцивілізації — рівня розвитку інформаційного суспільства людства, при якому ефективність життєдіяльності його складових визначається на досягненнях науково-технічного прогресу: освоєння комп'ютерних інформаційних технологій як засобів глобальної телекомунікації [181, с. 175].

На тлі становлення глобального інформаційного суспільства та входження України у світовий інформаційний простір особливої актуальності набуває підвищення ефективності адміністративно-правового регулювання кібербезпеки. Тим більше, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю [72].

На науковому рівні основні принципи правовідносин у міжнародній інформаційній діяльності як предмет дослі-

дження знаходяться на стадії формування, в тому числі у вітчизняній науці. За останнє десятиліття у зв'язку зі спробою прискорити темпи входження України в Європейський союз, а потім в число розвинених країн, до теми кібербезпеки неодноразово зверталися вітчизняні вчені, серед яких слід виділити Б. Кормич, О. Олійника, Я. Жаркова, В. Тація, О. Кисилевич-Чорнойван, А. Логунова, В. Ліпкана та інших. В даний час правовідносини у сфері кібербезпеки досліджують такі вчені, як В. Копилов, І. Бачило, І. Арістова, В. Цимбалюк та ін.

Кібербезпека досягається шляхом балансу між інформаційними правами і свободами різноманітних суб'єктів права і захистом національного інформаційного суверенітету. Адже питання кібербезпеки, та й національної безпеки взагалі, є, насамперед, питанням балансу між правами й інтересами людини і компетенцією та інтересами державної влади, балансу, який може бути встановлений лише за допомогою правових норм.

Дуже важливим аспектом визначення принципів формування та забезпечення функціонування системи кібербезпеки є врахування міжнародних правових норм. Головна мета забезпечення кібербезпеки повинна визначатися на основі широкого розуміння цього поняття як важливої складової національної безпеки і системоутворюючого фактору всіх сфер життєдіяльності людини, суспільства, держави, політичної, економічної, соціокультурної, науково-технологічній, оборонної, екологічної, власне інформаційної складових національної безпеки.

Найважливішою умовою і змістом державної зовнішньої політики з питань кібербезпеки має бути дотримання Конституції України про те, що Україна є суверенною і не-

залежною, демократичною, соціальною, правовою державою. У ракурсі зазначеного зовнішньополітична діяльність України має бути спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигідного співробітництва з членами міжнародного співробітництва на основі загальновизнаних принципів і норм міжнародного права. Участь у міжнародних та регіональних системах кібербезпеки є актуальною необхідністю сучасності. В умовах інформаційної революції та глобалізаційних інформаційних процесів, загострення інформаційної боротьби, окремій державі самостійно забезпечувати власну кібербезпеку проблематично. Глобалізаційні інформаційні процеси, глобальні комунікаційні системи вивели забезпечення кібербезпеки за межі юрисдикції однієї держави і вимагають участі у вирішенні цих проблем як на рівні світових, так і регіональних спільнот.

Глобалізаційні перетворення зумовлюють необхідність двовекторності інформаційної політики. По-перше, відсутність територіальних кордонів в єдиному інформаційному просторі сприяє набуттю кібербезпекою наднаціонального характеру. Міжнародна правова регламентація інформаційних відносин повинна гарантувати досягнення балансу інтересів усіх суб'єктів, недопущення домінування однієї зі світових культур у якості еталона та формування глобальної інформаційної системи на основі партнерства та консенсусу щодо основних загальнолюдських цінностей [124, с. 17–18]. По-друге, відсутність інформаційних кордонів сприяє розмиванню культур, що може спричинити загальну культурну деградацію людства. Тому особливо важливим є усвідомлення нових інформаційних загроз глобального масштабу та відображення його у виваженій національній політиці

забезпечення кібербезпеки суспільства, що дозволить виключно конструктивне використання потенціалу інформаційного суспільства. Роль кожної держави в такому випадку полягає у сприянні розвитку інформаційних процесів через створення різноманітних економічних, правових, ідеологічних та інших умов існування національного інформаційного простору.

Українські дослідники з Національного інституту стратегічних досліджень останнім часом активно розробляють загальнотеоретичні проблеми становлення інформаційного суспільства в Україні в контексті глобальних інформаційних процесів, формування інформаційної політики в Україні, зазначаючи провідну роль інформаційних технологій у модернізації суспільства. Зокрема, глибоко аналізуються процеси становлення та стратегії розвитку інформаційної політики в Україні. В контексті глобалізації інформаційних систем розглядаються концептуальні засади державної політики України в електронній сфері, розкриваються категорії — «інтереси особистості», «інтереси суспільства», «інтереси держави» в електронній сфері, аналізується питання кібербезпеки України. На основі світового досвіду характеризується роль інформаційних технологій як чинника суспільних перетворень. Виходячи з реалій формування світового інформаційного простору, дослідники роблять висновок про те, що електронна сфера поступово стає вирішальним чинником розвитку сучасної країни, відзначають, що найважливішою складовою сучасної інформаційної сфери є комп'ютерні мережі, серед яких найбільшого значення набула глобальна мережа «Інтернет» [163, с. 611–686].

Вітчизняні дослідники Ф. Медвідь та Р. Буга основним базовим національно-державним інтересом, геополітичним

пріоритетом і стратегічним завданням зовнішньополітичного курсу України в умовах глобалізації вбачають її виживання, підвищення життєспроможності та зміцнення як вільної, суверенної, незалежної держави сучасного світу за умов збереження національних цінностей, захисту економічного та політичного суверенітету, власної соціально-культурної ідентичності, перетворення з об'єкта геополітичних ігор на повноцінний суб'єкт геополітики, тобто на самостійного гравця, який визначає свої цілі і дії на міжнародній арені [102, с. 115].

У міжнародній практиці основу інформаційних ресурсів представляють національні інформаційні ресурси як суспільне надбання, культурна спадщина людства, яке оберігається міжнародним співтовариством для задоволення культурних і духовних потреб кожного. Для забезпечення свого суверенітету держави можуть встановлювати режим обмеженого доступу передачі інформації в інші держави тощо.

Найважливішою ознакою інформаційного суспільства є можливість кожного створити інформацію і знання, мати до них доступ, користуватися і обмінюватися ними.

Основна мета інформаційного суспільства — надати можливість людям реалізовувати свій інтелектуальний потенціал, свої можливості і здібності, сприяючи постійному розвитку та підвищенню рівня свого життя.

У практиці формування інформаційного суспільства в різних країнах виділяють три основних моделі: європейську, американську та азіатську [17, с. 52].

Європейська модель розвитку інформаційного суспільства характеризується соціальною орієнтованістю і активним залученням держави та міжнародних інституцій. Органи ЄС реалізують низку програм розвитку інформа-

ційного суспільства та створення Єдиного європейського інформаційного простору. Ці програми орієнтовані на забезпечення прав і свобод громадян, розвитку інформаційної інфраструктури, вільного доступу до неї та інформованості суспільства, створення пільгових умов для розвитку підприємництва у сфері інформаційних технологій.

Ознакою європейської моделі інформаційного суспільства є варіативність політичної спрямованості програм побудови та розвитку національних складових об'єднаної Європи, обумовлених новою регіональної геополітикою, становленням інформаційної (інтелектуальної) економіки держав, інформаційного законодавства, різними можливостями постіндустріального розвитку [180, с. 185].

При цьому варто підкреслити, що адміністративно-правові практики, на наш погляд, необхідно розглядати на рівні особи, держави та суспільства.

Американська модель розвитку інформаційного суспільства. Цій моделі основне навантаження щодо інформатизації, розвитку інформаційної інфраструктури припадає на приватний сектор. Держава забезпечує регулювання інформаційної діяльності, вільну конкуренцію, бере участь у реалізації найбільш масштабних проектів. Враховуючи передову роль приватного сектора, ця модель є більш комерціалізованою, орієнтованою на насичення ринку комерційними інформаційними продуктами і послугами.

Азіатська модель інформаційного суспільства, в якій більшість завдань з інформатизації вирішуються в межах взаємодії держави і великих корпорацій. Крім цього, приділяється увага також забезпеченню повсякденних потреб суспільства, доступності інформаційних продуктів і послуг.

Україна не стоїть осторонь процесу формування інформаційного суспільства. Одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати знання та інформацію, мати вільний доступ до них, обмінюватися, користуватися ними, сприяючи таким чином громадському і особистому розвитку та підвищенню якості життя. Більш того, в Україні сформовані правові засади побудови інформаційного суспільства: прийнято Закони України «Про Концепцію Національної програми інформатизації» та «Про Національну програму інформатизації», інших нормативно-правових актах, які регулюють суспільні відносини щодо створення інформаційних електронних ресурсів, захисту інтелектуальної власності на ці ресурси, впровадження електронного документообігу, захисту інформації. Ці та інші передумови дозволяють вважати, що український ринок інформаційно-комунікаційних технологій перебуває в стані активного становлення і може стати фундаментом розвитку інформаційного суспільства в Україні.

Сучасна міжнародна інформаційна діяльність визначається як один із провідних напрямків в умовах становлення глобального інформаційного суспільства, глобальної інформаційної цивілізації, глобального міжнародного інформаційного порядку, кібербезпеки міжнародного співтовариства [180, с. 164].

Особливу увагу інформаційні ресурси набувають в сучасних умовах швидкої глобалізації інформаційних процесів і прагнення розвинених країн досягти інформаційного домінування заради власних національних інтересів, завдань і так

далі. Саме тому стає необхідним дослідження проблем забезпечення кібербезпеки в сучасному глобалізованому світі.

Кібербезпека розглядається як глобальна проблема захисту інформації, захисту інформаційного простору та інформаційного суверенітету. Практичне розв'язання проблем кібербезпеки, притягнення до відповідальності за порушення або загрозу інформаційній безпеці у кожній державі здійснюється у порядку, передбаченому нормами міжнародного права, відповідними міждержавними договорами, а також внутрішнім законодавством. Кібербезпека регулюється певними нормами міжнародного права, які зафіксовані в документах ООН і ЮНЕСКО, в документах європейських міжнародних організацій, а також у нормативних актах окремих держав. Кожна розвинута країна має закони про захист інформації в різних галузях. Наприклад, Франція має Закон «Про інформацію, інформаційні файли і права людини», Німеччина, Австрія, Бельгія, Данія, Ірландія — Закон «Про захист інформації», Фінляндія, Ісландія — Закон «Про захист інформації про особу», Люксембург — Закон «Про використання інформації в процесі роботи з комп'ютером» [82, с. 39].

Межі національного інформаційного простору визначаються з інформаційного суверенітету держави — здатності держави контролювати і регулювати потоки інформації з-за меж держави з метою додержання національних законів, прав і свобод громадян, а також здатність держави гарантувати національну і державну кібербезпеку, як складових міжнародної кібербезпеки [180, с. 73].

На думку дослідників, інформаційний суверенітет виступає володінням і розпорядженням національними інформаційними ресурсами, які включають усю належну

державі інформаційну інфраструктуру, інформацію — незалежно від змісту, форми, часу і місця її створення, і забезпечується виключним правом держави на формування і здійснення національної інформаційної політики, власності на інформаційні ресурси, сформовані за державний кошт, створенням національних систем інформації, встановленням режиму доступу інших держав до інформаційних ресурсів України [111, с. 9].

У міжнародних інформаційних відносинах зберігається принцип суверенітету держави щодо її інформаційних ресурсів. Стаття 53 Закону України «Про інформацію» [141] декларує, що основою інформаційного суверенітету України є національні інформаційні ресурси. До інформаційних ресурсів України Закон відносить всю належну їй інформацію, незалежно від змісту, форм, часу, і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними за винятком випадків, передбачених законами і міжнародними договорами.

Стаття 54 цього Закону визначає, що інформаційний суверенітет України забезпечується:

- виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету;
- створенням національних систем інформації;
- встановленням режиму доступу інших держав до інформаційних ресурсів України;
- використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами.

Як справедливо зазначено І. Арістовою: «Інформаційний простір є основою соціально-економічного, політичного і культурного розвитку та забезпечення безпеки України.

Ефективне інформаційний простір повинен забезпечити побудову інформаційного суспільства в країні і входження її у світовий інформаційний простір» [15, с. 106].

До основних ознак і характеристик інформаційного простору країни дослідники відносять: єдині принципи і загальні правила взаємодії всіх суб'єктів інформаційної діяльності; наявність умов для безпечної інформаційної взаємодії держави, організацій і громадян; максимально повне задоволення інформаційних потреб держави, організацій і громадян на всій території країни; рівнодоступность суб'єктів інформаційної діяльності до відкритих інформаційних ресурсів і їх правова рівність; збереження балансу інтересів країни і світового співтовариства при входженні її в глобальний інформаційний простір і забезпечення власного інформаційного суверенітету [114, с. 253].

Українські дослідники С. Кудрявцева і В. Колос виділяють чотири основні напрями забезпечення безпеки національного інформаційного простору:

1. Захист інформації, захист національних інформаційних ресурсів.

2. Законодавчо-нормативне забезпечення захисту інформації.

3. Організаційно-технічне забезпечення інформаційної достатності.

4. Здійснення інформаційної експансії у світовий інформаційний простір з метою забезпечення національних інтересів [82, с. 30].

Уперше питання доступу до інформації на наднаціональному рівні було винесено на обговорення Ради Європи 21–23 вересня 1976 р. в м. Грозі, де було проведено колоквіум на тему: «Свобода інформації — обов'язок державних

органів забезпечувати доступ до інформації» [137, с. 189]. Висновки колоквіуму розглядалися Координаційним комітетом прав людини на його третьому засіданні (8-12 травня 1978 р.), де й було вирішено заснувати Комітет експертів для вивчення пропозицій, висловлених на колоквіумі. Комітет запропонував підготувати рекомендацію державам-членам із цього питання. Парламентська Асамблея Ради Європи схвалила 1 лютого 1979 р. Рекомендацію N1 854 (1979) про доступ громадськості до інформації, що є в розпорядженні державних органів, і свободу інформації. Беручи до уваги цю Рекомендацію, Комітет Міністрів Ради Європи затвердив у 1981 році Рекомендацію Rec(81)19E «Про доступ до інформації, що є в розпорядженні державних органів» [137, с. 190]. У 2002 р. Комітет Міністрів Ради Європи схвалив нову розширену Рекомендацію Rec(2002)2 «Про доступ до офіційних документів» (2002) [138, с. 86].

Остаточним визнанням права на доступ до інформації європейською спільнотою стало ухвалення Конвенції Ради Європи про доступ до офіційних документів (CETS № 205), яка була відкрита для підписання в червні 2009 р. [7]. Це перший у світі юридично обов'язковий для держав-учасниць багатосторонній міжнародний договір з цього питання. Конвенція набере чинності після 10 ратифікацій.

Розвиток міжнародних інструментів захисту прав людини зумовив те, що « ...в сучасному міжнародному праві сформувалася галузь, об'єктом якої є міжнародні відносини в галузі прав людини та основних свобод» [168, с. 107]. Міжнародно-правові акти, інструменти та інституції, які забезпечують її права у випадках недостатності або неефективності національних інструментів захисту являють собою важливий елемент кібербезпеки людини.

Основними документами, які визначають міжнародні стандарти права на доступ до публічної інформації, на сьогодні є:

1) Конвенція Ради Європи про доступ до офіційних документів від 18.06.2009;

2) Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля (ратифікована Законом України № 832-XIV від 06.07.99 р.);

3) Йоганесбурзькі принципи. Національна безпека, свобода висловлювань і доступ до інформації;

4) документи міжнародної організації «Артикль 19» (Article 19), зокрема: «Право громадськості знати. Принципи законодавства про свободу інформації», Модельний закон про свободу інформації;

5) «Про доступ до офіційних документів», Рекомендація Rec(2002) 2 Комітету Міністрів Ради Європи від 21.02.2002;

6) «Про доступ до інформації, що перебуває в розпорядженні державних органів», Рекомендація № R(81) 19 Комітету Міністрів Ради Європи від 25.11.1981;

7) «Про доступ громадськості до інформації, що є в розпорядженні державних органів, і свободу інформації», Рекомендація № 854 (1979) Парламентської Асамблеї Ради Європи;

8) «Про право на недоторканість приватного життя», Резолюція № 1165 (1998) Парламентської Асамблеї Ради Європи;

9) практика Європейського суду з прав людини.

Відповідно до перелічених міжнародних документів основними міжнародними стандартами у сфері права на доступ до інформації є:

- принцип максимальної відкритості — уся інформація у володінні публічних органів є відкритою, крім передбачених законом винятків;
- відомості, доступ до яких закривається, мають бути ясними, описуватися вузько і відповідати контролю згідно з «трискладовим тестом», а саме: 1) інформація повинна мати відношення до легітимної мети, передбаченої законом; 2) оприлюднення інформації повинно загрожувати спричиненням суттєвої шкоди вказаній легітимній меті; 3) шкода, яка може бути заподіяна вказаній меті, має бути вагомішою, ніж суспільний інтерес в отриманні інформації;
- обсяг інформації, доступ до якої обмежується, про публічну особу має бути значно меншим, ніж обсяг інформації про приватну особу;
- процедура доступу до інформації має бути чітко визначеною, а загальний строк надання інформації за запитом — стислим;
- передбачено не лише право на доступ до інформації, якою володіють органи державної влади та місцевого самоврядування, а й до інформації, яка належить приватним організаціям, якщо оголошення цієї інформації зменшить ризик шкоди головним суспільним інтересам;
- наявність спеціальний позасудовий механізм захисту права на доступ до інформації (інформаційний уповноважений);
- захист «викривачів» («whistleblowers»).

Головним міжнародно-правовим стандартом у галузі прав людини є комплексний акт, розроблений в рамках ООН і відомий як Хартія про права людини. Цю Хартію складають Загальна декларація прав людини, Міжнарод-

ний пакт про економічні, соціальні і культурні права і Міжнародний пакт про громадянські та політичні права. Ці акти стали головним стандартом і базою, на основі яких були розроблені цілий ряд інших міжнародних і національних правових актів у галузі прав людини, в тому числі відповідних розділів конституцій багатьох держав світу, зокрема і Розділ II «Права, свободи та обов'язки людини і громадянина» Конституції України 1996 р.

Першим фундаментальним міжнародно-правовим актом в рамках Хартії про права людини є Загальна декларація прав людини, прийнята Генеральною Асамблеєю ООН 10 грудня 1948 року. Ця декларація містить цілий комплекс юридичних гарантій, які визначають зміст і сутність кібербезпеки особи.

В результаті, норми статті 19 Загальної декларації прав людини встановлюють, що «кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів» [49].

Пошуки адекватних відповідей на виклики міжнародного розвитку представляють основу багатостороннього співробітництва України в галузі інформації та комунікації, свободи вираження та розвитку нових інформаційних технологій. Україна здійснює реформування інформаційної сфери для забезпечення національної участі в міжнародних програмах становлення інформаційного суспільства та європейської інтеграції, для вирішення внутрішніх державотворчих проблем, трансформації економіки та використання глобального інтелектуального надбання. Зараз сус-

пільство переживає етап проникнення інтелектуальних інформаційних технологій в різні сфери діяльності людини. Суспільство знань та інформації несе людству нові виклики і величезні можливості для вирішення його проблем та забезпечення його подальшого розвитку. Україна має можливість зробити свій великий внесок у формування міжнародної політики забезпечення кібербезпеки.

Всі країни зацікавлені в розвитку глобального інформаційного суспільства та використанні нових можливостей, які відкриваються завдяки поліпшенню доступу до інформації та кращому забезпеченню інформацією. Особливу увагу інформаційні ресурси набувають в сучасних умовах швидкої глобалізації інформаційних процесів і прагнення розвинених країн досягти безперечного інформаційного домінування заради вирішення своїх національних завдань. Саме тому стає необхідним ретельне дослідження теоретичних і практичних проблем кібербезпеки в сучасному глобалізованому світі.

Серед науковців триває дискусія щодо визначення сутності, вимірів, форм та механізмів глобалізації, наслідків її впливу на національну культуру та особистість. Окремі суспільства держави і регіони все більше набувають ознаки частин глобального цілого. Розвиток соціальної структури сучасних суспільств набуває наднаціональний вимір, народжується суспільство другого порядку — глобальне суспільство.

Адже початок XXI століття відзначився підписанням 22 липня 2000 року історичного для цивілізації документа — Окінавської хартії глобального інформаційного суспільства. В перших рядках Хартії лідери країн великої вісімки визнали розвиток інформаційно-комунікаційних технологій одним з найбільш важливих факторів формування

сучасного суспільства, що здійснює революційний вплив на спосіб життя людей, їх освіту і роботу, а також взаємодію уряду та громадянського суспільства. «Глобальне» «відкрите» «інформаційне» суспільство та єдиний інформаційний простір повинні стати базисом для розвитку, в першу чергу, глобального фінансово-економічного простору та потенціалом для творчого вирішення економічних, соціальних проблем та реалізації людьми своїх прагнень [118].

Очевидно, що розгортання глобалізаційних процесів не обмежується лише інформаційною та економічною сферою. Логічним наслідком є подальша глобалізація культурної, правової, наукової, освітньої та інших сфер суспільного життя, яка тягне за собою і глобальні соціальні проблеми, що можуть набути нищівного для суспільства характеру. Найвідчутніший наслідок інформаційної глобалізації — уніфікація змісту інформації на фоні домінування економічно сильних і політично впливових націй на всесвітньому інформаційному ринку, що кидає виклик культурній самобутності нації [151, с. 193]. Практика європейської інтеграції довела, що втрата самоідентифікації є одним з найнебезпечніших викликів суспільству, який в європейській свідомості поступається місцем тільки тероризму. Причиною такої ситуації є циркуляція великих, практично неконтрольованих, потоків інформації, що поступово стирають соціокультурні межі. Крім цього, небезпеки глобалізації полягають у можливості масової культури маніпулювати свідомістю, нав'язуванні чужих світоглядних концепцій, руйнуванні традиційної культури і менталітету [154, с. 25].

