6. Казанджі А.В. Сутність дефініцій «управління», «менеджмент», «керівництво» та діалектика їх зв'язку. Вісник Хмельницького національного університету. 2016, № 1, С. 254 – 259.

7. Квартальное В.А. Туризм. М.: Финансы и статистика, 2002. 320 с.

8. Кравченко В.О. Менеджмент: навч. посібн. Одеса: Атлант, 2013. 165 с.

9. Кучеренко В.С. Особливості та сучасні тенденції управління туристичною сферою. URL: http://jrnl.nau.edu.ua/index.php/IMV/article/download/2970/2928.

10. Ліпєц Ю.В. Впровадження стратегічного менеджменту на підприємствах України як прогресивного напрямку їх розвитку. URL: http://ipdo.kiev.ua/files/articles/but4.pdf.

11. Миронов Ю.Б., Свидрук І.І. Туризм як чинник економічного розвитку країни. Науковий вісник НЛТУ України. 2016. Вип. 26.6. С. 255-262.

12. Приживара С. Управління як специфічний вид діяльності. Державне будівництво. 2012. № 1. URL: http://www.kbuapa.kharkov.ua/e-book/db/2012-1/doc/1/07.pdf.

13. Пуценгейло П.Р. Економіка і організація туристично-готельного підприємництва. К.: Центр навч. літ-ри, 2007. 344 с.

14. Рульєв В.А. Менеджмент. К.: Центр учбової літератури, 2011. 312 с.

15. Сухарський В.С. Менеджмент: навч. посібник. Тернопіль: Астон, 2001. 340 с.

16. Шатун В.Т. Основи менеджменту: навч. посібн. Миколаїв: Вид-во МДГУ ім. Петра Могили, 2006. 376 с.

17. Шевченко В.С. Менеджмент та адміністрування (Менеджмент). Харків. нац. ун-т міськ. госп-ва ім. О.М. Бекетова. Харків: ХНУМГ ім. О.М. Бекетова, 2016. 104 с.

18. Gaworecki W.W. Turystyka. Warszawa: Polskie Wydawnictwo Ekonomiczne, 2000. 385 s.

**НАШИНЕЦЬ-НАУМОВА А. Ю.,**
доктор юридичних наук, доцент,
заступник декана з науково-методичної
та навчальної роботи
факультету права та міжнародних
відносин
*(Київський університет імені Бориса
Грінченка)*

**УДК 341:[001.102:351.86]**

## ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: МІЖНАРОДНИЙ ДОСВІД І МОЖЛИВІСТЬ ВИКОРИСТАННЯ

У статті представлені результати систематизації міжнародно-правових норм у сфері інформаційної безпеки та їх співвіднесення з міжнародними стандартами, дані щодо міжнародного досвіду у сфері інформаційної безпеки на основі застосування міжнародних стандартів інформаційної безпеки. Показана важливість використання досвіду застосування сучасних інформаційно-аналітичних систем для практичної реалізації процесів інформаційного забезпечення.

***Ключові слова:*** *інформаційна безпека, міжнародний досвід, забезпечення інформаційної безпеки.*

В статье представлены результаты систематизации международно-правовых норм в сфере информационной безопасности и их соотнесение с международными стандартами, данные по международному опыту в сфере информационной безопасности на основе применения международных стандартов информационной безопасности. Показана важность использования опыта применения современных информационно-аналитических систем для практической реализации процессов информационного обеспечения.

***Ключевые слова:*** *информационная безопасность, международный опыт, обеспечение информационной безопасности.*

The article presents the results of systematization of international legal norms in the field of information security and their correlation with international standards, data on international experience of law enforcement practice in the field of information security on the basis of the application of international standards of information security. It is shown the importance of using this experience of applying modern information and analytical systems for the practical implementation of information support processes.