З метою прискорення входження в інформаційну еру Україна вступила в такі міжнародні організації, як Міжнародний Союз електрозв'язку, Європейська конференція

адміністрацій пошти і зв'язку, Європейський інститут телекомунікаційних стандартів і Регіональне співтовариство в області зв'язку [63, с. 52].

Проблемами збалансованого обміну інформацією займаються організації, які вважаються суб'єктами міжнародного права: ООН, Рада Європи, Європейський Союз, НАТО, ЮНЕСКО, СНД, Всесвітня організація інтелектуальної власності та ін. Головними напрямами інформаційного співробітництва між ними є нарощування потужності регіональних телекомунікаційних мереж, формування інтелектуального потенціалу Європи та створення правової бази для функціонування регіонального інформаційного ринку.

Проблема кібербезпеки ґрунтується на фактичній залежності всіх сфер життєдіяльності суспільства і держави (економіки, політики, науки, культури), забезпечення національної та міжнародної безпеки, від конструктивного обміну інформацією, надійного функціонування інформаційних і телекомунікаційних систем, якісних технологій і коштів.

Міжнародне співробітництво у сфері кібербезпеки включає:

- розробку нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі кібербезпеки;
- входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на спільне вирішення проблем кібербезпеки;
- участь у роботі керівних, виконавчих та забезпечуючих підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів [46, с. 20].

На 56-й сесії Генеральної Асамблеї ООН було дано таке визначення терміна «кібербезпека»: «Інформаційна та ме-

режева безпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації та створення надійного джерела постачання обладнання, послуг та інформації» [63, с. 97].

У сферу кібербезпеки держави входять конкретні дії щодо забезпечення безпечних умов існуючих інформаційних процесів і розвитку таких процесів у майбутньому. Це охоплює регулювання питань захисту самої інформації, захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів. Досягти цього можливо за умови проведення необхідної державної політики кібербезпеки та створення необхідних правових та організаційних основ.

А. Логунов звертає увагу на те, що загальновизнаним у світі фундаментом міжнародного права є статут ООН, цілі, принципи та інші установки ООН є основою чинного міжнародного права. Статут ООН займає вищу позицію в ієрархії міжнародно-правових норм, що регулюють різні аспекти міжнародного життя, в тому числі і міжнародну безпеку. Статут ООН закріпив мета «сприяння економічному та соціальному прогресу всіх народів» [89, с. 217].

Аналіз правових норм Статуту ООН є підставою для висновків: цілі ООН закріплюються і реалізуються принципами, які є загальними принципами міжнародного права; принципи є важливими складовими механізмів як міжнародної безпеки, так і національної безпеки будь-якої країни [4].

Принципи формування та забезпечення функціонування системи кібербезпеки повинні бути спрямовані на реалізацію головної мети державної політики і визначатися

законом як важливі складові правових механізмів регулювання відносин у цій системоутворюючій складовій забезпечення національної безпеки.

Законом України «Про основи національної безпеки України» визначені основні принципи забезпечення національної безпеки, якими є: пріоритет прав і свобод людини і громадянина; верховенство права; пріоритет договірних (мирних) засобів у розв'язанні конфліктів; своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам; чітке розмежування повноважень та взаємодія органів державної влади у забезпеченні національної безпеки; демократичний цивільний контроль над Воєнною організацією держави та іншими структурами в системі національної безпеки; використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Відповідно до Закону України «Про національну безпеку України» наша держава має боротись проти міжнародного тероризму шляхом участі у заходах, які організовуються міжнародними організаціями для того, щоб вживати конкретних акцій для боротьби з міжнародними організованими злочинними угрупуваннями та міжнародним терористами. До цих заходів входить і протидія інформаційним загрозам. Україна, як і багато інших держав, приєдналась до багатьох міжнародних договорів щодо боротьби з тероризмом і прийняла низку національних законів, що надають додаткові повноваження правоохоронним органам та органам національної безпеки для боротьби з тероризмом. Сьогодні Україна є стороною 12 універсальних антитерористичних конвенцій, у тому числі у сфері боротьби з фінансуванням тероризму. Участь громадських організацій у

підтримці цих зусиль може лише вітатись. В цьому контексті у Міністерстві закордонних справ існує громадська рада, у нас активно відбуваються зустрічі із представниками громадських організацій для реалізації зовнішньої політики.

Варто також наголосити на тому, що участь громадських організацій у заходах по зміцненню безпеки у боротьбі з тероризмом є важливою, і в цьому контексті підтримка громадськими та політичними організаціями курсу на вступ України до Євросоюзу буде якнайбільше сприяти тому, щоби наша держава дійсно почувала себе у найкращих умовах безпеки.

Важливим також є врахування принципів міжнародного права, спрямованих на забезпечення національної безпеки та її складової кібербезпеки.

Статутом ООН визначені наступні принципи міжнародного права.

1. Принцип суверенної рівності. Стаття 2 статуту ООН встановлює, що організація заснована на принципі суверенної рівності всіх її членів.

2. Принцип сумлінного виконання міжнародно-правових зобов'язань. У Декларації про принципи міжнародного права 1970 р встановлено, що вказаний принцип поширюється тільки на зобов'язання, прийняті відповідно до Статуту ООН.

3. Принцип мирного вирішення міжнародних конфліктів.

4. Принцип незастосування сили встановлює, що всі члени ООН утримуються у своїх міжнародних відносинах від загрози силою або її застосування. При цьому вважаємо за доцільне звернути увагу на те, що Статут ООН передбачає застосування сили або загрози сили тільки в наступних випадках:

1) за рішенням Ради Безпеки ООН у разі наявності загрози миру; будь-якого порушення миру або акту агресії; 2) для здійснення права на самооборону у разі збройного нападу до прийняття Радою Безпеки відповідних заходів для встановлення міжнародного миру і безпеки.

5. Принцип поваги прав людини. Остаточна його редакція була визначена Заключним актом Наради з безпеки і співробітництва в Європі 1975 р.

6. Принцип невтручання в справи, що відносяться до компетенції будь-якої держави.

7. Принцип територіальної цілісності. Гельсінські угоди 1975 р. визначив цей принцип в якості самостійного принципу.

8. Принцип непорушності кордонів держав.

9. Принцип рівноправності і самовизначення народів. Цей принцип реалізує одну з найважливіших цілей ООН, якою є розвитком дружніх відносин між націями і зміцнення загального миру.

10. Принцип співробітництва зобов'язує держави здійснювати свою діяльність в рамках Статуту ООН, спрямовану на забезпечення миру і безпеки та сприяння економічному зростанню у всьому світі.

Наведені принципи міжнародного права доцільно враховувати при реалізації державної політики щодо участі України у міжнародних та регіональних системах кібербезпеки як повноправного, суверенної і незалежної держави, яка є членом ООН з відповідними правами, обов'язками і відповідальністю.

Правові норми міжнародного права, закріплені в Статуті ООН, створили умови для використання в інтересах України міжнародних і регіональних систем кібербезпеки.

Найважливішим органом міжнародної колективної безпеки є Генеральна Асамблея ООН, має широкі повноваження з питань підтримання миру і безпеки народів. Головним постійно діючим органом цієї організації є Рада Безпеки ООН. Україна, як член ООН має не тільки право, а й можливість ставити перед Генеральною Асамблеєю ООН і її постійно діючим органом — Радою Безпеки ООН актуальні проблеми як міжнародної, так і власної кібербезпеки. Рішення Ради Безпеки ООН є обов'язковими для виконання державами-членами ООН. Рада Безпеки ООН має широкі повноваження з питань прийняття рішень, спрямованих на підтримання міжнародного миру та безпеки. У 1999 р. Генеральною Асамблеєю ООН прийнята резолюція з питань кібербезпеки в умовах розвитку телекомунікацій, яка закликає членів Організації до активної участі в розробці норм міжнародного права в регулюванні міжнародних відносин у цій сфері діяльності [9].

У цьому зв'язку закономірно, що одним з важливих напрямів державної зовнішньої політики з питань кібербезпеки має бути співпраця України з НАТО в рамках програми «Партнерство заради миру». Взаємне забезпечення кібербезпеки на узгоджених умовах має бути одним з важливих напрямків співпраці з Північноатлантичним альянсом. Доречно нагадати про те, що зі штаб-квартирою НАТО і України більше десяти років діє угода про взаємний захист секретної інформації, якою здійснюється обмін в процесі співпраці. Певні можливості з питань забезпечення кібербезпеки має співробітництво на взаємно узгоджених умовах з ОБСЄ, структурами безпеки, що формуються ЄС. Україні ще належить визначити активну позицію з питань забезпечення власної кібербезпеки в рамках Орга-

нізації Договору про колективну безпеку (ОДКБ) країн СНД [119, с. 87].

Наявна науково-дослідна база, цілі та принципи міжнародного співробітництва, визначені Статутом ООН, створюють необхідні умови для забезпечення реалізації державної зовнішньої політики кібербезпеки відповідно до конституційних правовими нормами, закріпленими Основним законом України.

Україна бере активну участь у розробці питань кібербезпеки в рамках ООН. Так, за ініціативою України в ООН та її спеціалізованих установах були обговорені проблеми узгодження міжнародної стратегії інформаційної політики, міжнародно-правові аспекти функціонування мережі Інтернет.

Проблемами кібербезпеки, крім ООН, займаються також регіональні організації. Концепція регіональної політики у сфері кібербезпеки зумовила позиції країн ЄС, НАТО та ОБСЄ з інформаційного виміру європейської безпеки, сприяє пошуку спільних рішень у протидії інформаційним та комунікаційним загрозам, визначає пріоритети політики в сфері безпеки. У Європі мета політики кібербезпеки полягає в тому, щоб захистити цілісність інформації та інформаційної системи, гарантувати належні умови її звернення і цінність. Ці завдання необхідні для забезпечення незалежного здійснення державної політики і надійного використання інформаційно-комунікаційних технологій в соціальних та економічних областях.

Сучасний етап становлення громадянського суспільства визначається входженням України до провідних технологічно розвинутих країн світу, до глобального інформаційного простору. Саме тому Україна має використовувати досвід

таких країн, що вже мають досить серйозні напрацювання у сфері забезпечення кібербезпеки, зокрема досвід Європейського Союзу. Процеси глобалізації, які передбачають якісно новий рівень міждержавного співробітництва і конкуренції на міжнародній арені, стратегія європейського вибору України зумовлюють актуалізацію для вітчизняного правознавства завдання щодо аналізу актуальних проблем розвитку держави і права в контексті спільного європейського науково-дослідницького простору [167, с. 58].

Вирішення проблем кібербезпеки в межах Європейського союзу передбачає створення спільної стратегії європейської кібербезпеки, протидії кібервійни, інформаційному тероризму і боротьбі з інформаційною злочинністю.

Вступ України до Ради Європи, членство в Європейській телерадіомовній спілці полегшують її входження в європейський і разом з тим світовий масово-комунікаційний простір, надають нових можливостей для укладання міждержавних угод із сусідніми країнами про транскордонне теле- і радіомовлення, дають змогу поглиблювати кооперацію і співпрацю між європейськими та вітчизняними масово-комунікаційними системами. Водночас доведено, що членство в європейських структурах зобов'язує Україну дотримуватися встановлених ними міжнародних норм, виконувати міжнародні угоди і конвенції, включаючи документи щодо регуляції у сфері інформації та комунікації. За цих умов ставка, зазначає О. Зернецька, повинна бути зроблена на співпрацю не тільки з урядами, а й з міжнародними неурядовими організаціями завдяки впровадженню високошвидкісної інтерактивної диджитальної інформаційної мережі (тобто використання в комп'ютерній техніці та телекомунікаціях запису, передачі та обробки інформації за

допомогою бінарно-кодових знаків) для багатомовної комунікації з усім світом, використовуючи аудіо-, відео-, друковану комунікацію та комунікацію даних. Медіа- і віртуальна дипломатії повинні усвідомлюватись політичними лідерами України не просто як паблік рілейшнз, а як політична і економічна необхідність сталого розвитку нашої держави на порозі інформаційної ери [57, с. 323–335].

Роль інформатизації суспільства відображається у політичній модернізації. Принципово важливе значення інформаційних і комунікаційних технологій полягає в тому, що їхнє використання дає змогу розширити права громадян шляхом надання доступу до різноманітної інформації, збільшити ступінь їхньої участі в прийнятті політичних рішень і контролю за діяльністю державної влади, надати можливість активно виробляти якісну інформацію, а не тільки її споживати.

Використовуючи засоби економічного, інформаційного, політичного та міжнародно-правового впливу, глобалізація суттєво змінює розуміння концепції суверенної національної держави, оскільки все значнішу роль в управлінні державотворчим процесом покладається на наднаціональні утворення.

У Посланні Президента України до Верховної Ради України «Європейський вибір. Концептуальні засади стратегії економічного та соціального розвитку України на 2002–2011 роки» визначено, що курс на європейську інтеграцію є природним наслідком здобуття Україною незалежності. Європейський вибір України — це рух до стандартів інформаційного суспільства, соціально орієнтованого ринкового господарства, яке базується на засадах верховенства права, забезпечення прав та свобод людини та громадянина.

Внаслідок розвинутого інформаційно-технічного розвитку Євросоюзу, особливого значення в діяльності ЄС набуває проблема забезпечення кібербезпеки.

Спільна позиція країн-членів Європейського Союзу щодо змісту поняття «кібербезпека» була висловлена представником Швеції при обговоренні питань міжнародної кібербезпеки на 56-й сесії Генеральної Асамблеї ООН, згідно з якою кібербезпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації.

Серед основних європейських нормативно-правових актів, що регулюють суспільні відносини у сфері побудови інформаційного суспільства є Окінавська хартія глобального інформаційного суспільства від 22 липня 2000 року. В документі зазначається, що інформаційне суспільство дозволяє людям використовувати свій потенціал та реалізовувати свої спрямування в сфері інформаційно-комунікаційних технологій.

Завданням всіх суб'єктів міжнародної спільноти та окремої людини полягає не тільки стимулювання та сприяння переходу до інформаційного суспільства, а також в повній реалізації його економічних, соціальних та культурних переваг [118].

Слід зазначити, що в Окінавській хартії особливу роль посідає боротьба з комп'ютерною злочинністю як однієї з найнебезпечніших загроз інформаційного суспільства. Так, нормативно закріплено, що зусилля міжнародного співтовариства, спрямовані на розвиток глобального інформаційного суспільства, мають супроводжуватись узгодженими

діями зі створення безпечного та вільного від злочинності кіберпростору. Подальшого розвитку дані положення Хартії знайшли відображення в Європейській Конвенції «Про кіберзлочинність» від 23 листопада 2001 року, який був підписаний тридцятьма країнами, серед яких і Україна, з метою вироблення єдиної ефективної позиції протидії кіберзлочинам [93, с. 225].

Цікавим з точки зору кібербезпеки є досвід регулювання Інтернет-відносин деяких європейських країн. У більшості європейських країнах прийняті закони, що дають можливість притягнути до відповідальності провайдерів хостових послуг за розміщення на їхніх сайтах інформації незаконного змісту. Мережеві оператори не можуть бути притягнуті до відповідальності за зміст інформації, яка передається мережами, однак вони зобов'язані на умовах виданих ліцензій вжити необхідних заходів щодо користувачів і клієнтів, які використовують мережі для передання інформації незаконного змісту [93, с. 56].

Кібербезпека також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем може створити загрозу міжнародній безпеці.

До основних напрямів інформаційної політики ЄС належать:

1) політика лібералізації і приватизації телекомунікацій;

2) розвиток інформаційних послуг та мереж;

3) розвиток технічного і соціально-інформаційного забезпечення;

4) протидія інформаційним монополіям;

5) створення ринку інформаційних послуг;

6) недискримінація за інформаційною ознакою.

Створення інформаційного законодавства та сприйнятливої законодавчої бази, яка враховує як національні, так і міжнародні принципи регулювання інформаційних відносин, вважається головним чинником зростання прибутку країни від потенціалу інформаційно-комунікаційних технологій.

Новою стратегічною метою Європейського Співтовариства до 2015 року визнано удосконалення інформаційної та телекомунікаційної структур, стимулювання інноваційної діяльності, модернізацію системи освіти [85, с. 235].

Глобальні процеси впливають на національні та регіональні відносини, і завдання європейської спільноти полягає в узагальненні позитивних і негативних наслідків становлення інформаційного суспільства, трансформації демократичних інститутів, охорони основних прав і свобод людини в нових умовах, в захисті плюралізму і незалежності засобів масової комунікації, збереженні національного розвитку, культурної самобутності і мовного розмаїття країн Європи.

Відтак, Європейський Союз має достатньо досвіду у сфері становлення та розвитку інформаційного суспільства, де особливе місце приділено питанням забезпечення кібербезпеки.

Україна має використовувати позитивний досвід Євросоюзу, імплементувати положення законодавства, які сприятимуть ефективному регулюванню суспільних відносин в електронній сфері. Входження до європейських структур має розглядатися як інструмент реалізації національних інтересів.

Кібербезпека в НАТО охоплює стратегії інформаційної політики та інформаційного протиборства в контексті пе-

реосмислення стратегії безпеки XXI століття, створення системи регіональної кібербезпеки, здійснення спеціальних інформаційних операцій, роз'яснення цілей діяльності НАТО громадськості тощо.

Діяльність ОБСЄ в області кібербезпеки полягає у визначенні загальних підходів щодо прогнозування конфліктів, моніторингу кризових ситуацій, прийняття документів з кібербезпеки та застосуванні заходів превентивної дипломатії.

Таким чином, інформаційна політика міжнародних організацій, яка реалізується через міжнародну інформаційну діяльність, спрямована на політичну, економічну та культурну інтеграцію спільнот на основі використання нових перспективних технологій, створення ефективної системи забезпечення прав людини на вільний доступ та обмін інформацією як умови демократичного розвитку та ціннісно-смисловим орієнтирам.

Сьогодні дуже важливою є необхідність усвідомлення владою, політичною елітою, наукою, що забезпечення національної безпеки і всіх її складових, законотворча робота, прогнозування, перспективне і поточне планування, розробка стратегій, концепцій, доктрин, програм і проектів, напрямків сталого розвитку, державне управління, міжнародне співробітництво починається з інформаційного рівня. Інформаційна складова пронизує всі сфери життєдіяльності людини, соціальних систем. На цьому етапі формуються основи як кібербезпеки, так і національної безпеки в цілому. Інформаційними перш за все заходами та засобами здійснюється керівництво з питань реалізації державної політики у цій сфері діяльності.

Важливу роль з питань забезпечення як регіональної, так і власної кібербезпеки має висновок Україною двосторонніх

угод про взаємний захист кібербезпеки, і повинно розглядатися як перспективний напрямок державної зовнішньої політики. Таким чином, головна мета державної політики кібербезпеки повинна полягати в захисті: конституційних прав і свобод людини і громадянина, забезпечення єдності їх прав і обов'язків; духовних, морально-етичні, культурні, історичні, інтелектуальних і матеріальних цінностей суспільства, його інформаційної та природного середовища; конституційного ладу, суверенітету, територіальної цілісності, кібербезпеки у політичній, економічній, соціокультурній, науково-технологічній, оборонної та державної безпеки.

Для забезпечення реалізації Основних засад розвитку інформаційного суспільства в Україні на 2007-2015 роки визначальне значення має політика міжнародної співпраці України та її участь у розвитку глобального інформаційного суспільства. Ця співпраця має здійснюватися з метою узгодження стратегій розвитку інформаційного суспільства, сприяння в реалізації універсального підходу до спільних дій, зменшення цифрової та інформаційної нерівності.

Для вирішення зазначених завдань необхідно:

- розширити співпрацю з провідними міжнародними організаціями з розвитку інформаційного суспільства в рамках міжнародних договорів України щодо науково-технічного співробітництва та міжнародної технічної допомоги;
- забезпечити інтеграцію освіти, науки і культури України в глобальний культурний, освітній, науково-технічний інформаційний простір;
- реалізувати в рамках міжнародних договорів України спільні проекти, які забезпечують інтеграцію України в глобальний інформаційний простір.

Основні засади передбачається реалізувати через такі основні механізми:

- планування соціально-економічного розвитку України з урахуванням потреб розвитку інформаційного суспільства із зазначенням очікуваних результатів такого розвитку; розробка та прийняття відповідних державних програм для ефективного забезпечення завдань розвитку інформаційного суспільства в Україні;
- забезпечення громадської дискусії щодо засад формування інформаційного суспільства в Україні з метою доведення до населення прагнень органів державної влади та органів місцевого самоврядування, приватного сектору економіки, об'єднань громадян щодо розвитку інформаційного суспільства як визначального чинника економічного і суспільного розвитку;
- активна міжнародна співпраця з питань інформаційного суспільства;
- гармонійне поєднання можливостей органів державної влади та органів місцевого самоврядування, приватного сектору економіки;
- фінансування загальнодержавних програм, державних цільових програм з впровадження інформаційно-консультаційних технологій (ІКТ), соціально важливих, таких як забезпечення доступу до ІКТ у сільській місцевості, а також у важкодоступних районах;
- координація розробки та реалізації загальнодержавних програм, державних цільових програм та бізнес-проектів з метою зменшення інвестиційних ризиків, зниження операційних витрат;
- сприяння діяльності спеціалізованих бізнес-інкубаторів, технопарків, технополісів, центрів високих інфор-

маційних технологій та інших інноваційних структур з ІКТ.