***Key words:*** *information security, international experience, information security.*

**Вступ.** Підсилювачем здібностей людини завжди виступала техніка, яка використовувалася не тільки на благо, але і на шкоду особі, суспільству і державі. Єдність і боротьба протилежностей двох культур особливо посилюється під час переходу людства від епохи підсилювачів фізичних здібностей людини в енергетичній сфері до епохи підсилювачів розумових здібностей в інформаційній сфері. Такими підсилювачами, як відомо, є засоби обчислювальної техніки і зв'язку, які суттєво змінюють просторово-тимчасові характеристики суспільних відносин і породжують нові, раніше невідомі види девіантних відносин. Панівною соціальною групою в суспільстві стають власники інформації та ноу-хау технологій, суспільство трансформується з постіндустріального в інформаційне. Змінюється геополітичне інформаційне протиборство держав, яке все частіше набуває форми планомірних інформаційних операцій під прикриттям принципу свободи інформації.

Теоретичні питання забезпечення інформаційної безпеки досліджені недостатньо. Визначення напрямків правового забезпечення інформаційної безпеки вимагає системного підходу і правових оцінок з урахуванням аналізу особливостей інформаційних відносин, пов'язаних із забезпеченням інформаційної безпеки, впливом на них процесів глобалізації. Багатогранність інформаційних відносин і необхідність їх врегулювання вимагають розробки кодифікованого законодавчого акта, а також проекту основ забезпечення інформаційної безпеки [1, с. 98].

Україна активно бере участь у процесі формування інформаційного суспільства не тільки на національному рівні, а й у рамках міжнародних процесів, початок яким поклала Всесвітня зустріч на вищому рівні з питань інформаційного суспільства в грудні 2003 р. в Женеві та в листопаді 2005 р. в Тунісі. Основними принципами побудови інформаційного суспільства, які є визначальним вектором у цій діяльності, невипадково визначено зміцнення довіри і безпеки під час використання інформаційно-телекомунікаційних технологій і верховенство права. Основними напрямами міжнародного співтовариства у сфері розвитку інформаційного суспільства залишається дотримання рішень Окінавської хартії глобального інформаційного суспільства 2000 р. Знаковими з цієї позиції є слова Президента України Петра Порошенка під час Заходу високого рівня щодо діяльності ООН із підтримки миру у Нью-Йорку: «Зараз очевидно, що світ не став безпечнішим у XXI столітті. Ми все ще спостерігаємо війни та агресії» [2]. Важливою складовою частиною безпеки в сучасному світі є інформаційна безпека, яка визначає актуальність вдосконалення правового регулювання у сфері протидії новим викликам і загрозам національній безпеці [3, с. 53].

Сьогодні ми відчуваємо, що наявна в Україні законодавча база не повністю відображає потреби забезпечення інформаційної безпеки. Системна робота у сфері правового забезпечення інформаційної безпеки потребує наукового обґрунтування подальшої розробки таких нормативних актів, у яких би повною мірою були враховані міжнародні принципи і норми, спрямовані на зміцнення міжнародної інформаційної безпеки, та максимально враховувалися б національні інтереси.

**Постановка завдання.** Метою статті є узагальнення міжнародного досвіду правового регулювання інформаційної безпеки й обґрунтування концептуальних положень щодо системи правового регулювання у сфері забезпечення інформаційної безпеки України.

Необхідно зазначити, що у цьому напрямі здійснювалися наукові розвідки таких вчених, як: Б.В. Авер'янов, А.І. Арістова, О.А. Баранов, К.І. Беляков, В.М. Брижко, П.В. Діхтієвський, Р.А. Калюжний, В.К. Колпаков, Б.А. Кормич, В.І. Курило, В.А. Ліпкан, А.І. Марущак, А.М. Новицький, Н.Р. Нижник, В.Ф. Опришко, В.Г. Пилипчук, М.Я. Швець, В.А. Шамрай, В.К. Шкарупа, В.С. Цимбалюк та ін.

Для досягнення поставленої мети нам потрібно систематизувати міжнародні норми правового регулювання інформаційної безпеки та співвіднести їх із міжнародними стандартами у цій сфері.