Впровадження Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки дасть можливість забезпечити позитивні зміни в життєдіяльності суспільства і людини, а саме: збільшити рівень захисту прав і свобод людини та її добробуту, активізувати участь громадян в управлінні державою, сприяти розвитку демократії; підвищити конкурентоспроможність України, ефективність державного управління, продуктивність праці у всіх сферах економіки, рівень кібербезпеки людини, суспільства, держави, ступінь розвитку інформаційно-телекомунікаційної інфраструктури, зокрема українського сегменту Інтернету; забезпечити перехід економіки до моделі науково-технічного та інноваційного розвитку, збільшити частку наукоємної продукції, сприяти якості та доступності послуг освіти, науки, культури, охорони здоров'я за рахунок впровадження ІКТ; розширити можливості людини отримувати доступ до національних та світових інформаційних електронних ресурсів; створити нові робочі місця, поліпшити умови роботи і життя людини; поглибити запровадження нормативно-правових засад інформаційного суспільства [99, с. 39–41].

4.3. Електронна форма інформаційного капіталу в антикорупційній інфраструктурі

Для ефективного забезпечення кібербезпеки на рівні особи, держави та суспільства кожній країні необхідно розробити ідеологічну основу для цього. Таким чином, формується єдине розуміння організації діяльності суб'єктів забезпечення кібербезпеки, нормативно-правова основа, яка визначає спектр їх прав та обов'язків, а також створює єди-

ну державну політику адміністративно-правового забезпечення кібербезпеки в Україні.

В Україні діє Стратегія національної безпеки України і Воєнна доктрина України, котрі є документами, обов'язковими для виконання, і основою для розробки конкретних програм за складовими державної політики національної безпеки. Стратегія національної безпеки України розрахована на термін до 2020 р. Основними її цілями є:

- мінімізація загроз державному суверенітету та створення умов для відновлення територіальної цілісності України в межах міжнародно-визнаного державного кордону;
- відновлення мирного розвитку Української держави;
- набуття нової якості економічного й гуманітарного розвитку, забезпечення інтеграції України до Євросоюзу та її майбутнього як демократичної, правової, соціальної держави.

Стратегія відносить до основних загроз національній безпеці:

- агресивну політику Росії;
- неефективність системи забезпечення національної безпеки України;
- корупцію та неефективну систему державного управління;
- економічну кризу, виснаження фінансових ресурсів держави, зниження рівня життя населення;
- загрози енергетичній, інформаційній, екологічній і техногенній безпеці.

До недавнього часу в Україні діяла Доктрина кібербезпеки України, яка була основою для формування державної політики у сфері кібербезпеки України; розроблення про-

ектів концепцій, стратегій, цільових програм і планів дій із забезпечення кібербезпеки України; підготовки пропозицій щодо дальшого системного вдосконалення правового, методичного, науково-технічного і організаційного забезпечення кібербезпеки України. Зміст Доктрини кібербезпеки України 2009 року не дає повного уявлення про сукупність офіційних поглядів, цільових настанов, керівних принципів, напрямів діяльності, спрямованих на реалізацію державної політики кібербезпеки з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз. Доктрина не визначає важливі аспекти забезпечення кібербезпеки України.

Єдиним нормативно-правовим актом, який би визначив та закріпив систему цих поглядів, став Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007р. Проте, названий Закон не передбачає розгляду різновидів кібербезпеки. До того ж у цьому законі достатньо повно виписані технічні аспекти кібербезпеки, але майже не приділено уваги інформаційно-психологічним аспектам.

Вагомим стало прийняття законів України: «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Національну програму інформатизації», «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про телекомунікації». На основі зазначений нормативно-правових актів було прийнято Розпорядження КМУ «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» від 15 травня 2013 р.

З урахуванням змін обстановки, характеру і змісту загроз національній безпеці України в електронній сфері, зі змінами інформаційного законодавства в Україні, основні

шляхи і напрями реалізації концептуальних положень кібербезпеки держави мають бути зазначені в науково обґрунтованій концепції превентивних заходів в системі кібербезпеки, якої на сьогодні в Україні немає.

Система забезпечення кібербезпеки має включати комплекс превентивних заходів із надання гарантій захисту життєво важливих інтересів особи, держави, суспільства, своєчасного і адекватного реагування на увесь спектр інформаційних безпекогенних чинників з метою захисту національних інтересів та національної безпеки.

Питання кібербезпеки стало предметом наукових дискусій у рамках робіт таких вчених, як І. Арістова, І. Березовська, В. Голубєв, В. Гурковський, О. Дзьобань, Р. Калюжний, В. Конах, Б. Кормич, В. Ліпкан, Ю. Максименко, А. Марущак, В. Цимбалюк, О. Юдін, Р. Юсупов та ін. Однак вивченню сьогоденної концепції кібербезпеки України не приділялося уваги вітчизняними дослідниками.

В Україні за останні два роки відбулися суттєві зміни у нормативно-правовій базі, що стосується адміністративно-правового забезпечення кібербезпеки. Тому вивчення цього питання, а також визначення шляхів удосконалення, вбачаємо за доцільне проаналізувати, які зміни можна внести до нього. Функції щодо реалізації державної політики у цій важливій складовій забезпечення національної безпеки; організаційну структуру державних органів, інших суб'єктів та їх повноваження щодо реалізації державної політики у цій сфері; порядок координації діяльності суб'єктів з питань забезпечення кібербезпеки особи, держави і суспільства; сили і засоби для активних дій в процесі можливих інформаційних протистоянь із супротивниками і конкурентами, попередження інформаційної агресії та застосування проти

України інформаційної зброї та інших негативних інформаційних впливів, можуть слугувати основою для дії концепції та проблеми її функціонування в державі.

Таким чином, на нашу думку, можна виокремити такі ключові напрями концепції превентивних заходів в системі кібербезпеки України:

1) формування державної політики кібербезпеки з відповідними органами;

2) удосконалення адміністративно-деліктного законодавства в сфері кібербезпеки України:

3) створити спеціалізовану службу, основним завданням якої б стало забезпечення координації дій всіх державних та недержавних інституцій у сфері забезпечення кібербезпеки України.

4) реформування законодавства, що стосується кібербезпеки;

5) забезпечення програм відкритого доступу до публічної інформації та створення ефективних умов щодо її отримання;

6) реформування наявної системи електронного урядування;

7) розробка цілісної теорії загроз.

Першим напрямом концепції превентивних заходів в системі кібербезпеки має стати формування державної політики кібербезпеки з відповідними органами. При цьому має відбуватися урахування усіх рекомендацій міжнародних інституцій та створення належної нормативно-правової бази. Наразі до такої системи належать:

- Конституція України;
- Закони України: «Про основи національної безпеки України», «Про інформацію», «Про Основні засади роз-

витку інформаційного суспільства в Україні на 2007–2015 роки», «Про Концепцію Національної програми інформатизації», «Про Національну програму інформатизації», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про внесення змін до Закону України «Про ратифікацію Конвенції про кіберзлочинність», «Про доступ до публічної інформації», «Про Раду національної безпеки і оборони», «Про боротьбу з тероризмом», Цивільний кодекс, Кримінальний кодекс, Кодекс України про адміністративні правопорушення;

- Укази Президента України: «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері кібербезпеки України», «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення кібербезпеки України», «Про заходи щодо захисту інформаційних ресурсів держави», «Про Міжвідомчу комісію з питань інформаційної політики та кібербезпеки при Раді національної безпеки і оборони України»;
- Постанови Кабінету Міністрів України: «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах», «Питання Адміністрації Державної служби спеціального зв'язку та захисту інформації»;
- Розпорядження Кабінету Міністрів України: «Про схвалення Концепції розвитку електронного урядування в Україні», «Питання впровадження системи впровадження системи електронної взаємодії органів виконавчої влади».

Національна безпека України забезпечується шляхом проведення виваженої державної політики відповідно до

прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах.

Вибір конкретних засобів і шляхів забезпечення національної безпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам.

Другим напрямом концепції превентивних заходів в системі кібербезпеки України є удосконалення адміністративно-делікатного законодавства в сфері кібербезпеки України:

- виокремлення в межах КУпАП окремого розділу, об'єктом адміністративних правопорушень яких є кібербезпека людини (особи, громадянина), держави та суспільства. Під час розгляду складу кожного з правопорушень у сфері кібербезпеки, що передбачені КУпАП, виникають певні труднощі, тому що чинний КУпАП не має окремої глави, присвяченій саме правопорушенням в електронній сфері, а правопорушення, які можна віднести до кібербезпеки, розташовані у різних главах Особливої частини КУпАП;
- аналіз відповідних статей чинного КУпАП дозволяє дійти висновку, що суб'єктом адміністративного правопорушення визнається лише фізична особа. Але останнім часом у законодавстві з'являються норми, які передбачають накладення стягнень на юридичних осіб, зокрема, за правопорушення у сфері кібербезпеки. Так, наприклад, згідно частини 7 статті 20 Закону України «Про державну таємницю» дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасо-

ваний або його дія може бути зупинена Службою безпеки України на підставі акту проведеної нею перевірки, висновки якого містять дані про недодержання державним органом, органом місцевого самоврядування, підприємством, установою, організацією умов, передбачених статтею 20 Закону України «Про державну таємницю». За вчинення адміністративного порушення у сфері кібербезпеки на фізичних осіб найчастіше накладається штраф. На нашу думку, до цього виду адміністративної відповідальності також варто притягати і юридичних осіб — порушників законодавства. Враховуючи вищевикладене, необхідно передбачити у чинному КУпАП розділ, який би містив перелік проступків в електронній сфері, а також закріпити у чинному КУпАП норми, які б передбачали адміністративну відповідальність юридичних осіб.

- посилення адміністративної відповідальності за правопорушення інформаційного характеру, оскільки на сьогодні, здебільшого, передбачені такі види адміністративних стягнень як штраф від п'яти до п'ятисот неоподаткованих мінімумів доходів громадян та конфіскація засобів вчинення правопорушення чи продукції отриманої внаслідок порушення вітчизняних норм права, а також у поодиноких випадках виправні роботи, попередження та відшкодування збитків;
- доповнення КУпАП статею, що передбачає відповідальність за курси нейролінгвістичного програмування (НЛП), що завдають шкоду психіці людини (громадянина), а також нормою, що закріплює відповідальність за порушення правил збирання, розголошення та використання комерційної таємниці;

– доповнити Кодекс України про адміністративні правопорушення окремою статтею 188–43, що передбачатиме **відповідальність за невиконання законних вимог посадових осіб Служби безпеки України;**
– в Закон України «**Про основи національної безпеки України» внести** зміни до визначення терміну **«національна безпека»** як захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються, зокрема, кібербезпека, у тому числі кібербезпека та захист інформації;
– статтю 7 Закону України «**Про основи національної безпеки України» доповнити переліком обставин, що можуть вважатися загрозою національній безпеці.** Так, **в електронній сфері** — використання засобів масової інформації для поширення порнографії, пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками; розголошення інформації, яка становить державну або іншу передбачену законом таємницю, а також службової і конфіденційної інформації, спрямованої на забезпечення потреб та національних інтересів суспільства і держави; неналежний рівень надійності і захищеності національної інформаційної інфраструктури в умовах надзвичайного та воєнного стану; несанкціоновані дії, спрямовані на порушення цілісності та доступності державних інформаційних ресурсів;
– статтю 8 Закону України «**Про основи національної безпеки України»** доповнити основними напрямами державної політики з питань національної безпеки в електронній сфері, додаючи такі:
– удосконалення законодавства з питань кібербезпеки, у тому числі кібербезпеки;

- запобігання проявам комп'ютерної злочинності та комп'ютерного тероризму;
- удосконалення засобів захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;
- удосконалення форм і способів протидії інформаційним заходам, які спрямовані на послаблення обороноздатності держави;
- забезпечення повноправної участі України в міжнародному співробітництві у сфері боротьби з комп'ютерною злочинністю та комп'ютерним тероризмом.

Третім напрямом концепції превентивних заходів в системі кібербезпеки, на нашу думку, є створення спеціалізованої служби, основним завданням якої б стало забезпечення координації дій всіх державних та недержавних інституцій у сфері забезпечення кібербезпеки України. Такою службою може бути Державна служба з питань кібербезпеки, яка повинна: приймати перспективні управлінські, технічні, адміністративні і фізичні заходи, які сприяють підвищенню кібербезпеки; видавати рекомендації і доводити їх до відома всіх зацікавлених відомств. Основна функція Служби має полягати в координації усіх республіканських програм в сфері кібербезпеки незалежно від їхньої відомчої приналежності.

Доречно зауважити, що при Міністерстві інформаційної політики України створено Експертну раду згідно з Положенням «Про Експертну раду при Міністерстві інформаційної політики України як дорадчий орган, що має своєю метою забезпечення взаємодії з науково-дослідними установами, неурядовими аналітичними центрами, інститутами громадянського суспільства, іншими вітчизняними та

зарубіжними організаціями [131]. Актуальним залишається питання створення єдиного в своєму роді органу, який би був незалежним від усіх гілок влади та консолідував зусилля зазначених вище суб'єктів.

Крім того, потребує уточнення не тільки коло суб'єктів, що забезпечують кібербезпеку України, але й їх завдання, функції, повноваження в цій сфері.

Необхідно відмітити, що навіть стислий аналіз вітчизняних та зарубіжних нормативно-правових актів дозволяє зробити висновок про актуалізацію шляхів удосконалення кібербезпеки та впорядкування інформаційних відносин в усіх сферах життєдіяльності суспільства та функціонування державних і недержавних інституцій. Хоча державне та міжнародне регулювання процесу інформатизації не завжди відповідає динамічності розвитку інформаційної сфери. На це є як об'єктивні причини, так і проблеми конкретної країни. Так, нестабільна політична ситуація в Україні та загалом перехідний період становлення нашої держави як незалежної, не дозволяють в передбачені строки реалізувати заплановані заходи, що направлені на забезпечення кібербезпеки.

Саме тому, одним із шляхів підвищення ефективності кібербезпеки України, на нашу думку, є більш жорсткий контроль посадових осіб, які відповідальні за виконання доручених їм завдань.

Лише системне, комплексне та цілеспрямоване виконання покладених заходів усіма суб'єктами, сприятиме підвищенню ефективності реалізації державної політики в сфері кібербезпеки України.

Четвертий напрям концепції превентивних заходів в системі кібербезпеки полягає в ефективному, якісному

реформуванні законодавства, що стосується кібербезпеки. Водночас, розглядаючи адміністративно-правове регулювання інформаційної сфери як основу забезпечення кібербезпеки держави слід зазначити, що упродовж останніх років законодавча база України в електронній сфері поповнилася низкою Законів, з-поміж яких надзвичайно важливими є Закони: «Про інформацію», «Про державну таємницю», «Про захист інформації в автоматизованих системах», «Про науково-технічну інформацію», Закон «Про систему іномовлення України», який Верховна Рада ухвалила 8 грудня 2015 року тощо.

Україна у червні 2014 року Україна підписала Угоду про Асоціацію з ЄС, і протягом двох років має привести своє законодавство до європейських стандартів, тобто до червня 2016 року.

Члени робочої групи при парламентському Комітеті з питань свободи слова та інформаційної політики, до якої входять народні депутати, представники громадських організацій та медіаіндустрії, обговорили проект Стратегії розвитку законодавства України з питань свободи слова та діяльності ЗМІ відповідно до європейських стандартів, який розроблено за підтримки спільної програми ЄС та РЄ «Зміцнення інформаційного суспільства в Україні». Стратегія зокрема передбачає зміни до Конституції України, ухвалення законів про аудіовізуальні послуги; про саморегулювання або співрегулювання; про запобігання монополізації та контроль за концентрацією на ринках медіапослуг, про загальнодержавну цільову програму розвитку медіаграмотності в Україні; внесення змін до низки діючих законів тощо.

Нова редакція Закону «Про суспільне телебачення і радіомовлення України» дала можливість запустити одну з

найважливіших медіареформ: перетворення державного мовлення на суспільне.

Закон «Про реформування державних і комунальних друкованих засобів масової інформації». Ця реформа, до якої країна йшла багато років, передбачає приватизацію державних і комунальних друкованих видань у два етапи: спершу один рік — добровільно для охочих редакцій, наступні два роки — роздержавлення решти видань.

Закон «Про внесення змін до деяких законодавчих актів України (щодо особливостей трансляції (ретрансляції) реклами, яка міститься у програмах та передачах іноземних телерадіоорганізацій)», яким Верховна Рада заборонила транслювати рекламу на російських каналах в Україні та узаконила так званий список адаптованих каналів, що складає Національна рада з питань телебачення і радіомовлення; Постанова «Про тимчасове призупинення акредитації журналістів та технічних працівників деяких засобів масової інформації Російської Федерації при органах державної влади України».

Закон України «Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації та реалізації принципів державної політики у сфері телебачення і радіомовлення». Цей закон набув чинності 1 жовтня 2015 року, його основною метою є відкриття даних про кінцевих власників та структуру власності телерадіоорганізацій і провайдерів програмної послуги.

Розроблення національної правової бази, її гармонізація з міжнародними інституціями, тобто приведення відносин у сфері інформації у відповідність до міжнародних стандартів сприятиме зміцненню кібербезпеки України та підвищенню її міжнародного авторитету як демократичної і

правової держави. Вирішивши проблему неефективного законодавства, передбачивши механізми його реалізації, можна буде забезпечити реальне здійснення передбаченого Конституцією України права людини на свободу інформації, оскільки для України настав час, коли цим питанням буде надано комплексного та дієвого характеру.

В зв'язку з цим, доцільним є реалізація таких завдань:

1) прийняти Концепцію національної інформаційної політики України та спрямований на реалізацію її положень Інформаційний кодекс України, який виступить базовим нормативним актом, що регулюватиме діяльність в електронній сфері України; включення до Стратегії національної безпеки України спеціального розділу «Стан кібербезпеки України», в якому слід чітко визначити актуальні проблеми державної політики забезпечення кібербезпеки та зосередити увагу на необхідності їх вирішення;

2) створити єдиний державний реєстр власників ЗМІ;

3) постійно удосконалювати індустрію інформаційних послуг та інфраструктуру єдиного інформаційного простору України.

П'ятим напрямом концепції превентивних заходів в системі кібербезпеки є забезпечення програм відкритого доступу до публічної інформації створення ефективних умов щодо її отримання.

За роки членства України в Раді Європи почали створюватися і поступово впроваджуватися в життя механізми залучення громадськості до вироблення та реалізації відкритої та прозорої державної політики. Відчувається нагальна потреба наукового дослідження таких механізмів, однак в науковій літературі не спостерігається інтересу до цієї проблеми. Отже, існує необхідність прийняття законодавчих

норм, які забезпечували б процедури взаємозв'язку органів державного управління та громадян України у сфері вироблення нової суспільної політики, яка містить дієві механізми стримувань і противаг, а також забезпечує основне право громадянина на інформацію про діяльність владних структур. Вироблення таких норм може бути вагомим кроком на шляху лібералізації та демократизації національного законодавства.

Система зв'язків з громадськістю, що є невід'ємною складовою діяльності органів державного управління у демократичних країнах, насамперед, у країнах — членах Ради Європи, забезпечує дієву взаємодію рівноправних і взаємозалежних суб'єктів суспільного життя. Така система фінансується з державних бюджетів, але жодного року за досліджуваний період у проектах Державного бюджету України не передбачалося коштів на фінансування зв'язків з громадськістю, які сприяли би аналізу й оцінюванню, насамперед, правозахисної діяльності влади, чи врахування пропозицій громадян у цій сфері [40, с. 40].

Англійське Public Relations (PR) переводиться як «взаємини із громадськістю». Це словосполучення було вперше використане в 1807 році третім президентом США Т. Джефферсоном, котрий вважав, що без цілеспрямованого конструювання відносин із громадськістю демократія неможлива.

Існує близько 500 визначень піару, найбільш вдале визначення запропоноване в 1999 році Європейською піар-конференцією (CEPR). Піар — це свідома організація комунікації. Ціль піару — досягти взаєморозуміння й встановити плідні стосунки між організацією і її аудиторіями шляхом двосторонньої комунікації. Саме структури і підрозділи зв'язків з громадськістю, що функціонують як на загаль-

нодержавному рівні, так і в сфері сектору безпеки, змогли б забезпечити взаємодію між державою, силами безпеки й громадянським суспільством.

Ставши частиною Ініціативи «Партнерство «Відкритий Уряд» (ПВУ) ще в 2011 р., Україна почала роботу з приєднання до Декларації Відкритого Уряду, що передбачало збільшення відкритості інформації і даних для включення громадян у процеси прийняття рішень, запровадження найвищих стандартів професійної і доброчесної поведінки державних службовців [81].

Забезпечення реалізації Ініціативи «ПВУ» у 2014–2015 рр. покладено на Кабінет Міністрів України, одним із напрямів якої є забезпечення доступу до публічної інформації. З 6-ти взятих зобов'язань за 2 роки було виконано лише 3 пункти [81].

Очікується, що прийнята у 2015 р. Національна стратегія у сфері прав людини вирішить частину проблем, забезпечивши запровадження ефективного позасудового механізму реалізації права на доступ до публічної інформації та забезпечивши систему гарантій доступу населення до Інтернету [148]. Натомість інший документ, переданий у 2015 р. на розгляд Кабміну — проект концепції кібербезпеки України [25] — став об'єктом критики громадськості через незрозумілість місії документу, наявність методологічної помилки (не прописані інтереси), змішаність принципів та завдань державної політики тощо [186].

Закон України «Про внесення змін до статті 28 Бюджетного кодексу України щодо доступу до інформації про бюджетні показники у формі відкритих даних» передбачає оприлюднення бюджетних запитів, квартальної та річної звітності про виконання Державного бюджету України, паспортів бюджетних програм та звітів про виконання паспор-

тів бюджетних програм, рішень про місцеві бюджети, інформації про виконання Державного бюджету України та місцевих бюджетів (крім бюджетів сіл і селищ) [125].

Прийнятий Закон України «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917–1991 років» має за мету врегулювання основних засад, принципів, гарантій, шляхів реалізації державної політики щодо забезпечення доступу до архівної інформації репресивних органів [28].

Закон України «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції» пропонує впровадити механізм подання індивідуальних та колективних звернень в електронній формі [50].

Беручи до уваги проблеми, що виникають у процесі реалізації права на доступ до публічної інформації в Україні, вважаємо за доцільне вжити наступних заходів:

- розширити коло установ та організацій, для яких проводяться інформаційні кампанії;
- відслідковувати та поширювати інформацію про випадки, коли відстоювання права на доступ до інформації змінило ситуацію громадянина на краще (т. зв. «success stories»);
- проводити більше освітніх заходів для представників правової сфери щодо застосування норм законодавства у сфері інформації;
- заохочувати розробку та застосування ІТ-технологій для покращення роботи посадових осіб та спрощення їх звітності;
- прискорити впровадження електронного урядування;
- розпочати впровадження якісного підходу до прийняття рішень, оскільки існуюча система часто призводить

до невиконання норм закону про доступ до публічної інформації;

- сприяти зміцненню довіри між органами влади та громадськими організаціями.

Шостим напрямом концепції превентивних заходів в системі кібербезпеки вбачається реформування наявної системи електронного урядування.

Сьогодні проявом оптимізації взаємодії індивідів та держави на новому рівні є спроба впровадження програм електронного уряду, покликаних сприяти зменшенню бюрократичності, збільшенню відкритості і прозорості діяльності органів управління та поступовому відходу від тотального використання паперової технології. У вітчизняній науковій літературі дослідженню проблематики електронного урядування, його характеристик та стану впровадження в практичну діяльність органів влади присвячено роботи таких провідних науковців, як Д. Дубов, С. Дубова, І. Клименко, С. Кузнєцова, К. Линьова, О. Мітченко, З. Пісковець, О. Рискова, В. Шеверда, О. Юлдашев та ін. З огляду на це, особливої уваги потребує така форма організації державного управління, як електронне урядування, впровадження якої було розпочато кілька років тому і яке наразі набуває все більшої підтримки суспільства.

В Україні діє Концепція розвитку електронного урядування, затверджена Розпорядженням КМУ від 13 грудня 2010 р., в якій сформовані основні принципи та прогнози щодо запровадження електронного урядування в державних органах влади та органах місцевого самоврядування.

До основних завдань електронного уряду відносяться: організація державного управління на основі електронних засобів обробки, передачі та розповсюдження інформації;

надання послуг державних органів всіх гілок влади всім категоріям громадян (пенсіонерам, робітникам, бізнесменам, державним службовцям тощо) електронними засобами; інформування тими ж засобами громадян про роботу державних органів [31].

На сьогодні вперше розвиток е-урядування визначено одним з головних пріоритетів на національному рівні. Наразі, в Україні працює вже понад 20 важливих для громадян та бізнесу е-послуг у земельній, будівельній, екологічній та соціальних сферах. У 2015 році громадяни України отримали можливість використовувати електронні петиції — новий інструмент е-демократії, щоб ефективніше взаємодіяти з владою і привертати увагу до вирішення важливих для громади проблем.

Громадяни України дедалі активніше освоюють сучасні інформаційно-комунікативні технології, використовують їх в особистому, громадському та професійному житті, впроваджують у бізнес-процеси, що дозволяє оптимізувати часові та матеріальні витрати, а отже, збільшити їх ефективність. Держархбудінспекція видала першу електронну ліцензію на будівництво в Україні 26 липня 2016 р. Електронна система дозволяє подати документи у будь-який зручний час 24 години 7 днів на тиждень через мережу Інтернет, витративши на це не більше декількох хвилин. Поступово, але неухильно відбувається знайомство громадян із механізмами та інструментами електронного урядування на теренах України, що разом із вивченням закордонного досвіду в цій сфері підвищує бажання повноцінного впровадження та реалізації концепції електронного урядування в нашій державі.

Сьомим напрямом концепції превентивних заходів в системі кібербезпеки має стати системно-аналітична роз-

робка цілісної теорії загроз. Розглядаючи поняття «кібербезпека» через захищеність від небезпек та загроз, виникає проблема розробки цілісної теорії загроз, оскільки немає єдиної методології в визначенні загроз, в їх співвідношенні між собою. Раніше загрози мали зовнішній та воєнний характер, коли невоєнні та воєнні засоби практично неможливо було використовувати комплексно, але зараз в умовах взаємозалежності світу та нових технологій загрози носять, як правило, комплексний характер [90, с. 39].

Руйнування творчого інтелектуального потенціалу, неготовність системи освіти до підтримання процесів випереджувального розвитку країни призводить до того, що з огляду на рівень розвитку цієї галузі за кордоном і той факт, що багато держав світу приділяють значну увагу інформаційній безпеці, Україна й досі не має достатньої кількості кваліфікованих фахівців, які б змогли на належному рівні ефективно протидіяти інформаційній агресії.

Низький загальний рівень інформаційної інфраструктури сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, котрі пропагують власний спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство й державу, руйнуючи морально-етичні основи генофонду української нації [60, с. 17].

Авторське бачення «загроз» в інформаційній безпеці пропонується як сукупність умов та факторів, які становлять небезпеку життєво важливим інтересам особи, держави та суспільства у зв'язку з можливістю негативно впливати на свідомість і поведінку громадян, а також на інформаційно-комунікаційну інфраструктуру.

Унікальною особливістю інформаційної загрози є те, що вона виступає як самостійна загроза і водночас є основою для інших видів загроз на інформаційному рівні, в тому числі і їх першопричиною.

Таким чином, джерелами загроз інформаційного простору є суперечності певних інтересів, систем цінностей, цілей між особистістю та суспільством, державою або наявністю в однієї зі сторін стосовно іншої домагань, претензій або інших спонукань до конфлікту.

Основними реальними та потенційними загрозами інформаційній безпеці України є:

1) у зовнішньополітичній сфері:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;
- прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують стабільному та безпечному функціонуванню національних інформаційно-телекомунікаційних систем;
- зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також інтернет;

2) у сфері державної безпеки:

- негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканності кордонів України;
- використання засобів масової інформації, інтернету для пропаганди сепаратизму за етнічною, мовною, релігійною й іншими ознаками;
- несанкціонований доступ до інформаційних ресурсів органів державної влади;

- розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

3) у воєнній сфері:

- порушення встановленого регламенту збирання, оброблення, зберігання й передання інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;
- несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;
- реалізація програмно-математичних заходів із метою порушення функціонування інформаційних систем у сфері оборони України;
- перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління;
- інформаційно-психологічний вплив
- на населення України, у тому числі особовий склад військових формувань, із метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

4) у внутрішньополітичній сфері:

- недостатня розвиненість інститутів громадянського суспільства, недосконалість партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;
- негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;
- поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;

5) в економічній сфері:

- відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій;
- недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель;
- несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах;
- використання неліцензованого й несертифікованого програмного забезпечення, засобів і комплексів оброблення інформації;
- недостатній рівень розвитку національної інформаційної інфраструктури;

6) у соціальній та гуманітарній сферах:

- відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури;
- недодержання прав людини і громадянина на отримання інформації, необхідної для захисту їх соціально-економічних прав;
- поширення в ЗМІ не властивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської й національної гідності;
- тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля;

- послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;
- відставання розвитку українського кінематографу, книговидання, книгорозповсюдження й бібліотечної справи від рівня розвинутих держав;

7) у науково-технологічній сфері:

- зниження наукового потенціалу в галузі інформатизації та зв'язку;
- низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку;
- відтік за кордон наукових кадрів та суб'єктів права інтелектуальної власності;
- недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій і техніки;
- неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;

8) в екологічній сфері:

- приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру;
- недостатня надійність інформаційно-телекомунікаційних систем збору, обробки й передачі інформації в умовах надзвичайних ситуацій;
- низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування й реагування на надзвичайні ситуації.

Однією з характерних тенденцій, яка склалася в сучасних умовах, є випереджальний розвиток форм, способів, технологій і методик впливу на свідомість (підсвідомість), і психічний стан людини порівняно з організацією протидії негативним, деструктивним психологічним впливам, інформаційно-психологічним захистом особистості й суспільства загалом.

При цьому, акцентується увага про можливі деформації у системі масового інформування й поширення дезінформації, які ведуть до потенційних порушень суспільної стабільності. Ці впливи можуть призводити до порушень психічного й фізичного здоров'я, відхилення від норм поведінки, до зростання ризикованих соціальних й особистісних ситуацій.

Сьогодні не існує достатніх гарантій захисту особи від загроз, пов'язаних з порушенням кібербезпеки особи. Тому виникла значною мірою соціальна небезпека безконтрольного застосування технологій, засобів і методів психофізичного впливу на певні соціальні групи людей через свідомість і підсвідомість людини з метою формування необхідних подій та маніпулювання громадською думкою. Кібербезпека особи й суспільства є складовою кібербезпеки держави: її забезпечення займає особливе місце в державній політиці. Ця особливість визначається специфікою загроз та їх джерел. Найбільш важливими об'єктами захисту у сучасних умовах є індивідуальна та масова свідомість. Руйнація свідомості небезпечніше руйнації в економіці, тому що втрата національних, духовних цінностей веде до виродження народу і краху суспільства.

Діяльність органів виконавчої влади у сфері забезпечення кібербезпеки в Україні має бути зосереджена на конс-

труктивному поєднанні діяльності держави, громадянського суспільства та людини за трьома головними напрямами:

- інформаційно-психологічному, зокрема щодо забезпечення прав і свобод людини й громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі;
- технологічного розвитку зокрема стосовно розбудови та інноваційного оновлення національних інформаційних ресурсів, упровадження новітніх технологій створення, оброблення та поширення інформації;
- захисту інформації, зокрема щодо забезпечення конфіденційності, цілісності й доступності інформації, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

Контрольні запитання

1. Особливості глобалізації світового суспільства як механізму глобального планування та довгострокового перерозподілу ресурсів.

2. На чому базується вітчизняний досвід використання інформаційно-психологічного протиборства в XIX столітті?

3. Які заходи вживав уряд напередодні Другої світової війни для зміцнення апарату спецпропаганди?

Теми рефератів

1. Оцінки вітчизняних та закордонних експертів перемоги США над СРСР у «холодній війні».

2. Наслідки вчинення кіберзлочинів.

3. Умови, які сприяють вчиненню кіберзлочинів.

РОЗДІЛ 5. КРИТИЧНА ІНФРАСТРУКТУРА КІБЕРБЕЗПЕКИ УКРАЇНИ ТА СВІТОВОГО ПРОЦЕСУ

5.1. Юридична логіка публічного адміністрування в антикорупційному забезпеченні кібербезпеки України

За умов сучасного розвитку кіберкапіталу як системного електронного контролю, моніторингу та представництва за діяльністю всіх сфер суспільного життя актуальним постає питання юридичної логіки публічного адміністрування. Адже сьогодні значна кількість українських громадян потерпає від соціально-економічної кризи, до якої додається військово-політичний конфлікт. При цьому, одним із чинників цих негативних суспільних явищ виступає корупція, що вже набула системного характеру. Така корупція вважається реальною загрозою національній та світовій безпеці, оскільки перешкоджає проведенню ефективної діяльності, визначальних у цьому напрямі, військових та правоохоронних структур вітчизняного та міжнародного процесу.

Дослідженням щодо протидії корупційним проявам у системі публічного адміністрування України здійснюються у працях таких вітчизняних науковців як: М.Я. Азаров, В.Т. Білоус, О.В. Бандурко, В.О. Глушков, Ю.В. Грошовий, В.Т. Зеленецький, М.Н. Курко, А.Ю. Ковальчук, П.М. Лісовський, М.І. Мельник, А.М. Подоляка тощо. Проте, у теоретичних представленнях і підходах різних авторів щодо юридичної логіки публічного адміністрування в антикорупційному забезпеченні кіберкапіталу України спостерігаються фрагментарність та відсутність всебічної концептуальної

моделі. Цей факт свідчить про відсутність теоретично обґрунтованого понятійно-категоріального апарату як системно-аналітичного дослідження, що до цього дня залишається надзвичайно актуальною.

Оптимальною юридичною формою такого публічного адміністрування в антикорупційному забезпеченні кіберкапіталу України представляється побудова його у вигляді взаємодоповнюючої єдності системної процедури дослідження. Саме така системна процедура механізму реалізації на кожному з її етапів повинна задавати концептуальний напрям дослідження, адекватний природі публічного адміністрування і ефективному взаємозв'язку основних важливих параметрів щодо антикорупційного забезпечення кіберкапіталу України.

Після здійснення Революції гідності Україна все ж залишається найбільш корумпованою країною Європи. Так, за даними досліджень Індексу Transparency International, Україна здобула 30 балів зі 100 можливих. За даними досліджень за 2017 рік Україна посіла 130 місце зі 180 країн світу. Це на один бал більше та на одну позицію вище. Ніж у минулому році (29 балів, 131 місце зі 176 країн). Для порівняння, ще в 2007 році Україна займала 118-те місце зі 179 країн, що досліджувалися протягом того року [80, с. 68].

У цьому сенсі повільний ріст індексу України, належний показник сприйняття корупції громадянами, падіння динаміки зростання вдвічі порівняно з 2016 роком пояснюється відсутністю дієвих форм у сфері протидії корупції та неефективною діяльністю органів правопорядку щодо виявлення корупційних правопорушень та притягнення винуватців до відповідальності, недостатністю політичної волі керівництва країни до рішучої боротьби з корупцією та

зазначити ефективно діючі законодавчі ініціативи парламенту, які загрожують новоствореній антикорупційній кіберінфраструктурі.

Як результат, корупція залишається для бізнесу та звичайних громадян однією з важливих проблем, які можуть виникнути в діяльності представників публічної влади та в процесі адміністрування. Зазначається, що публічне адміністрування — це керування діяльністю апарату управління підприємством, установою чи організацією неприватної форми власності, у тому числі органу державної влади, органу місцевого самоврядування, суб'єкту громадянського суспільства. Кожен суб'єкт публічної адміністрації наділений відповідною компетенцією, яка, як правило, дає йому можливість вибирати у конкретних ситуаціях той чи інший варіант поведінки, варіант конкретних дій, тобто відобразити зміст своєї регулятивної, сервісної або управлінської діяльності в тій формі, яка відповідає публічним інтересам. При цьому, конкретними прикладами дій публічної адміністрації, в яких виражається зміст її діяльності, можуть бути: видання акту публічного управління, надання адміністративної послуги, прийняття рішення у скарзі, її розгляд, проведення наради, призначення ревізій, перевірок, здійснення контрольно-наглядової діяльності тощо.

Контрольно-наглядова діяльність публічного адміністрування

Під «контрольно-наглядовою діяльністю держави» варто вбачати такі втручальні провадження, які здійснюються за ініціативою адміністративного органу як результат щодо юридичного оформлення прав, свобод і законних інтересів особи (наприклад, видача дозволів, ліцензій, сертифікатів, посвідчень, проведення реєстрації тощо). Це, у свою чергу,

полягає у встановленні (перевірці) відповідності певної діяльності (поведінки) приватної особи вимогам закону, а у випадку виявлення порушень — у застосуванні адміністративних стягнень. В чинному законодавстві та вітчизняній юридичній науці ця діяльність йменується як «державний контроль (нагляд)» та/або «адміністративний контроль (нагляд)». Основним змістом цих втручальних проваджень є: документальні перевірки; фактичні перевірки діяльності; періодичне отримання інформації, звітів, і здійснюються у формі перевірок, ревізій, інспектування.

В площині контрольно-наглядової діяльності корупція може мати місце як наслідок відмови провести перевірку, неналежного проведення перевірок і приховування фактів вчинених порушень, проведення перевірок виключно з метою отримання незаконної вигоди [13].

Корупційні ризики в системі публічної адміністрації України

У цьому змісті необхідно визначити зміст поняття «корупційні ризики». Це сукупна матриця правових, організаційних та інших чинників, що породжують, мотивують осіб до скоєння корупційних правопорушень під час виконання ними функцій держави або місцевого самоврядування. Специфіка публічного адміністрування створює кіберпотенційні (електронні, інформаційні, віртуальні) можливості для існування суперечливих потреб та інтересів — суб'єкта, соціальних груп, суспільства та самої держави, зіткнення яких в управлінському процесі уможливлює виникнення різноманітних конфліктних ситуацій, а іноді призводить і до скоєння корупційних правопорушень. На практиці зіткнення таких інтересів, а отже, і наявність корупційних ризиків значною мірою зустріча-

ється у таких сферах державного управління, як надання адміністративних послуг та здійснення контрольно-наглядової функції держави.

Отже, основними корупційними ризиками в системі публічної адміністрації України є:

– поєднання в одному органі виконавчої влади функцій з вироблення політики та нормотворчості з функціями поточного адміністрування (у т. ч. надання адміністративних послуг та контрольно-наглядової діяльності). Така практика породжує проблеми підзаконної нормотворчості, зокрема. Коли органи виконавчої влади, які мають застосовувати законодавство, самостійно розробляють таке законодавство, керуючись, насамперед відомчими (корпоративними) інтересами. Наприклад, нормативні акти, які застосовують податкові органи, розробляються не Міністерством фінансів, а Державною податковою адміністрацією. Таким чином, повноваження органів публічної адміністрації мають відповідати вимогам Конституції України та законів України, не можуть визначатися у підзаконних нормативно-правових актах, оприлюднено тлумачитися у актах виконавчої влади; поєднання в одній інституції функцій з надання адміністративних послуг і контрольно-наглядових (інспекційних) функцій, що породжує корупційні ризики, пов'язані з «розмиванням місії» відповідного органу, зменшенням об'єктивності розгляду та перегляду адміністративних справ. Крім того, обслуговуючий тип діяльності та інспекційний тип діяльності потребують різних методів та форм. Також очевидно, що у випадку порушення правил видачі певного дозволу (ліцензії), орган, що інспектуватиме діяльність приватної особи, з одного боку, не буде зацікавлений у виявленні та

фіксації помилки з боку свого ж «відомства», а з іншого боку, фактично опиняється в полі корупційних діянь.

Безперечно, послабленню корупційного ризику сприятиме інституційне (організаційне) розмежування функцій з надання адміністративних послуг та контрольно-наглядових функцій, що сприяє зростанню об'єктивному розгляду адміністративних справ державними органами управління, а також виявленню випадків незаконних дій інших адміністративних органів. Це надає можливість розробки дієвих механізмів протиборства з корупційними маніпуляціями у системі державного управління та публічного адміністрування, що може стати ухвалення проекту Концепції реформи публічної адміністрації в Україні. У разі схвалення Урядом даного проекту та його послідовного впровадження може бути зняти значну кількість інституційних та функціональних конфліктів у публічній адміністрації та породжуваних ними корупційних ризиків.

Протиборство корупційним проявам у системі державної служби України

Необхідно озвучити, що в юридичній логіці протидія корупційним маніпуляціям у системі державної служби України розглядається як складна соціальна система, що містить певну кількість ефективно діючих раціональних складових (кореляційно-апроксимаційних, фізично-ентропійних тощо). Так, М.Я. Азаров у своїх працях вважає, що система характеризується тенденціями до збереження, саморегуляції та саморозвитку. Характерною ознакою для протидії корупції у державній службі України є те, що її суб'єкти і об'єкти відрізняються за правовим статусом та мають різну організаційно-структурну форму [47, с. 203].

З іншого боку О.В. Бандурко зазначає, що ефективність діяльності системи щодо протидії корупційним проявам у системі державної служби в Україні залежить від методів управління та кваліфікації кадрів [106, с. 145].

Адже такого погляду дотримується В.Т. Білоус та інтерпретує тим, що Президентом, Верховною Радою, Кабміном України постійно приділяється увага протидії корупційним проявам у державі і злочинності. З цього приводу підписано та ратифіковано низку міжнародних конвенцій про міждержавне співробітництво, створена певна правова база, сформовані спеціальні структури для боротьби з організованою злочинністю та корупцією.

При цьому, дослідник В.О. Глушков стверджує, що особливе місце в розв'язанні проблем протидії корупційним маніпуляціям, посідає спеціально створений державний орган — **Комітет координації по боротьбі з корупцією і організованою злочинністю при Президентові України**. Саме цей Комітет координує діяльність усіх правоохоронних та інших державних органів щодо виконання законів України, Указів, розпоряджень Президента, Уряду та рішень з питань протидії корупційним проявам та організованій злочинності, розробляє стратегічні та тактичні заходи щодо протидії злочинності та корупції.

Водночас, А.П. Закалюк доводить, що методи державного управління, які застосовуються у сфері протидії корупційним проявам, зокрема у системі державного служби, залежать від стратегії і тактики протидії корупції в Україні, а також від стратегії соціально-економічних перетворень. Визнаючи сукупність методів управління у сфері протидії корупційним маніпуляціям, необхідно враховувати і те, що процес виконання здійснюється та контролюється уповно-

важеним державним органом та його посадовими особами [152, с. 517].

Таким чином, формування єдиної державної антикорупційної політики потребує належного законодавчого *забезпечення, суспільної волі та громадянської активності.* Саме комплекс нормативно-правових приписів, що регулюють, допускають і визначають здійснення механізмів запобігання корупції, а також відповідальність за вчинення корупційних порушень, забезпечення належного координування і реалізації антикорупційної політики в системі превентивних заходів. «Побудова цілісної інституційної системи повинна відповідати міжнародним стандартам у світовій практиці, а саме: конвенціям ООН і Ради Європи проти корупції). При цьому варто враховувати особливості української правової системи, політичної волі та ментальності громадян» [157, с. 25].

Корупційні ризики в публічній службі

Загальноприйнятою є думка, що один із ризиків складає непрозорий та недостатній рівень оплати праці більшості публічних службовців, оскільки присутній суб'єктивізм з боку керівництва у визначенні конкретних розмірів оплати праці. В дійсності, масштабні та суспільно небезпечні корупційні правопорушення здійснюються державними службовцями вищих категорій посад, чиї заробітна плата та соціальні гарантії забезпечують заможне та безбідне життя. За таких обставин рівень моральності та ідеологічної спрямованості при виконанні своїх професійних обов'язків певних держслужбовців мав би бути найвищим. Натомість, моральні та ідеологічні переконання є викривленими і не відіграють для них ролі обмежувачів [110, с. 4]. Виходячи з цього, вважається доцільним використовувати заходи, за-

пропоновані Молдаваном Е.С., зокрема розробки Концепції реалізації морально-ідеологічних антикорупційних заходів у системі протидії зі спекулятивними маніпуляціями.

Безперечно, наявність значної кількості корупційних ризиків становить загрозу для демократичного суспільства. Особливо це стосується ризиків щодо функціонування публічної служби в Україні. Як підкреслює дослідник Хорошенюк О., що сутність антикорупційного законодавства полягає в тому, щоб обмежити та нейтралізувати чинники корупції, запобігти конфліктам інтересів (з особистих та службових потреб), на нормативному рівні визначити межі правомірної та етичної поведінки особи, уповноваженої на виконання функцій держави [178, с. 201].

Адже сучасний розвитку ефективної та прозорої антикорупційної інфраструктури України свідчить про те, що вже встановлена певна нормативна база щодо регулювання питання протидії корупції. До неї можна віднести закон України «Про запобігання корупції», Закон України «Про державну службу», Закон України «Про Національне антикорупційне бюро України», а також Закон «Про антикорупційний суд» та інші. Однак, антикорупційне законодавство потребує постійного оновлення відповідно до змін у стані суспільно-дипломатичних відносин, а також інвестиційної діяльності в сфері інноваційно-виробничої економіки. Лише таким чином можна запобігти появі нових корупційних ризиків та сприяти усуненню існуючих.

Крім того, варто ствердити, що використання необхідних міжнародних стандартів та проведення аналізу досвіду зарубіжних країн з метою подальшого напрацювання конструктивних пропозицій щодо запобігання та боротьби з корупцією в Україні є мудрим рішенням у побудові право-

вої держави. При цьому необхідно здійснювати належний контроль та локальний моніторинг як вияву зловживання владою, використанню службових повноважень в особистих цілях громадянами і публічною владою.

Національна безпека в антикорупційній інфраструктурі України

Національна безпека, згідно ст. 1 Закону України «Про основи національної безпеки України», визначається як захищеність життєво важливих інтересів людини і громадянина, держави та суспільства, за якої забезпечуються сталий розвиток суспільства. своєчасне виявлення запобігання і нейтралізація реальних та потенційних загроз національним інтересам у низці сфер, зокрема у сфері боротьби з корупцією, при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам [54]. У ст. 7 цього Закону також зазначено, що поширення корупції в органах державної влади, зрощення бізнесу і політики. організованої злочинної діяльності» є однією із загроз національній безпеці України, яка негативно впливає на стабільність в суспільстві.

Забезпечення національної безпеки покладається на суб'єктів, вичерпний перелік яких наведено у ст. 4 названого закону України. Це — Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; прокуратура України; Національне антикорупційне бюро України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та

інші військові формування, утворені відповідно до законів України; органи і підрозділи цивільного захисту; громадяни України та об'єднання громадян. Компетенція перелічених суб'єктів у відповідних сферах визначається з урахуванням їх функцій та повноважень, що регламентуються положеннями ст. 9, 10 Закону України «Про основи національної безпеки України».

Діяльність суб'єктів забезпечення національної безпеки створена Конституцією України, Законом України «Про основи національної безпеки України», іншими законодавчими актами, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також виданими на їх виконання іншими нормативно-правовими актами. До них, зокрема, належить і Закон України «Про запобігання корупції», яким визначаються правові та організаційні засади функціонування системи запобігання корупції в Україні, зміст та порядок застосування превентивних антикорупційних механізмів та правила щодо усунення наслідків корупційних правопорушень [52].

До спеціально уповноважених суб'єктів у сфері протидії згідно з п. 13 ч. 1 ст. 1 названого Закону України, відносяться: органи прокуратури, Національної поліції, Національне антикорупційне бюро України та Національне агентство з питань запобігання корупції. Незважаючи на відсутність у зазначеному переліку органів Служби безпеки України спеціальні підрозділи по боротьбі з корупцією та організованою злочинністю вітчизняної спецслужби також відіграють важливу роль у сфері запобігання, виявлення та припинення корупційних правопорушень, керуючись при цьому положеннями ст. 7, 9 Закону України «Про основи національної безпеки України» та ст. 2 Закону України

«Про Службу безпеки України» [55]. За цих обставин розв'язання антикорупційної інфраструктури значною мірою залежить від ефективності функціонування системи забезпечення національної безпеки, яка визначається здатністю своєчасного реагування на кризові ситуації.

Поглиблення концептуального розуміння корупційного діяння як деструктивного соціального явища у правовій системі, заходів щодо його запобігання та протидії, досліджені передумов виникнення сприятимуть розвитку антикорупційної інфраструктури, що є прерогативою в структурному змісті сучасного кіберкапіталу. Тому саме юридична логіка публічного адміністрування в антикорупційному забезпеченні повинна створити якість нормативно-правової бази за вільний доступ громадян до інформації як адміністративно-правового захисту автономії окремих осіб. При цьому, варто стверджувати, що процес прийняття мудрих рішень як фундаментальної матриці розбудови правової держави має бути інформаційно прозорим та відкритим з метою ретельного його розгляду. Все це сприятиме ефективному визнанню ролі активних й незалежних засобів масової інформації в системі кіберкапіталу як запобігання від корупційного впливу політичних та інших складових у суспільному житті.

5.2. Британський досвід протидії корупції

На сьогодні корупція є інтернаціональною проблемою, властивою як розвиненим країнам, так і країнам із низьким рівнем розвитку. Досвід боротьбі з корупцією у Великій Британії налічує не одне століття, отже його було перейнято великою кількістю не лише європейських країн, але й світу.

Ще у період Середньовіччя одним із засобів боротьби із корупцією вважався незалежний аудит, перше нагадування про який міститься у архіві казначейства Англії та Шотландії 1130 р.

На зламі XIX — XX ст. з'являються перші антикорупційні закони — «Про хабарництво в публічно-правових організаціях» 1889 р., «Про продаж посад» 1889 р. «Про попередження корупції» 1906 р. та закон 1916 р., яким були внесені зміни та доповнення до попереднього закону.

Відповідно до Закону про хабарництво 1889 р. особи, що їх визнано винними у вимозі хабара або отриманні чи згоді на отримання подарунка, займу, винагороди або будь-чого, що має цінність, як засобу, який може спонукати службовця вчинити певну дію або утримуватися від її вчинення, повинні понести покарання у вигляді тюремного ув'язнення або сплати вартості отриманого подарунка чи винагороди. Хабарник позбавлявся права бути обраним чи призначеним на публічну посаду терміном на сім років. У разі визнання винною особа може бути назавжди позбавлена службових прав і прав на компенсацію та пенсію.

Закон про продаж посад 1889 р. передбачав відповідальність за корупцію у вигляді позбавлення волі терміном до двох років і позбавлення права обіймати відповідні посади у разі продажу, купівлі, інших угод з метою отримання посади, в тому числі посад, пов'язаних із працею за наймом як на території Сполученого королівства, так і британських колоніях.

Антикорупційні закони 1906 та 1916 р. значно посилили відповідальність за вчинення злочинів у цій сфері. Так, Закон 1906 р. передбачав кримінальну відповідальність, незалежно від того, чи вчинила особа, яка одержала хабар, ті

дії, за вчинення яких його було надано, та незалежно від мотивів, якими користувалася особа, що дала хабара. Покарання за цей злочин — тюремне ув'язнення на строк від трьох до семи років.

Закон 1916 р. предметом хабарництва визначав угоду або пропозицію укласти угоду з центральним урядом або окремими урядовими відомствами.

Окремим складом корупційного злочину, на підставі Закону про попередження зловживань із нагородами 1925 р., вважався підкуп з метою отримання почесних нагород. Покарання для особи, яка дала хабар, — позбавлення волі на термін до двох років та / або штраф, а для особи, що одержала хабар, — позбавлення волі до трьох місяців та/або штраф.

Крім того, британський законодавець передбачає відповідальність за підкуп суддів та суддівських чиновників з метою вплинути на їх дії в межах службових повноважень у вигляді штрафу або позбавлення волі на строк до двох років.

Що ж стосується службовців взагалі, за загальноприйнятими правилами, вони повинні відмовлятися від усіх подарунків у зв'язку з виконанням офіційних обов'язків, окрім різдвяних, якщо це календарі, записники, предмети канцелярського обігу невеликої вартості, що мають назву або знак компанії, що дає можливість розглядати їх як рекламні матеріали.

Для реалізації антикорупційної стратегії держави розроблено Програму затвердження принципів чесності та непідкупності у всіх сферах життя суспільства, на підставі якої у 1994 р. було створено незалежний державний Комітет із стандартів поведінки у суспільному (державному) житті. Цей орган оцінює поведінку, фінансову та комерційну діяльність усіх керівників, в тому числі міністрів, інших

державних службовців, членів Парламенту, представників місцевої влади.

У 1995 р. Комітетом було прийнято Кодекс поведінки, який передбачив наступні принципи державної праці чиновників: непідкупність, об'єктивність, підзвітність, відкритість, чесність, лідерство тощо, які повинні стримувати недобросовісних чиновників від корупційних дій.

На початку XX ст. у Великій Британії замислилися над оновленням антикорупційного законодавства. У 2011 р. набув чинності Закон про протидію хабарям, який є намаганням привести національне законодавство відповідно до міжнародно-правових вимог, зокрема Конвенції Організації економічного співробітництва та розвитку про боротьбу із підкупом іноземних посадових осіб при укладанні міжнародних комерційних угод 1997 р.

Наразі можна визнати, що новий британський закон виявився одним із самих простих і одночасно жорстких у світі. Він складається з 20 статей і передбачає лише чотири склади злочинів: давання хабаря, отримання хабаря, підкуп посадових осіб іноземних держав, невиконання комерційними організаціями обов'язку із попередження хабарництва. Максимальний термін позбавлення волі за вчинення цих злочинів — 10 років позбавлення волі із конфіскацією майна, а також штраф (для компаній).

Крім того, Закон забороняє будь-які види стимулюючих платежів при здійсненні економічної діяльності.

При цьому дія закону розповсюджується, відповідно до принципу екстериторіальності, на злочини, вчинені у будь-якій державі, громадянином або комерційною організацією Великої Британії чи британських заморських територій, особа, яка мешкає на території Об'єднаного королівст-

ва та його заморських територій, та будь-якої компанії, що має бізнес у Британії та на її заморських територіях. Отже, Закон продемонстрував намагання британського законодавця до прозорості як у роботі державних органів, так і комерційній діяльності британських та зарубіжних компаній.

Аналіз міжнародного досвіду у боротьбі з корупцією підтверджує факт, що корупція, як явище, вийшла за межі адміністративно-територіальних кордонів. Прояви корупції чинять свій негативний вплив не тільки на основи національної безпеки, але й на економіку. Досвід Великобританії у боротьбі із корупцією, в тому числі, але не виключно у публічній службі, є одним із найдавніших. Один із перших законів про корупцію в державних органах був прийнятий ще в 1889 році. Аналізуючи законодавство про боротьбу з корупцією Великобританії необхідно звернути увагу на високу правову культуру громадян та сталі традиції професійної етики державної служби.

Варто зауважити, що антикорупційне законодавство Великобританії вимагає від посадових осіб доводити свою невинність, що свідчить про певну презумпцію вини державних службовців. Одним із основних законів в цій сфері, являє собою Закон Великобританії «Про боротьбу з хабарництвом» (UK Bribery Act), що набрав чинності 1 липня 2011 року. Даний закон має екстериторіальну дію та передбачає кримінальне покарання як за отримання, так і за давання хабара. Його дія поширюється на організації, які ведуть бізнес або мають частку свого бізнесу на території Великобританії, а також на державних службовців, при цьому не має значення, де здійснювалися корупційні дії. Антикорупційне законодавство Великобританії визначає наступні корупційні правопорушення: вимога, згода на отримання або отри-

мання хабаря, здійснюване службовою особою; пропозиція, обіцянка або давання хабаря посадовій особі; хабарництво щодо іноземної посадової особи; нездатність запобігти хабарництву представником організації або всією організацією. Корупційне правопорушення вважається скоєним, якщо особа дає хабар державній посадовій особі, а також пропонує переваги, і має намір вплинути на посадову особу, або щоб отримати перевагу при веденні операцій. Давання хабара посадовій особі іноземної держави є правопорушенням, якщо давання хабара відбувається громадянином Великобританії або резидентом, незалежно від місця скоєння. Таке правопорушення вважається вчиненим, якщо фізична особа здійснює дачу хабаря іноземній державній посадовій особі, а також пропонує переваги офіційній особі: з наміром вплинути на іноземну державну посадову особу в якості посадової особи; щоб зав'язати або зберегти ділові відносини або отримати перевагу при здійсненні ділових операцій. Відповідальність за вказані діяння передбачена у вигляді: позбавлення волі на строк до десяти років для фізичних осіб; штраф, розмір якого не обмежений законом, що може застосовуватися як до фізичних, так і до юридичних осіб; конфіскація незаконно отриманого прибутку; компанія може бути виключена зі списку постачальників державних органів; у компанії виникають серйозні репутаційні ризики, які можуть вплинути на ринкову вартість компанії, та інші негативні наслідки [3, с. 35]. Відповідальність розповсюджується як на особу, яка дає хабар (хабародавець), так і на компанію, в інтересах якої це здійснюється. Тобто дія закону розповсюджується на будь-яких осіб, суб'єктів, які мають відношення до компанії, в тому числі на асоційованих осіб.

Вказаний закон також передбачає систему превентивних заходів щодо запобіганню хабарництву. Для того, щоб уникнути відповідальності, компанії повинна довести, що вжила всіх заходів необхідних для виявлення ризиків та попередження корупції, а саме: оцінила ризики настання хабарництва, має місце зацікавленість вищого менеджменту у попередженні та запобіганні хабарництву; регулярна перевірка партнерів, посередників, агентів, бізнес-процесів, втілення антикорупційної політики та заходів в середині компанії Таким чином, мають бути втілені відповідні дисциплінарні процедури в середині компанії, так звані «compliance codes» з метою недопущення давання та отримання хабаря.

Повноважним державним органом в сфері антикорупційного контролю у Великобританії є Управління по боротьбі із шахрайством в особливо великих розмірах (UK Serious Fraud Office) [10, с. 46]. Даний орган є незалежним у своїй діяльності, наділений повноваженнями здійснювати розслідування злочинів у сфері шахрайства, хабарництва та корупції. Це провідне відомство Великобританії в області розслідування і кримінального переслідування у справах про хабарництво і корупцію за кордоном в таких випадках, коли кримінальне переслідування входить в компетенцію Великобританії. Воно також займається справами, пов'язаними з внутрішньою корупцією, попри ті, що є компетенцією поліції і Королівської прокурорської служби. У компетенцію Управління входить відкриття і розслідування справ, що відносяться до найбільш резонансних випадків. Критерієм підключення Управління до розслідування є перевищення розміру грошових коштів, виведених із законного обігу, в 1 млн. фунтів стерлінгів. Цікаво, що юрисдикція вка-

заного органу не розповсюджується на територію Шотландії, острова Мен і Нормандських островів, а розповсюджується в Англії, Уельсі і Північній Ірландії і щодо корупції за кордоном, будь-яким чином пов'язаною з Великобританією. Голова Управління призначається Генеральним прокурором Великобританії і підпорядковуються йому. Одним із спеціальних відділів є відділ збирання інформації про діяльність державних службовців, компаній, фізичних осіб щодо фактів порушення положень Закону «Про боротьбу з хабарництвом». Збирання інформації відбувається конфіденційно, приймаються в тому числі, анонімні звернення, що є проявом громадянської позиції, після чого «потенційний правопорушник зобов'язаний надати мотивовану відповідь та докази вжиття необхідних заходів та процедур із попередження хабарництва» [108, с. 58].

Безпосередньо корупційні процеси у Великобританії відстежує, так званий Комітет Нолана, який було засновано в жовтні 1994 року. Його зусилля зосереджені на основних ділянках громадського життя, які викликають найбільшу стурбованість громадськості: це члени парламенту, які працюють консультантами фірм, що прагнуть впливати на державну політику; це колишні міністри та інші посадові особи, що працюють в тих галузях індустрії, регулюванням яких перед тим займалися в уряді та інші аспекти громадського життя, За результатами роботи Комітету палата Громад парламенту вирішила призначити парламентського директора стандартів, заборонити протекцію та розголосити сторонні заробітки членів парламенту [113, с. 85].

Можна дійти висновків, що у Великобританії діє ефективна система боротьби із корупцією, яка спирається не тільки на законодавство, але й на підтримку держави та

самого суспільства. Прийняті антикорупційні закони виконуються незалежно від рівня правопорушників та їх статків. Не дивно, що саме цю країну міжнародна неурядова організація по боротьбі з корупцією «Transparency International» визначає як одну з найменш корумпованих країн серед 176 країн світу — Великобританія посідає 10-те місце, наряду з Люксембургом та Німеччиною, що свідчить про ефективні її антикорупційної політики. Підсумовуючи вище зазначене, вважаємо, що досвід Великобританії крокує попереду у подоланні корупційний ризиків в публічній службі в порівнянні із досвідом інших країн, в тому числі і України, що беззаперечно позитивно впливає, в кінцевому результаті і на стандарти життя пересічних громадян, їх права та гарантії захищені та дотримані.

З огляду на це протягом останніх років в Україні вищим керівництвом держави зроблено багато кроків у сфері подолання корупції. Зокрема:

- прийнято ряд нормативно-правових актів, положення яких концептуально змінили підхід до питань організації дієвої протидії корупції, посилили відповідальність суб'єктів, упорядкували систему та повноваження органів протидії вказаному протиправному явищу тощо;
- введено систему обов'язкового щорічного електронного декларування суб'єктів відповідальності за вчинення корупційних діянь;
- створено нові державні незалежні інституції (НАБУ, НАЗК, ДБР, САП тощо), діяльність яких направлена на моніторинг дотримання положень законів та підзаконних актів у зазначеній сфері, виявлення корупціонерів, документування їх протиправної діяльності та притягнення винних осіб до юридичної відповідальності (в

першу чергу кримінальної) за вчинення протиправних діянь, які містять ознаки злочину передбаченого відповідною статтею Особливої частини кримінального кодексу України [188, с. 12];

- активно залучається громадськість, представники регіональних та загальнонаціональних ЗМІ до моніторинг) дотримання корупційного законодавства всіма суб'єктами декларування незалежно від посади, рангу, статусу тощо;
- в ЄРДР зареєстровано, документується, оголошено ряд підозр та передано матеріали досудового слідства до суду з приводу вчинення корупційних діянь представниками вищих органів державної влади, суддями, депутатами рад всіх рівнів (в тому числі й народними) тощо.

Однак, як свідчать реалії сьогодення та показники статистичних досліджень [41], громадяни продовжують вважати проблему корупції в повсякденному житті однією з найнагальніших для України (94,4 %), а корумпованість органів влади як окремий випадок, на думку українців, практично не поступається їй за серйозністю (93,8 %). При цьому, 85,5 % дорослого населення України оцінює загальний рівень корумпованості суспільства вище середнього. Лише 1,8 % опитаних вважають корупцію мало поширеною або зовсім відсутньою.

Населенням 40,7 % усіх основних сфер та інституцій України розглядаються як надто корумповані [78].

Також, вважається за доцільне враховувати думку відомого фахівця у сфері вивчення проблем протидії корупції Сар Дж. Пундея, який зазначав про те, що корупція «не є інфекцією, яку раптом може підхопити здорове суспільство. Вона є наслідком явищ і тенденцій політики, економіки

та загалом розвитку держави. Жодна країна ніколи не була повністю вільною від неї» [149, с. 17].

Тому, зважаючи на викладене, беручи до уваги Євроінтеграційні спрямування України, вважається за доцільне вивчити досвід провідних країн у сфері протидії корупції та інтегрувати найбільш прогресивні ідеї до національного законодавства, адаптувавши їх з урахуванням того, що корупція, яка поширена в нашій державі, має свою специфіку.

Однією з країн Євросоюзу, яка не ввела режим безвізового перегину державного кордону з Україною, стала Велика Британія. При цьому, зі слів посла вказаної країни Джудіт Гоф, її держава не вбачає можливостей для візової лібералізації з Україною найближчим часом. Одна із основних причин — тотальна корумпованість у всіх сферах суспільного життя української держави [45].

При цьому Британія, у відповідності до статистичних дослідження рівня поширення корупції, системно перебуває в рейтингу держав з найменшим її рівнем.

Перший нормативний акт про корупцію в державних органах влади було прийнято ще у 1889 р., а акти 1906 і 1916 рр. про упередження корупції стали реакцією суспільства на поширення цього явища. Для відстеження та протистояння корупції, у Великій Британії у жовтні 1994 р. створено так званий Комітет Подана — Комітет із стандартів публічної сфери (це незалежний консультативний орган, який діє при британському уряді. Був створений прем'єр-міністром Дж. Мейджором, а назву отримав від прізвища першого його голови — Дж. Нолана). Створенню цього комітету передував публічний скандал. Так, 20 жовтня 1994 р. англійська газета «The Guardian» надрукувала статтю, в якій стверджувалось, що два члени парламенту, Н. Гамільтон і

Т. Сміт, ініціювали в палаті общин розгляд низки питань на користь відомого бізнесмена М. Аль-Файеда. За даними видання, йшлося про, приблизно, 22 питання, за кожне з яких М. Аль-Файедом було заплачено в середньому по 2000 фунтів стерлінгів. Згодом цей скандал отримав назву «гроші-запитання». Т. Сміт визнав ці звинувачення і те, що він отримав від бізнесмена 25 000 фунтів стерлінгів, та негайно залишив пост молодшого міністра у справах Північної Ірландії. Н. Гамільтон наполягав на помилковості звинувачень, але під тиском прем'єр-міністра Дж. Мейджора був змушений покинути пост міністра Департаменту- торгівлі і промисловості 25 жовтня 1994 р., через п'ять днів після появи публікації. У відповідь на суспільне занепокоєння цією справою, в день відставки Н. Гамільтона прем'єр-міністр оголосив у Палаті общин про створення нового органу — Комітету зі стандартів публічної сфери. До його функцій було віднесено дослідження стану публічної сфери Сполученого Королівства і розробку загальних рекомендацій стосовно виявлених проблем. Зусилля цього комітету спрямовані на запобігання корупції в основних ділянках суспільного життя, пов'язані, здебільшого, з діяльністю членів парламенту, які працюють консультантами фірм, що прагнуть впливати на державну політику, та колишніх міністрів і інших посадових осіб, які працюють у тих галузях індустрії, регулюванням яких перед тим займалися в уряді [182].

В цілому, національне законодавство Великої Британії у сфері боротьби з корупцією є досить розгалуженим. Вказане обумовлено тим, що окремі норми матеріального права, які стосуються правовідносин, які виникають внаслідок вчинення корупційного діяння, можуть міститися у різних нормативних актах різних галузей права.

Для запобігання корупційним діям у сфері державного управління вказаної країни, діяльність державних службовців має низку обмежень. Зокрема, службовцям вищих груп заборонено займатися загальнонаціональною політикою, а брати участь у місцевій політичній діяльності можливо лише з дозволу керівництва відповідного міністерства чи відомства. Такий же дозвіл на участь у політичній діяльності потрібен і для цивільних службовців нижчих груп. За це вони зобов'язані виявляти лояльність та стриманість в усьому, що стосується їхніх установ. Для службовців міністерств і відомств існують також обмеження щодо участі у фінансових операціях. Зокрема, вони не повинні брати участь в угодах із акціями, земельними ділянками й іншим майном, які можуть призвести до зіткнення їхніх приватних інтересів із службовими. Після закінчення служби вони можуть займатися деякими видами діяльності, тільки одержавши на це спеціальний дозвіл [67].

Підсумовуючи вищевикладене, можливо зробити висновок, що у Великій Британії до питань протидії корупції відносяться досить принципово та системно.

У правовій доктрині зазначеної держави є ряд прогресивних та передових ідеї, які необхідно імплементувати до українського законодавства. Однак, на нашу думку, вказаний процес не потрібно реалізовувати шляхом звичайного («сліпого») копіювання. Зазначене обумовлено тим, що норми, які діють у Великій Британії, «не працюватимуть» в Україні внаслідок суттєвих історичних та культурних відмінностей.

Вважається, що у випадках існування масштабної корупції головне — це усунення її причин, а не боротьба з конкретними проявами останньої.

При цьому, необхідно враховувати, що корупційна діяльність розвивається та адаптується до реалій сьогодення, тому антикорупційні заходи повинні бути системним, плановим процесом, який реалізується з врахуванням міжнародного досвіду, однак і розумінням того, що саме корупція в Україні має свою історичну специфіку.

5.3. Досвід Німеччини щодо запобігання корупції

Варто зазначити, що в загальноприйнятому розумінні ризик — це ступінь ймовірності певної негативної події, яка може відбутися в певний час або за певних обставин на території об'єкта підвищеної небезпеки і/або за його межами; це також можливість виникнення та вірогідні масштаби наслідків негативного впливу протягом певного періоду часу. Зокрема, *корупційний ризик* — це показник, за допомогою якого можна було би встановлювати ймовірність корупційних дій та їх наслідки за конкретний проміжок часу [189, с. 62].

Як зазначено в роз'ясненні Міністерства юстиції України від 12.04.2011 р., перше місце серед корупційних ризиків посідає недоброчесність поведінки державних службовців. Одним із основних напрямів у сфері запобігання корупції є виявлення корупційних ризиків, які можуть виникнути в діяльності державних службовців, а також усунення умов та причин виникнення цих ризиків [79].

Виокремлення корупційних ризиків в діяльності посадових і службових осіб публічної влади, а саме: недоброчесність державних службовців; виникнення конфлікту інтересів; безконтрольність з боку керівництва; наявність дискреційних повноважень [183, с. 268].

Саме судова і правоохоронна системи покликані захищати права людини та надбання демократії цивілізованої

держави. Проте реформування судових і правоохоронних органів залежить не лише від концептуального та нормативно-правового забезпечення їх діяльності. Реформуючи ці системи, потрібно розв'язати низку нагальних проблем: однією з яких є подолання корупції у судових і правоохоронних органах та їх комерціалізації, запобігання впливу на їхню діяльність кримінальних і бізнесових структур; забезпечення прозорості діяльності усієї вертикалі правоохоронних органів для громадських інституцій; скорочення чисельності працівників правоохоронних органів з метою підвищення, ефективності їх діяльності та рівня матеріального забезпечення; розробка механізму цивільного демократичного контролю за діяльністю правоохоронних органів (це забезпечить парламентський контроль та участь у призначеннях і звільненнях керівників правоохоронної системи, а також їх звітність). Подоланню корупції сприятиме і реструктуризоване бюджетне планування, а також постійне фінансування судових і правоохоронних органів у повному обсязі. Потрібно також посилити контроль за виконанням законів України, за якими працівники судових і правоохоронних органів не мають права брати участь у будь-якій підприємницькій діяльності [43, с. 222].

На відміну від України, де організація роботи поліції та її підпорядкованість визначені лише у Законі України «Про Національну поліцію» [143], у ФРН правові та організаційні засади діяльності кримінальної поліції визначені не тільки Законом ФРН «Про Федеральну поліцію», але й безпосередньо законом, що регулює діяльність кримінальної поліції — Закон «Про утворення федерального відомства з кримінальних справ» [179].

Це відомство, за словами його керівника Дітера Романа, налічує близько 40 тисяч співробітників. Натомість стежити за безпекою на вулицях окремих міст та поселень — компетенція земельної поліції кожної із 16 федеральних земель. Діяльність земельної поліції визначається земельними законами. А ще, вона орієнтується на єдиний федеральний зразок закону про поліцію (MEPolG), затверджений конференцією міністрів внутрішніх справ федерації та її 16 земель. Крім того, у Німеччині є Федеральне відомство з кримінальних справ — кримінальна поліція — і відповідні автономні відомства в кожній із земель. Ще одна поліцейська організація федерального рівня — це поліція Бундестагу (Polizei DBT), що відповідає за порядок та безпеку в приміщеннях та на території парламенту ФРН. Німеччина — федеративна держава. Кожна з шістнадцяти земель має широкі повноваження й власні міністерства внутрішніх справ. Чи можуть застосовувати зброю співробітники всіх цих відомств? У різних землях дещо різні закони щодо цього. Деякі земельні відомства ухиляються від чіткої відповіді, чи озброєні їхні співробітники, посилаючись на секретність, інші дозволяють носити зброю в оперативних цілях. Німецькі поліцейські в певних ситуаціях мають право застосовувати вогнепальну зброю. І це регламентується федеральними й земельними законами. Приміром, згідно з §§ 60–62 закону про громадську безпеку та порядок федеральної землі Гессен (HSOG), поліцейський має право стріляти на ураження, якщо на злочинця не діють інші методи безпосереднього примусу. Так само допускається вести вогонь по неживих предметах чи — якщо це єдиний спосіб захистити власне життя або життя колеги — навіть попри небезпеку влучити у випадкового перехожого. Можна від-

кривати вогонь при скупчені людей, якщо в натовпі є особи, що скоюють насильницькі злочини й не реагують на повторні попередження. Не дозволяється стріляти в людину, якщо вона виглядає молодше 14 років, але цей пункт не діє, якщо поліцейському загрожує безпосередня небезпека [130].

Про ефективне реформування правоохоронних органів у Німеччині свідчить створена Центральна психологічна служба поліції Баварії, яка швидко та гнучко реагує на актуальні потреби практичних підрозділів. Так, у цій країні жодне планування великих заходів або акцій не обходиться без участі психологів у робочій групі або оперативному штабі поліцейських сил [19].

Разом із тим, у одному з гамбурзьких досліджень виявилось, що лише 9 із 100 допитів у злочинах проти життя відповідали кримінальному процесуальному праву: недостатнє пояснення прав про свободу дачі свідчень та можливості проконсультуватися у правозахисників тощо [11, с. 39].

Під час реформування поліції України, слід враховувати положення ст. 36 Конвенції ООН проти корупції та ст. 20 Кримінальної конвенції Ради Європи про боротьбу з корупцією щодо забезпечення спеціалізації правоохоронців, які здійснюють заходи з боротьби з корупцією. Більше того, це дасть можливість забезпечити виконання Україною рекомендації, наданої в рамках оцінки реалізації Стамбульського плану дій по боротьбі з корупцією, щодо скорочення кількості правоохоронних органів, представники яких уповноважені складати протоколи про адміністративні корупційні правопорушення.

Отже, з огляду досвіду Німеччини *корупційний ризик в Україні* можна більш повно визначити як ступінь, ймовірності корупційного діяння, яке може відбутися в певний час

або за певних обставин на території України; це також можливість виникнення та вірогідні масштаби наслідків корупційних діянь протягом певного періоду часу.

Як показує аналіз досвіду поліції ФРН та України, досить схожими є корупційні ризики, які пов'язані з недоброчесністю, у тому числі недостатнім професіоналізмом державних службовців; виникненням конфлікту інтересів; безконтрольністю або недостатнім контролем з боку керівництва; наявністю дискреційних повноважень.

Усунення корупційних ризиків в діяльності державних службовців, у тому числі поліції, виключить можливість порушення ними законодавства України, позитивно вплине на покращення роботи органів державної влади. Мінімізація корупційних ризиків теж позитивно вплине на роботу та сприятиме підвищенню їх авторитету.

5.4. Вища освіта як протидія корупційним маніпуляціям

На сучасному етапі розвитку освіти в Україні невід'ємною складовою світового інтеграційного процесу є європейська правова інтеграція. У цьому відношенні Європейський Союз існує як співробітництво держав, об'єднаних на основі права, оскільки вперше в історії Європи її намагаються об'єднати не силою, а виключно правовими нормами. Адже право здобуває перемогу там, де «кров і залізо» зазнавали поразки за поразкою протягом століть. Лише союз, заснований на вільному волевиявленні його членів, може сподіватися на тривале існування, в якому важливими цінностями є свобода і рівність, що впроваджуються в життя та гарантуються правовими засобами. Усе це знайшло відображення в установчих договорах, на основі яких було

створено Європейський Союз як єдиний інтелектуальний простір освіти.

Тому існування саме Європейського Союзу постає можливим лише завдяки створенню спільної системи освіти та контролю її якості в адміністративно-правовому аспекті.

Теоретичним осмисленням освіти України в законодавчому полі світової та європейської інтеграції займається значна кількість дослідників. Автори звертають увагу на публікації таких науковців та аналітиків як:

- у світовій та європейській інтеграції як цивілізаційної проблематики — З. Бжезинській, Ю. Габермас, М. Кастельє, Н. Луман, Ю. Павленко, М. Курко, В. Курило, С. Хантінгтон, В. Глушков та ін.;
- з аналізу проблем світового розвитку української освіти, його сучасного етапу та історичних перспектив — Т. Андрущенко, М. Головатий, М. Недюха, В. Баранівській, М. Попович, В. Ткаченко, П. Саух тощо;
- досліджень проблем вищої освіти — В. Андрущенко, М. Згуровський, В. Кремень, Ю. Зіньковський та ін.;
- зарубіжних досліджень проблем університетської освіти — Дж. Вос, Г. Драйден, Б. Кларк, Д. Ньюмен, Б. Ріддінгс та ін.;
- проблем світогляду, ціннісно-правових орієнтацій — В. Гриценко, Л. Губерський, А. Ковальчук, В. Заросило, А. Подоляка, К. Муравйов та ін.

Сьогодні існує значна кількість концепцій освіти України як правової суб'єктності людини. Адже в сучасному стані розвитку України як ціннісно-демократичної та правової держави особливої актуальності набуває саме освіта як протидія корупційним маніпуляціям свідомістю на рівні особистості, держави та суспільства. Такий підхід обумовлений

ефективною правовою культурою та обізнаністю громадян розвиватися швидше та якісніше. При цьому належний рівень (якість, ефективність) реалізації державної політики у сфері освіти обумовлюється сукупністю умов та факторів, серед яких відповідне місце займає контроль як важливий інструмент впливу на організаційно-управлінську діяльність правової свідомості.

Контроль якості освіти

За цих умов варто з'ясувати в сукупній матриці щодо визначення поняття «контроль» (англ. «control» та франц. «controle»), в якій «адміністративно-правовий контроль» відіграє особливу роль. У тлумачних словниках української мови до терміну «контроль» наводяться наступні визначення:

- перевірка відповідності чого-, кого-небудь встановленим вимогам;
- перевірка, облік діяльності кого-, чого-небудь, нагляд за кимось, чимось;
- установа або орган, що здійснює перевірку, нагляд за ким-, чим-небудь [27, с. 243].

Оскільки соціальний контроль є сукупною матрицею впливу на діяльність особистості, держави та суспільства, то варто акцентувати окрему увагу на зміст соціального контролю. У свою чергу, Г.В. Осіпов тлумачить соціальний контроль як систему процесів і механізмів, що забезпечують підтримування соціально прийнятих зразків поведінки та функціонування соціальної системи в цілому [159, с. 78].

У Радянському енциклопедичному словнику [158, с. 1020] соціальний контроль визначено як механізм, за допомогою якого суспільство і його підрозділи (групи, організації) забезпечують дотримання системи обмежень (умов), порушення яких завдає шкоду функціонуванню соціальної системи.

Як вважає дослідник Б.А. Буйвол, що «соціальний контроль слід розуміти як цілісну систему соціальних регуляторів (державних або суспільних інститутів, права, моралі, звичаїв, традицій, установок)» [23, с. 3].

З огляду В.М. Пальченкової соціальний контроль — це механізм, за допомогою якого суспільство та його складові елементи (групи, організації) забезпечує дотримання певних умов (обмежень), порушення яких завдає збитків функціонуванню соціальної системи. В якості таких обмежень виступають правові та моральні норми, звичаї, адміністративні рішення... Однозначно соціальний контроль користується й заохоченням за дотримання соціальних норм [74].

Отже, у широкому розумінні, на наш погляд, соціальний контроль містить у собі низку соціокультурних, політичних, економічних, правових механізмів впливу на структуру свідомості окремої особи, держави та суспільства відповідно їх потребам та інтересам. При цьому, завдяки контролю у поведінці правової суб'єктності людини (особи, групи, членів суспільства) виявляються відхилення від встановлених норм та правил, що у свою чергу сприяє підтримці стабільності та злагодженості функціонування відповідних осіб, груп, класів, етносів.

Особливим проявом соціального контролю є державний контроль, який має різнобічний понятійно-категоріальний апарат, оскільки функція контролю — це спостереження відповідним підконтрольним об'єктом з метою отримання достовірної інформації про стан законності.

Втім, О.Ф. Скакун, Д.А. Бондаренко розглядають державний контроль «як діяльність уповноважених суб'єктів (державних органів і посадовців) з перевірки фактичних даних про відповідність (невідповідність) контрольованих

об'єктів формально-визначеним нормативам (стандартам)» [159, с. 143].

З огляду Т.В. Маматової державний контроль як правова складова — це «реалізація функції втручання держави в діяльність організацій будь-яких сфер діяльності у разі виникнення загрози безпеці (людини, держави, навколишнього середовища; це процес «вироблення коригувальних дій, що базується на порівнянні фактичного та заявленого стану об'єкта відповідно до визначених критеріїв; державний контроль (інформаційний компонент) — це виявлення фактів або намірів, що можуть призвести до виникнення загрози безпеці (людини, держави, навколишнього середовища)» [95, с. 25].

Прозорість та якість української освіти в світлі вимог європейської освітньої інтеграції

Реформування системи освіти в Україні пов'язані з пошуком істини як нових ідей щодо інтеграції у світовий освітній простір. Це запровадження основних положень Болонської декларації, що передбачає врахування національних підходів до організації навчання змісту освіти. Принциповим є те, як здійснюються в правовому полі на практиці новітні документи щодо освіти. Серед них варто назвати, насамперед, такі як Міжнародна стандартна класифікація освіти версій 2011 та 2013 років (у галузевій частині), принципи та інструменти Болонського процесу для вищої освіти (охоплюючи стандарти і рекомендації щодо забезпечення якості).

У цьому аспекті запропонований провідними науковцями НАПН проект Національної стандартної класифікації освіти дав змогу на правових засадах осмислити загальну архітектуру національної освіти, обґрунтувати концепту-

альні пропозиції до оновлення ст. 53 Конституції України, законопроєктів «Про освіту», «Про вищу освіту», «Про професійну освіту» тощо.

Прийнятий новий Закон «Про вищу освіту» є системним проектом змін, що підготовлений у результаті прозорого демократичного діалогу всіх зацікавлених соціальних груп, який здатний вивести вищу освіту України на європейський шлях розвитку, при цьому зміцнити позиції вищого навчального закладу на світовому ринку освіти та інновацій.

Аналізуючи новації Закону, основними його положеннями, на нашу думку, є розширення автономії ВНЗ. Це право розпоряджатись заробленими коштами на власний розсуд, визнавати вчені ступені, отримані в іноземних ВНЗ, самостійно визначати організацію навчального процесу тощо. Адже зовнішнє незалежне тестування (ЗНО) законодавчо закріплено як основний критерій при вступі до ВНЗ. Кожен сертифікат повинен становити не менш як 20 відсотків конкурентного балу; встановлюються такі освітньо-кваліфікаційні рівні і ступені молодший спеціаліст, бакалавр, магістр, доктор філософії, доктор наук.

Доступ до Єдиної державної електронної бази з питань освіти має здійснюватись через офіційний веб-сайт МОН. До неї вноситься вся інформація про видані дипломи; створено Національне агентство з якості вищої освіти, яке проводитиме ліцензійну експертизу, а також акредитацію спеціальності.

Як і раніше, статус національного відповідному вищому національному закладу присвоює Президент, але за поданням Національного агентства з якості вищої освіти; визначено розмір мінімальної стипендії для бакалаврів і магіст-

рів — не менше прожиткового мінімуму, а для молодшого спеціаліста не менше третини; закон «Про вищу освіту» не передбачає норми щодо відпрацювання для студентів ВНЗ, які навчаються за рахунок державного чи місцевого бюджетів; надані широкі демократичні права; трудовий колектив сам обиратиме ректора, а МОН підписуватиме з ним контракт; значно розширені в новому законі свободи студентського самоврядування [51].

Моніторинг якості системи освіти

Управління якістю освіти не може бути ефективним без наявності правової контрольованої системи, що дозволяє отримати своєчасну достовірну інформацію. На сучасному етапі контролю та якості освіти здійснюється запровадження різноманітних методів технологій збирання і обробки здобутої інформації, що вимагає налагодження моніторингу як правової інформаційної системи.

Загальновідомо, що моніторинг — це відстеження, діагностика, прогнозування результатів діяльності, що попереджає неправомірну оцінку події, факту за даними одиничного виміру (оцінювання).

Основна мета моніторингу якості системи освіти — це створення інформаційних умов для формування цілісного уявлення про правовий стан системи освіти, про якісні та кількісні зміни в ній, а також і доступ до цієї інформації громадськості, різних суб'єктів (користувачів) освітніх послуг.

У державній політиці система моніторингу регулюється Постановою Кабінету Міністрів України від 14 грудня 2011 року № 1283 «Про порядок проведення моніторингу та оцінки якості освіти». Стосовно цієї правової норми основними завданнями моніторингу є: отримання об'єктивної інформації і про якість освіти, стан системи освіти, а також

прогнозування її розвитку, оцінювання правового стану системи освіти відповідно до завдань державної політики в сфері освіти, правового забезпечення структурних підрозділів державної влади статистичною та аналітичною інформацією про якість освіти.

Основними методами проведення моніторингу є: достовірність (об'єктивність) оброблення інформації про якість освіти; системність оцінювання якості освіти в законодавчому полі її діяльності; оперативність доведення до відома управлінських структур освітою та громадськості результатів моніторингу.

Таким чином, органіторинг є правовим інструментом оперативного отримання даних про явища (події, факти) і процеси, що відбуваються в освітній діяльності вищих навчальних закладів. Це надає правову змогу до оперативного (мобільного, швидкого) реагування та координування за якістю освітнього процесу. Саме у цьому контексті імплементація закону «Про вищу освіту» є нормативно-правовим удосконаленням зовнішніх інститутів забезпечення якості вищої освіти.

Компетентність як запорука якості освіти

Традиційно завдання освіти визначається низькою знань, умінь та навичок, які повинна опанувати людина як правова суб'єктність у законодавчому полі діяльності. У цьому відношенні саме компетентність відповідає необхідному усвідомленню сучасних завдань освіти.

У світовій освітній практиці поняття компетентності є визначальним. Центральні компетенції, визначені на симпозіумі «Ключові компетенції для Європи» (1996 р., м. Берн), ознаменували загальносвітову тенденцію оновлення освітнього процесу.

Необхідно вважати, що компетентнісний підхід — це один із факторів, що сприяє модернізації змісту освіти, оскільки доповнює сукупність освітніх інновацій. Молодь завдяки освіті має опанувати міжкультурні компетенції: прийняття відмінностей, повага до інших і здатність жити з людьми інших культур, мов і релігій. Адже компетентність надає здатність вчитись навчатись в інформаційному суспільстві, в якому безперервне навчання є нормою особистого, професійного та правового життя.

Саме така матрична формула комплектності (універсуму) є вільною ідеєю для єдиного правового поля світової та європейської освіти, що передбачає володіння усною та письмовою комунікацією.

Нормативно-правова інформація в системі освітньої ентропії

У сучасних межах високоорганізованих цілісних систем функціонують специфічні механізми контролю та якості освіти. При цьому логічним є вивчення нормативно-правової інформації у взаємозв'язку із ентропією як теорії випадкових подій (фактів, ситуацій тощо) у системі їх невизначеності, що загалом становить закономірний процес. Така міра невизначеності, невпорядкованості правової системи є її тлумаченням як виразник інформаційних можливостей освітньої сфери діяльності.

Крім того, необхідно зауважити, щоб зберегти власну (кожного, всіх) якісну визначеність освіти, цілісна високоорганізована система не повинна бути занадто визначальною метою убезпечення її контрольного впливу.

Безперечно, не повною мірою нормативно-правова інформація здатна виконувати функцію усунення невизначеності у правових утвореннях освіти. Такого роду інформація

призводить до зростання ентропії в освітній системі. В результаті нелінійності навколишньої інформації може відбуватися негадана зміна стану системи — біфуркація як вияв нового життєвого циклу.

Саме така структура «правової системи визначає траєкторію її еволюції у напрямі щодо досягнення стану аттрантора, досягнувши якого система еволюціонує навколо свого стану рівноваги... Це видається можливим виключно за умови долання процесу структурних змін, викликаних або потужним зовнішнім впливом, або накопиченням внутрішнього хаосу, що призводить до незворотних змін та відхилення від стану рівноваги [122, с. 122].

Таким чином, існує значний науковий інтерес до вивчення ентропійних процесів, що відбуваються в сфері освіти, оскільки сутнісні характеристики цих процесів є малодослідженими. На наш погляд, саме це і є випадкова закономірність, оскільки невизначеність, що внутрішньо відповідає процесам структурних змін, в даному разі освіти, викликає ризикові процеси у реальній правовій дійсності. Тому нормативно-правова інформація в системі освітньої ентропії є критерієм якості упорядкування законодавчого поля, що артикулює загальні закономірності та її наукове прогнозування.

Шляхи протидії корупційним маніпуляціям у вищій освіті України

Як відомо, корупція має прояви на різних рівнях суспільства. Тому деструктивний вплив цього явища може спричинити шкоду як стосовно окремих осіб, так і системи в цілому. З огляду юридичного оформлення заходів у боротьбі з корупцією має відбуватися шлях імплементації відповідних положень до чинних нормативно-правових актів.

Наприклад щодо функціонування субсистеми спеціального антикорупційного громадського моніторингу в системі вищої освіти України з внесенням відповідних поправок до кримінально-виконавчого кодексу України.

За цих умов нагальним є питання щодо блокування ініціатив у сфері освіти, що спрямовані на дискредитацію і нейтралізацію викривачів корупції. Подібне блокування носить значною мірою політичний характер, оскільки матрицею для корупційного середовища виступає корупційна діяльність саме у політичному середовищі країни, що дозволяє реалізувати неправомірні ініціативи з корупційним елементом.

Необхідно зазначити, що корупція стала звичайним явищем у багатьох цивілізованих державах, матеріальний добробут й сталі політичні традиції яких дають змогу приховати розмах величезного збитку, який корупція завдає соціальній і гуманітарні сферам. Тому на належному рівні в освітній сфері України має працювати громадський нагляд за розслідуванням справи про корупційне діяння. Саме такий громадський контроль у якості експертної комісії повинен стежити за негативними корупційними явищами. Для цього повинен створюватись на робочих місцях моральний клімат у боротьбі з хабарництвом.

Прикладом цьому може слугувати Великобританія як країна менш корумпована порівняно з іншими країнами Європи. «В юриспруденції Великобританії не існує загально визначеного терміну «корупція», закріпленого в нормативно-правових актах, але існує велика кількість дефініцій цього поняття» [5, с. 271]. При цьому, суб'єктами корупційних правопорушень у Великобританії є публічні посадові особи, хоча у певних випадках ними можуть бути й інші

державні службовці та будь-які особи, у тому ж числі юридичні. Проти них законодавством Великобританії застосовуються порівняно «м'які» санкції за вчинення корупційних правопорушень.

Таким чином, саме сприятливий моральний клімат у вищій освіті України, ефективні умови для інтелектуального розвитку між суб'єктами права різних країн можуть бути створені лише за наявності демократично-ціннісної узгодженості національних правових систем партнерів. Серед них мовний закон має бути важливим елементом у міжнародному паритеті. Для цього повинен здійснюватися єдиний європейський інтелектуальний простір, що забезпечуватиме гармонізацію та зближення законодавств окремих країн у сучасних умовах мультикультуралізму. Таке існування спільного освітнього ринку повинно досягатися завдяки правовим нормам та світовим і загальноєвропейським стандартам.

Контрольні запитання

1. Назвіть геополітичні особливості сучасного інформаційного простору.
2. Дайте визначення кіберзброї.
3. Основні об'єкти при застосуванні кіберзброї у мирний та воєнний час.

Теми рефератів

1. Засоби для ураження і знищення інформаційної системи.
2. Основні способи застосування кіберзброї.
3. Об'єкти деструктивного інформаційного впливу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cooruption, Inequality, and the Rule of Law : The Building Pocket Makes the Easy Life / By Eric M. Uslaner. — Cambridge University Press, 2008. — 360 p.].
2. Council of Europe Convention on Access to Official Documents, Tromso, 2009 / / CETS № 205.
3. Breslin, Brigid ; Doron Ezickson ; John Kocoras (2010). «The Bribery Act 2010 raising the bar above the US Foreign Corrupt Practices Act». Company Laweyr. Sweet & Maxwell. 31 (II) . ISSN 0144-1027 C. 35.].
4. Charter of the United [Електронний ресурс]. — Режим доступу: http://www.un.orglen/documents/charter/.].
5. Cooruption, Inequality, and the Rule of Law : The Building Pocket Makes the Easy Life / By Eric M. Uslaner. — Cambridge University Press, 2008. — 360 p.].
6. Council of Europe Convention on Access to Official Documents, Tromso, 2009 / / CETS № 205.
7. Hells U., Karras A., Scherer K.R. Multichannel communication of emotion: synthetic signal production // Facets of Emotion. Recent research / Ed. K.R.Scherer/ — Hillsdate, N.J. — 1988. — P. 162.
8. Resolution adopted by the General Assembly UN [on the report of the First Committee (A/53/576)] «Development in the field of information and telecommunication in the context of information security». — Distr. General A/RES/53/70, 4 January, 1999, N.Y.
9. Sullivan, G. (2011). «The Bribery Act 2010 : Part One: an overview». Criminal Law Review. 2011 (2). ISSN 0011-135X. C. 46.
10. Альбрехт П.-А. Правове і політичне есе про розвиток в системі кримінального правосуддя Німеччини — полі-

ція, прокуратура, захист та кримінально-виконавча система // Der eigene weg der Ukraine. Deutschland : Berliner Wissenschafts-Verlag. 2013. 302 p.
11. Аналітичний звіт «Корупційні ризики надання адміністративних послуг та контрольно-наглядової діяльності в Україні», підготовленого Центром політико-правових реформ та фондом «Демократичні ініціативи» [Електронний ресурс]. — Режим доступу: https://www.coe.int/t/dghl/cooperation/economiccrime/corruption/technical%20papers/344-upac-coruption-admin ControlSup-uk.pdf.
12. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є Основи кібербезпеки / За ред. проф. В.О. Хорошка. вид., доп. і перероб. — К. : Вид. ДУІКТ, 2009. — 292 с.
13. Арістова, І.В. Державна інформаційна політика : організаційно-правові аспекти : Монографія / І.В. Арістова. — Х. : Вид-во ун-ту внутр. справ, 2000. — 368 с.
14. Баранов О.А. Інформаційне право України : стан, проблеми, перспективи / О.А. Баранов. — К. : ВД «Софт-Прес», 2005. — 316 с.
15. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов — СПб. : Юридический центр Пресс, 2001. — 789 с.
16. Беззубов Д.О. Суспільна безпека (організаційно-правові засади забезпечення): монографія / Д.О. Беззубов. — Київ : «МП Леся», 2013. — 425 с.
17. Бесчастний В. Міжнародний досвід у діяльності міліції України // Віче. Грудень, 2009. — № 24. URL : http://veche.kiev.ua/joLirnal/1780/7feed (дата звернення: 06.03.2018).
18. Биккенин Н.Б. Социалистическая идеология. 2-е изд., доп. / В. Биккенин. — Москва : Политиздат, 1983. — 415 с.

19. Битяк Ю.П. Адміністративне право України : підручник / [Битяк Ю.П., Богуцький В.В., Гаращук В.М. та ін.] ; за ред. Ю.П. Битяка. — Харків : Право, 2007. — 520 с.
20. Бодрияр Ж. Символический обмен и смерть / Ж. Бодрияр. — Екатеринбург : У-Фактория, 2006. — 200 с.
21. Буйвол Б.А. Социальний контроль и его воздействие на поведение людей : автореф... канд. юрид. наук. — Киев, 1973. — С. 3.
22. Бусарев Г. Авторские права в рекламе / Г. Бусарев // [Електронний ресурс] : Режим доступу: http://www.reklamodatel.ru/static/art2359.htm].
23. В Україні найближчим часом з'явиться доктрина кібербезпеки http://na.mil.gov.ua/25677-v-ukra%D1%97ni-najblizhchim-chasom-zyavitsya-doktrina-informacijno%D1%97-bezpeki].
24. Ващук Я. Використання об'єктів інтелектуальної власності в рекламі / Я. Ващук // [Електронний ресурс] : Режим доступу: http://patent.km.ua/ukr/articles/i487.
25. Великий тлумачний словник сучасної української мови (з дод. і допов.) / [уклад. і голов. ред. В.Т. Бусел]. — К. ; Ірпінь : ВТФ «Перун», 2005. — 1728 с.
26. Висновок на проект Закону України «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917–1991 років» (реєстр. № 2540 від 03.04.2015 р.).
27. Войцих Н.М. Державна політика в українському інформаційному просторі: стан та проблеми [Електронний ресурс] / Н. Войцих // Режим доступу : http://www.ijimv.knukim.edu.ua/zbirnyk/1_2/2-vojzih.pdf.
28. Гілея. Науковий вісник. Випуск 71 (№ 4). К. 2013 р. — С. 752.

29. Голобуцький, О. «Електронний уряд» / О. Голобуцький, О. Шевчук. — [Електронний ресурс] — Режим доступу : http://golob.narod.ru/egovper.html.
30. Горбулін В.П. Національна безпека — щит держави // Урядовий кур'єр. — 1996 — 22 серпня (№ 157–158).
31. Горбулін В.П. Стратегічне планування: вирішення проблем національної безпеки : монографія / В.П. Горбулін, А.Б. Качинський. — Київ : НІСД, 2011. — 288 с.
32. Гура М. Реклама як об'єкт авторського права / М. Гура // [Електронний ресурс] : Режим доступу: http://www.yurgazeta.com/oarticle/1019/].
33. Давидов П. Освіта України в контексті світових цивілізаційних конфліктів. // П. Давидов / Всеукраїнська науково-практична конференція з міжнародною участю 14–15 травня 2015 р. Модернізація соціогуманітарного простору: історичний досвід, виклики та перспективи. Збірка матеріалів. — Житомир-Вінниця. — С. 95–99.
34. Даль В. Толковый словарь живого русского языка : В 4-х томах / Владимир Даль. — Москва : Русский язык, 1980. — Т. 4. — 894 с.
35. Данільян О.Г. Національна безпека України: структура та напрямки реалізації : [навч. посібник] / О.Г. Данільян, О.П. Дзьобань, М.І. Панов. — Х. : Фоліо, 2002. — 285 с.
36. Джури И. Средства массовой информации в вооруженных силах США // Зарубежное военное обозрение. — 1992. — № 8. — С. 21–22.
37. Дзьобань О.П., Ставицька О.В. Депривaційний стан суспільства і питання національної безпеки // О.П. Дзьобань, О.В. Ставицька / Психологічні аспекти національної безпеки: Тези Другої Міжнародної науково-практич-

ної конференції. — Львів : Львівський державний університет внутрішніх справ, 2008. — С. 70–75.
38. Довідник «Основні засади діяльності прес-служб органів державної влади та місцевого самоврядування: світовий та український досвід». — Донецьк : ДонДУУ, 2011. — 96 с.
39. Дослідження щодо стану справ з корупцією [Електронний ресурс]. — Режим доступу : http://pravo.org.ua/ua/news/20872033-1.3.-doslidgeennya-schodo-stanu-sprav-z-koruptsieyu.
40. Дубас О.П. Інформаційний розвиток сучасної України у світовому контексті : монографія / О.П. Дубас. — К. : Ґенеза, 2004. — 208 с.
41. Дунаєва Т.Є. Європейський досвід реформування судових та правоохоронних органів // Питання боротьби зі злочинністю : зб. наук. пр. ІВПЗ НАПрН України. Вип. 20. Х. : Право, 2010. С. 222–230.
42. Европейская конвенция об обустройстве и предпринимательстве от 13 декабря 1955 г / Международная организация по миграции // Сборник международных правовых документов, регулирующих вопросы миграции. — М., 1994 г.
43. Електронний ресурс]. — Режим доступу : https:// www.volyn.com.ua/nevvs/94485-ukraintsi-ne-otrymaiut-bezvizu-z-velykobrytaniieiu-cherez-koruptsiiu-v-derzhavnii-mihratsiinii-sluzhbi.
44. Жарков Я.М. Кібербезпека особистості, суспільства, держави : підручник / Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва та ін. — К. : Видавничо-поліграфічний цента Київський університет», 2008. — 256 с.
45. Жук І. Корупція в Україні : спроба аналізу // Наук. вісник Національної академії ДПС України (економіка, право). — 2001. — № 2. — С. 203.

46. Жуков В. Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. — 2001. – № 1. — С. 2–9.
47. Загальна декларація прав людини. Прийнята Генеральною Асамблеєю ООН 10 грудня 1948 р. / Док.ООН/PES/317 А.
48. Закон України «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції» http://zakon4.rada.gov.ua/laws/show/577-19].
49. Закон України «Про вищу освіту» [Електронний ресурс] — режим доступу www.golos.com.ua/Article.aspx &id=345592].
50. Закон України «Про запобігання корупції». Відомості Верховної Ради України. — 2014. — № 49. Ст. 2056.
51. Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради. — 1992. — № 48. — 650 с.
52. Закон України «Про основи національної безпеки України». Відомості Верховної Ради України. — 2003. — № 39. — Ст. 351.
53. Закон України «Про Службу безпеки України». Відомості Верховної Ради України. — 1992. — № 27. Ст. 382.
54. Здравомыслов А. Г. Потребности. Интересы. Ценности / А. Г. Здравомыслов. — М. : Политиздат, 1986. — 223 с.
55. Зернецька, О. В. Глобальний розвиток систем масової комунікації і міжнародні відносини. — К. : Освіта, 1999. — 351 с.
56. Зотова О.В. Правовий режим космического пространства как важный элемент піддержки международного мира и безопасности / О.В. Зотова, Ю.М. Колосов // Московский журнал международного права. — 2011. — № 2.

57. Інтермен як нова особистість / І.Девтеров // Вища школа. — К. : Знання, 2011. — № 9. — С. 83–91.
58. Кібербезпека держави: підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.]; в 2 т. — Т. 2. / за заг. ред. В.В. Остроухова. — К. : ДНУ «Книжкова палата України», 2016. — 328 с.
59. Кабмін схвалив законопроект про заборону антиукраїнських книжок та введення дозволів для російських. — Електронний ресурс: — Режим доступу: http://www.unian.ua/politics/1510723-kabmin-shvaliv-zakonoproekt-pro-zaboronu-antiukrajinskih-knijok-ta-vvedennya-dozvoliv-dlya-rosiyskih.html].
60. Калюжний Р.А. Інформаційне забезпечення управлінської діяльності в умовах інформатизації : організаційно-правові питання теорії і практики : підручник для студ. вищ. навч. закл. / Р.А. Калюжний, В.О. Шамрай, М.Я. Швець та ін. ; за ред. Р.А. Калюжного та В.О. Шамрая. — К. : Академія державно-податкової служби України, 2002. — 296 с.
61. Кісілевич-Чорнойван О.М. Міжнародне інформаційне право : навч. посібник. — К. : ДП «Вид. Дім «Персонал», 2011. — 160 с.
62. Клейменова С. Авторські правовідносини як форма реалізації правомочностей суб'єктів авторського права: Автореф. дис... канд. юрид.наук : 12.00.03. / НАН України. Ін-т держави і права ім. В.М. Корецького. — К., 2004. — 20 с.
63. Когденко А.Р. Жінка у космосі. Актуальні проблеми експериментальної медицини. IV науково-практична конференція 27–28 травня 2002 року. Київ. — 81 с.
64. Колесник, О.С. Поет та відтворення архетипу у міфопоетичному світо відношенні / О.С. Колесник // Актуальні

філософські такультурологічні проблеми сучасності : Зб. наук. праць. — Київ, 2000. — С. 124.
65. Колісніченко Н.М. Державна служба в Європейському Союзі. — С. 40–47.
66. Колосов Ю.М. Международное космическое право / Ю.М. Колосов, В.И. Кузнецов : учебник «Международное право» (гл. XIII). — М. : 1998. — 364 с.
67. Конвенція про захист прав та гідності людини у зв'язку із застосуванням біології і медицини : Конвенція про права людини та біомедицину», прийнята радою Європи в 1997 р.
68. Конвенція про кіберзлочинність від 23.11.2001. [Електронний ресурс]. — Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575].
69. Конвенція про міжнародну відповідальність за шкоду, завдану космічними об'єктами. Електронний ресурс. — Режим доступу : http://zakon4.rada.qov.ua/laws/show/502/96]
70. Конституція України від 28 червня 1996 року // Відом. Верховної Ради України. — 1996. — № 30. — Ст. 141.
71. Концепція національної безпеки України // розбудова держави. — 1997. — № 4. — С. 41–46.
72. Концепція соціального контролю в сучасній теоретико-правовій науці / В. М. Пальченкова // Юридична наука. — 2015 — № 8 — С. 7–14 — Режим доступу : http://nbuv.gov.ua/UJRN/jnn_2015_8_3].
73. Копан О.В. Забезпечення внутрішньої безпеки України : теоретико-управлінські засади. Введення в поліцейську стратегію : монографія / Копан О.В. — Київ : НАВС України, 2001. — 427 с.
74. Кормич Б.А. Кібербезпека: організаційно-правові основи : Навч. посібн. / Б.А. Кормич. — К. : Кондор, 2008. — 382 с.

75. Кормич Б.А. Організаційно-правові засади політики кібербезпеки України : монографія / Б.А. Кормич. — О. : Юридична література, 2003. — 472 с.
76. Корупційні практики в Україні : сприйняття vs реальний досвід громадян [Електронний ресурс]. — Режим доступу : https://wwvv.oporaua.org/novyny/41958-korupts iini-prakt\ky-v-ukraini-spry'iniattia-vs-reahiyi-dosvid-hro madian].
77. Корупційні ризики в діяльності державних службовців : роз'яснення міністерства юстиції України від 12.04.2011 р. [Електронний ресурс]. — Режим доступу : http://zakon5. rada.gov.ua/laws/show/n0026323-11].
78. Корупційні ризики в публічній службі : компаративно-правовий аналіз досвіду країн Східної та Західної традицій права»: тези доповідей регіонального науково-практичного круглого столу, м. Запоріжжя : ЗНУ, 2018. — 244 с.
79. Круглий стіл Партнерство «Відкритий уряд» в Україні : Перезавантаження http://ti-ukraine.org/news/oficial/5308. html].
80. Кудрявцева С.П., Колос В.В. Міжнародна інформація. Навчальний посібник / С.П. Кудрявцева, В.В. Колос. — К. : Видавничий Дім «Слово», 2005. — 400 с.
81. Курко М.Н. Адміністративно-правове регулювання вищої освіти в Україні [Текст] : монографія / М.Н. Курко ; Харк. нац. ун-т внутр. справ. — Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2010. — 376 с.
82. Ліпкан В.А. Кібербезпека як складова національної безпеки України / В.А. Ліпкан // Інформаційні технології в економіці, менеджменті і бізнесі : Проблеми науки, практики і освіти : Зб. наук. праць VIII Міжнар. наук.-

практ. конф. — Ч. 2. — К. : Вид-во Європ. ун-ту, 2003. — С. 443–453.
83. Ліпкан В.А., Ю.Є. Максименко, В.М. Желіховський. Кібербезпека України в умовах євроінтеграції : Навчальний посібник. — К. : КНТ, 2006. — 280 с.
84. Лісовський П.М. Інформологія : Людина і Всесвіт : навч. посіб. — К. : Видавничий дім «Кондор», 2018 — 152 с.
85. Лісовський П.М. Феномен маніпуляції свідомістю : сутність, структура, механізм у сучасному суспільстві (соціально-філософський аналіз) [Текст] : дис. ... канд. філос. наук : 09.00.03 / Лісовський Петро Миколайович ; Укр. держ. ун-т фінансів та міжнар. торгівлі. — К. , 2009. — 191 с.
86. Лісовський П.М. Феноменологія мудрості: духовні пріоритети та імперативи (соціально-філософський контекст) : монографія / П.М. Лісовський. — Київ : Вид-во НПУ імені М.П. Драгоманова, 2016. — 351 с.
87. Логунов, А.Б. Региональная и национальная безопасность : Учебное пособие / А.Б. Логунов. — М. : Вузовский учебник, 2009. — 432 с.
88. Лопатин, В.Н. Вопросы военной реформы и национальной безопасности России / В.Н. Лопатин // Вестник Межпарламенской Ассамблеи СНГ. — СПб., 1996. — № 2. — С. 38–42.
89. Лукк А.А., Нерсесов И.А. Вариации во времени различных параметров сейсмотектонического процесса // Изв. АН СССР. Физика земли. — 1982. — № 3. — С. 10–33.
90. Макаренко Є.А. Проблема безпеки в інформаційному суспільстві / Є.А. Макаренко // Інформаційні системи. Шлях України. — К. : Фонд «Інформаційні системи України», 2004. — С. 24–25.

91. Макаренко, Є.А. Міжнародна інформаційна політика: структура, тенденції, перспективи : Дис. д-ра політ. наук : 23.00.04 / Київ. націон. ун-т ім. Т. Шевченка. — К., 2003. — 475 с.
92. Максименко Ю.Є. Теоретико-правові засади забезпечення кібербезпеки України : дис.... канд. юрид. наук : 12.00.01 / Ю.Є. Максименко. — К., 2007. — 186 с.
93. Маматова Т. Трактування поняття «державний контроль» у сучасному законодавстві України та його уточнення / Т. Маматова // Вісник державної служби України. — 2004. — № 1. — С. 23–26.
94. Мамчур Л. Правове регулювання реклами (цивілістичний аспект) : Автореф. дис... канд. юрид. наук : 12.00.03 / Львів. нац. ун-т ім. І. Франка. — Л., 2006. — 20 с.
95. Марущак А.І. Кібербезпека як об'єкт дослідження правової науки / А.І. Марущак // Актуальні проблеми управління кібербезпекою держави : зб. матер. наук.-прак. конф., 17 березня 2010 року м. Київ. — К. : Наук. вид. відділ НА СБ України, 2010. — С. 36–41.
96. Марущак А.І. Інформаційне право : Доступ до інформації : Навч. посіб. / А. І. Марущак. — К., 2007. — 280 с.
97. Марущак, А. І. Інформаційне право: регулювання інформаційної діяльності : Навчальний посібник. К. : Видавничий дім «Скіф», КНТ, 2008. — 344 с.
98. Мастяниця Й.У., Соснін О.В., Шаманський Л.Є. Інформаційні ресурси України: проблеми державного регулювання : Монографія / За заг. ред. О.В. Сосніна. — К. : ЮСД, 2002. — 141 с.
99. Матузов Н.И. Правовая система и личность / Н.И. Матузов. — Саратов : Изд-во Саратовской госуд. акад. права, 1999. — 459 с.

100. Медвідь Ф. М., Буга Р. І. Національні інтереси України та їх пріоритети в умовах глобалізованого світу: небезпеки та загрози // Наукові праці МАУП, 2010. — Вип. 3 (26). — С. 113–117.].
101. Медвідь Ф.М. Доносо В.Д.Х., Доносо В.С.Ф. Кібербезпека України в системі національної безпеки / Ф.М. Медвідь, В.Д.Х. Доносо, В.С.Ф. Доносо // Проблеми модернізації України : [зб. наук. пр.]. Вип. 1: Матеріали Всеукр. наук.-практ. конф. «Модернізація України: проблеми та технології успішності (питання економіки, права, соціології, освіти і культури)», 12 листопада 2015 р. / редкол. : А.М. Подоляка (голова) [та ін.] — Київ : ДП «Видавничий дім «Персонал», 2015. — С. 194–199.
102. Медвідь Ф.М., Димарчук О.Л., Курчина Т.О. Глобалізація засобів масової інформації: концептуальні засади // Наукові праці МАУП / Редкол. : А.М. Подоляка (гол. Ред.) [та ін.]. — Вип. 4(31). — Київ : ДП «Видавничий дім «Персонал», 2011. — С. 88–92.
103. Международное космическое право / П/р. Пирадова О. С. — М. 1997. — 200 с.
104. Мельник М.І. Корупція: сутність, поняття, заходи протидії : монографія / М.І.Мельник. — К. : Атіка, 2001. — С. 145.].
105. Мендельброт Б. Фрактальная геометрия природы. — М. : Мысль, 2002. — 126 с.].
106. Минаева Т. Новый подход к борьбе со взяточничеством в Великобритании / Слияния и поглощения. 2013, — № 3, с. 58.
107. Міжнародні правові акти та законодавство окремих країн про корупцію. Упорядн. М. І. Камлик, Є. В. Невмержицький, Л. М. Частка, А. О. Мірошник. За ред. Романюка Б. В., Камлика М. І. — К. : Шкляр, 1999.

108.Молдован Е.С. Напрями запобігання та протидії корупції на державній службі : морально-ідеологічний аспект. — С. 1–7.
109.Набруско В. Чи стане Україна господарем у власному інформаційному просторі? / В. Набруско // Дзеркало тижня. — 2008. — № 34 (713). — С. 9–12.
110.Набув чинності закон про заборону частини російських фільмів і серіалів, а також деяких телепрограм. Електронний ресурс. — Режим доступу: http://ru.telekritika.ua/pravo/2015-06-04/107794].
111.Незнамова З.А. Понятие коррупции и коррупционных преступлений // Международное сотрудничество в сфере борьбы с транснациональной преступностью и коррупцией: Материалы международной научно-практической конференции 30–31 марта 2000 — Екатеринбург, 2000. — Вып. 1. — С. 84–91.].
112.Нижник, Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : [навч. посіб. для вищих навч. закл.] / Н.Р. Нижник, Г.П. Ситник, В.Т. Білоус; за заг. ред. П.В. Мельника, Н.Р. Нижник. — Ірпінь, 2000. — 304 с.].
113.Общая теория права и государства : учебник / под. ред. В. В. Лазарева. — М. : Юристь, 2000. — 520 с.
114.Ожегов С.И. Словарь русского языка : 70000 слов / сост. С.И. Ожегов / под ред. Н.Ю. Шведовой. — Изд. 23-е. — М. : Изд-во «Рус. яз.», 1990. — 915 с.
115.Ожегов С.И. Толковый словарь русского языка : 72500 слов, 7500 фразеологических выражений / Ожегов С.И., Шведова Н.Ю. / Рос. АН ; Ин-т. русского язика ; Рос. фонд культуры. — [2-е изд., испр. и доп.] — Москва : АЗЪ, 1994. — 907 с.

116. Окинавская хартия глобального информационного общества (Дата проголошення 22.07.2000) [Електронний ресурс]. — Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=998_163.].
117. Олійник О.В. Кібербезпека України: доктрина адміністративно-правового регулювання : дис ... д-ра юрид. наук : 12.00.07 / О.В. Олійник; Ін-т законодавства Верховної Ради України. — Київ, 2013. — 451 с.
118. Олійник О.В., Соснін О.В., Шиманський Л.Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної України // Держава і право : Збірник наукових праць. — Вип. 13. — С. 534–541.
119. Остапишин П.П. Забезпечення кібербезпеки у галузі реклами: методологічні підходи / П.П. Остапишин // Науковий вісник НЛТУ України. — 2003. — Вип. 23.7. — Ст. 368–372.
120. Павлова Ю.В. Правовая энтропия : дис... канд. юрид. наук : спец. 12.00.01 / Ю.В. Павлова. — Владимир, 2004. — 173 с.
121. Пазенюк В.С. Гуманістичний принцип сучасної філософії освіти / В.С. Пазенюк // Філософія освіти. — 2005. — № 1. — С. 53–73.
122. Панарин А.С. Глобальное информационное общество: вызовы и ответы / А.С. Панарин // Глобальная информатизация и безопасность России / [общ. ред. В.И. Дебреньков]. — М. : Изд-во Московского университета, 2001. — 398 с.].
123. Парламент ухвалив два закони щодо доступу до відкритих даних http://www.telekritika.ua/pravo/2015-04-09/105929].
124. Петрик В. Щодо визначення кібербезпеки та її різновидів / В. Петрик // Форми та методи забезпечення кібер-

безпеки держави : зб. матер. міжнар. наук.-практ. конф. (м. Київ, 13 березня 2008 р.). — К. : Видавець Захаренко В.О., 2008. — 216 с.

125. Петрик В.М. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: Навч. посіб. / В.М. Петрик, А.О. Штоквиш, В.І. Полевий та ін. — К. : Росава, 2006. — 208 с.

126. Питання концепції реформування інформаційного законодавства України / Р. Калюжний, В. Гавловський, В. Цимбалюк, М. Гуцалюк // Збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». К. : НТУУ «КПІ», Міносвіти і науки України, СБУ. — К. — 2000. — С. 17–21.

127. Політологія : підручник / І.С. Дзюбко, К.М. Левківський, В.П. Андрущенко та інші ; за заг. ред. І.С. Дзюбка, К.М. Левківського. — 2-е вид., випр. і допов. — К. : Вища школа, 2001. — 415 с.

128. Поліція Німеччини : головне не презумпція правоти поліції а довіра до неї. Антикор — национальный антикоррупционный портал. URL : https : //antikor.com.ua/articles/126586-politsija_nimechchini_golovne_-_neprezumptsija_pravoti_politsiji a dovira do neji. (дата звернення: 21.03.2018).

129. Положення про Спеціалізовані експертні ради при Міністерстві інформаційної політики України. Електронний ресурс — Режим доступу : http://mip.gov.ua/cr/documents/14.html.

130. Попеляр А.В., Ольшевська О.В. Кібербезпека. http://intkonf.org/popelyar-av-olshevska-ov-informatsiyna-bezpeka

131. Постанова Кабінету Міністрів України «Про питання діяльності Міністерства інформаційної політики

України» від 14 січня 2015 р. № 2 // Офіційний Вісник України. — 2015 р., № 6, стор. 36, стаття 124, код акту 75443/2015.
132. Почепцов Г.Г. Национальная безопасность стран переходного периода. — К, 1996. — 136 с.
133. Правове забезпечення інформаційної діяльності в Україні / за заг. ред. Ю.С. Шемшученка, І.С. Чижа. — К. : ТОВ «Юридична думка», 2006. — 384 с.
134. Про авторське право і суміжні права: Закон України від 23.12.1993 р. № 3792-XII // Відомості Верховної Ради України. — 1994. — № 13 від 29.03.1994. — Ст. 64.
135. Про доступ до інформації, що перебуває в розпорядженні державних органів : Рек. № Я (81) 19.
136. Про доступ до офіційних документів : Рек. Rec (2002) 2 Ком. міністрів Ради Європи від 21.02.2002р. // Бюл. Бюро інформації Ради Європи в України 10 / Редкол. : А. Дмитрук, Т. Іваненко, О. Павличко. — К. : Бюро інформації Ради Європи в України. — С. 86.
137. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : Постанова Кабінету Міністрів України № 266 від 29.04.2015 [Електронний ресурс]. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/266-2015-%D0%BF/page#n11].
138. Про затвердження Положення про Державну службу України з лікарських засобів. Президент України, Положення від 08.04.2011 №440/2011 Поточна редакція від 28.02.2013 : Електронний ресурс. — режим доступу : http: zakon2.rada.qov.ua/laws/show/440/2011.
139. Про інформацію : Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України. — 1992. — № 48. — т. 650.

140.Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 р. // Юрид. вісник України. — 1998. — № 18. — С. 8–16.
141.Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII // Відом. Верхов. Ради України. — 2015. — № 40–41. — Ст. 379.
142.Про національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98 // Відомості Верховної Ради України. — 1998 / — № 27–28. — Ст. 181.
143.Про основи національної безпеки України: Закон України від 19 черв. 2003 р. № 964-IV // Відом. Верховної Ради України. — 2003. — № 39. — Ст. 351.
144.Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січ. 2007 р. № 537-V // Відом. Верховної Ради України. — 2007. — № 12. — Ст. 102.
145.Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 року, № 287/2015. Офіційний вісник України від 09.06.2015. — 2015. — № 43. — Ст. 1353.
146.Проект Національної стратегії у сфері прав людини станом на 25 березня 2015 року (українською мовою) [Електронний ресурс]. — Режим доступу : http://old.minjust.gov.ua/file/44709].
147.Пундей Сар Дж. Боротьба з корупцією. Критичний огляд з аналізом міжнародного досвіду // Матеріалі українсько-американського семінару «Проблеми економічного зростання: питання доброчесності». — Львів, 1997, С. 17.
148.Ревнюк Н.І. Формування національної самосвідомості майбутніх учителів засобами педагогічного краєзнавс-

тва // Теоретико-методичні проблеми виховання дітей та учнівської молоді. Збірник наукових праць. — Вип. 14. Книга 2. — Кам'янець-Подільський : Видавець Зволейко Д.Г., 2010. — С. 492–500.
149. Ровинская, Т.Л. Информационная глобализация: вызов культурной самобытности европейских государств / Т.Л. Ровинская // Государство в эпоху глобализации: экономика, политика, безопасность / [отв. ред. Ф. Г. Войтоловский и А. В. Кузнецов]. — М. : ИМЭМО РАН, 2008. — Вып. 3 : Мировое развитие. — 219 с.
150. Романюк Б.В. У боротьбі з організованою злочинністю та корупцією важливі конкретні дії // Боротьба з організованою злочинністю і корупцією (теорія і практика). — К. : 2004. — № 9. — С. 517.
151. Роскошний А.П. Концептуальні проблеми модернізації вищої освіти. Матеріали міжнародної наукової конференції. — Донецьк, 1998. — 154 с.
152. Рубцов В.П. Освіта, як фактор сталого розвитку територіальних громад. Європейський контекст // Освіта, як фактор національної безпеки. Матеріали Всеукраїнської науково-практичної конференції 20 грудня 2002 р. — К, 2003. — С. 25–29.
153. Серов Л. О роли дезинформации в современных конфликтах и войнах / Л. Серов // Зарубежное военное обозрение. — 2001. — № 7. — С. 29–33.
154. Симонов, П.В. Созидающий мозг. — М. : Наука, 1993. — 109 с.
155. Скулиш Є. Антикорупційна політика держави та її вплив на розвиток суспільства // Вісник Національної академії прокуратури України. — 2. — 2011. — С. 22–28.
156. Советский энциклопедический словарь. — М. : Сов. Энциклопедия, 1989. — 1263 с.

157. Социологический энциклопедический словарь. На русском, английском, немецком, французском и чешском языках. Редактор-координатор. — академик РАН Г. В. Осипов. — М. : Издательство НОРМА (Издательская группа НОРМА — ИНФРА — М), 2000. — 140 с.
158. Становлення і розвиток української державності : [зб. наук. пр.] / МАУП. — К. : ДП «Видавничий дім «Персонал», 2015. — 284 с.
159. Степко О.М. Аналіз головних складових кібербезпеки держави / О.М. Степко // Інститут міжнародних відносин Національного авіаційного університету. — 2011. [Електронний ресурс]. — Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/Nvimvnau/2011_1/83-92.pdf].
160. Стець розповів, для чого потрібне Міністерство інформаційної політики. [Електронний ресурс] : Режим доступу: http://espreso.tv/news/2014/12/01/stec_rozpoviv__dlya_choho_potribne_ministerstvo_informaciynoyi_polityky
161. Стратегії розвитку України : теорія і практика / За ред. О.С. Власюка. — К. : ЮС, 2002. — 864 с.
162. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / А.А. Стрельцов ; [ред. В.А. Садовничий, В.П. Шерстюк]. — М. : МЦМНО, 2002. — 296 с.
163. Сухарев Е.Е. Авторское право в издательском бизнесе и СМИ. Практическое пособие / М.А. Невская, Е.Е. Сухарев, Е.Н. Тарасова. — М. : Изд-во Дашков и К., 2009. — 300 с.
164. Тацишин І. Адміністративно-правове закріплення безпеки інформаційних відносин у галузі реклами / І. Тацишин // Вісник Львівського університету. Серія юридична / М-во освіти і науки України, Львів. нац. ун-т

ім. І. Франка ; [редкол. : В.Т. Нор (відп. ред.) та ін.]. — Л., 2008. — Вип. 46. — С. 88–91.

165. Тацій В. Шлях «спроб та помилок» надто дорого обходиться суспільству / В. Тацій // Віче. — 2005. — № 9. — С. 58–65.

166. Тимченко Л.Д. Международное право : ученик / Л.Д. Тимченко. — Х. : Консум, 1999. — 528 с.

167. 169. Тихомиров О. О. Класифікації забезпечення кібербезпеки // Вісник Запорізького національного університету : зб. наук. праць. Юридичні науки. Запоріжжя: Запорізький національний університет. — 2011. — № 1. — С. 164–166.

168. Тихомиров О.О. Забезпечення кібербезпеки як функція держави : дис ... канд. юрид.н. спец. 12.00.01 / О.О. Тихомиров ; Нац. акад. внутр. справ. — К., 2011. — 233 с.

169. Третьякова В.Г. Правове регулювання біоетичних проблем у контексті застосування міжнародних та європейських стандартів. — К. : Парламентське вид-во, 2007. — 304 с.

170. Трофименко В. Некоторые аспекты авторского и смежных прав в рекламной деятельности / В. Трофименко // Юридичний радник. — 2005. — № 6 (8). — С. 44–47.

171. Ульянова Г.О. Форми захисту авторських прав / Г.О. Ульянова // Південноукраїнський правничий часопис. — 2008. — № 2 — С. 169–170.

172. Харченко Л.С. Кібербезпека України : Глосарій / Л. С. Харченко, В. А. Ліпкан, О. В. Логінов; за заг. ред. Р. А. Калюжного. — К. : Текст, 2004. — 136 с.].

173. Химическая энциклопедия. Гл. Ред. И.Л. Кнуянц. Изд. «Советская энциклопедия». — Т. 1. — М. — 1988. — 623 с.

174.Хорнби А.С. Толковый словарь современного английского языка для продвинутого этапа: Специальное издание для СРСР. — М. : Изд-во «Русский язык», 1982. — Т. 2. — 528 с.
175.Хорошенюк О. Протидія корупційним проявам у системі публічної служби України : становлення нормативно-правової бази. — С. 199–209.
176.Хотенець П.В., Невзоров І.Л. Правові та організаційні аспекти діяльності кримінальної поліції ФРН // Боротьба з організованою злочинністю і корупцією (теорія і практика). К. , 2014. — № 2 (33). — С. 145–149.
177.Цимбалюк В.С. Інформаційне право (основи теорії і практики) / В.С. Цимбалюк. Монографія. — К. : «Освіта України», 2010. — 388 с.
178.Цимбалюк В.С. Сутність кібербезпеки в умовах входження України до глобальної кіберцивілізації / В. Цимбалюк // Науковий вісник академії ДПС України. — 2007. — № 4. — С. 174–178.
179.Чубенко І. Зарубіжний досвід боротьби з корупцією в органах виконавчої влади [Електронний ресурс] / І. Чубенко. — Режим доступу : http://wvvw.dgpn.Iviv.ua'ind ex.php?option=com content&task=vievv&id=363&It emid=32.
180.Шатрава С.О. Корупційні ризики в діяльності органів внутрішніх справ: сутність та зміст // Науковий вісник Ужгородського національного університету: Серія Право. Вип. 21. Ч. II. Том 2. С. 268–270.
181.Шиллер Г. Манипуляторы сознанием / Пер. с англ. ; Науч. ред. Я.Н. Засурский. — М. : Мысль, 1980. — 326 с.
182.Шпак Н.О. Переваги використання інформаційно-комунікаційних технологій в Україні / Н.О. Шпак, О.І. Вегнер // Вісник Національного університету «Львівської

політехніки». Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку. — 2012. — № 727. — С. 461–467.
183. Шутов, Р. Глиняний фундамент кібербезпеки — [Електронний ресурс] — Режим доступу : http://osvita.mediasapiens.ua/media_law/law/koli_sosud_napivporozhniy_scho_robiti_z_kontseptsieyu_informatsiynoi_bezpeki/.
184. Щорічник Комісії міжнародного права ООН. 1973. — Т. 2. — С. 201.
185. Юридична відповідальність за корупційні діяння (структурно-логічні схеми) : навч. посіб. / авт.-упоряд. : Р.Ф. Черниш, І.М. Осауленко. Житомир : Полісся, 2017. — 264 с.
186. Яцків І.І. Адміністративно-правові засади протидії корупції в Україні : дис. ... канд. юрид. наук : 12.00.07. К 2011. — 240 с.

Навчальне видання

Ю.П. ЛІСОВСЬКА

КІБЕРБЕЗПЕКА: РИЗИКИ ТА ЗАХОДИ

Навчальний посібник

Керівник видавничих проектів: Ястребов А.О.
Друкується в авторській редакції
Дизайн обкладинки: Тишківська Н.М.
Комп'ютерна верстка: Тишківська Н.М.

Підписано до друку 14.11.2018 р.
Формат 60×84 1/16. Папір офсетний.
Гарнітура Palatino Linotype.
Умовн. друк. аркушів — 15,81.
Обл.-вид. аркушів — 10,40.
Тираж 300 прим.

ТОВ «Видавничий дім «КОНДОР»
Свідоцтво серія ДК № 5352 від 23.05.2017 р.
03067, м. Київ, вул. Гарматна, 29/31
тел./факс (044) 408-76-17, 408-76-25
www.condor-books.com.ua

Лісовська Юлія Петрівна

Народилась 8 березня 1990 року на Черкащині.
Кандидат юридичних наук, доцент.
Має понад 50 наукових праць.
Коло науково-суспільної діяльності — адміністративне право та кібербезпека.

КОНДОР