**Результати дослідження.** Темпи розвитку сучасних інформаційних технологій значно випереджають темпи розробки рекомендаційної та нормативно-правової бази керівних документів, що діють на території України. Тому питання аудиту «як оцінити рівень інформаційної безпеки» обов'язково тягне за собою наступне: за якими критеріями робити оцінку ефективності захисту інформації? Внаслідок цього на додаток до вимог, рекомендацій і керівних документів доводиться застосовувати методики міжнародних стандартів (ICO 17799, 9001, 15408, стандартів Британського інституту стандартів та ін.), а також використовувати методи кількісного аналізу ризиків у сукупності з оцінками економічної ефективності інвестицій в забезпеченні безпеки і захисту інформації. У зарубіжних нормативних документах встановлено набір вимог для різних типів інформаційних засобів і систем залежно від умов їх застосування. Особливості розвитку вітчизняної нормативної бази у цій сфері полягають у тому, що відсутній комплексний підхід до проблеми захисту інформації (розглядаються переважно питання несанкціонованого доступу до інформації та питання забезпечення захисту від побічних електромагнітних випромінювань і наведень) і, крім того, розроблені національні стандарти та керівні документи не брали до уваги міжнародні стандарти ISO / IEC. Нині ці недоліки почали усуватися. З метою вдосконалення вітчизняної нормативної бази спільно з іншими зацікавленими міністерствами і відомствами реалізуються нові ініціативи в цьому напрямі.

Із використанням міжнародного правового регулювання інформаційної безпеки пов'язані такі проблеми, як [4]:

– необхідність працювати з інформацією різного типу (структурованою і неструктурованою інформацією);

– різні підходи до джерел і форматів даних (телебачення, радіо, друковані видання, Інтернет, бази даних та ін.);

– великі обсяги даних;

– необхідність гнучко й оперативно налаштовувати систему на різні завдання відповідно до мінливих обставин;

– необхідність синхронізації потужностей системи;

– необхідність ефективно аналізувати бази даних;

– необхідність прогнозування розвитку ситуацій;

– необхідність моніторингу відкритого інформаційного простору (Інтернет / ЗМІ);

– необхідність застосовувати максимально стандартизовані рішення.

Рішення перерахованих проблем вимагає застосування сучасних аналітичних систем для якісного забезпечення використання міжнародного досвіду правового забезпечення інформаційної безпеки [5, с. 25]. На цій основі видається можливим створення і використання

єдиного міжнародного правового простору, який, на нашу думку, уможливить ефективне використання міжнародного досвіду нормативно-правового регулювання процесів забезпечення інформаційної безпеки в нашій країні. Основні процеси сьогоднішнього етапу державного будівництва України в сфері інформаційної безпеки вимагають від структур, які забезпечують прийняття органами державної влади обґрунтованих рішень, постійного вдосконалення ефективності роботи на таких напрямках діяльності, як:

– безперервний моніторинг і зважена аналітична оцінка глобальних напрямків зміцнення безпеки України;

– інтегроване ситуаційне моделювання проблем безпеки;

– ранжирування варіантів (способів і засобів) рішення проблем безпеки.

Перелічені напрямки діяльності характеризуються: колективністю, інтелектуальністю, інтерактивністю, унікальністю.

Широкий спектр проблем забезпечення інформаційної безпеки особистості, суспільства і держави, розвитку культури кібербезпеки, забезпечення недоторканності приватного життя і захисту прав на доступ до інформації, захисту інформаційних систем, ресурсів і мереж, розширення застосування інформаційних технологій у державному управлінні і під час надання державних послуг, а також інші проблеми інформаційної безпеки потребують системного правового регулювання на основі ретельного аналізу міжнародних правових норм, зарубіжного законодавства, чинного законодавства України і правозастосовчої практики. Правові підходи до визначення інформаційного суспільства поки обмежувалися перерахуванням його ознак і завдань. Однак нині зміни в цій сфері відбуваються стрімко і вимагають неослабної, постійної уваги до зазначених вище питань, визначення нових пріоритетів та завдань і є каталізатором для продовження досліджень у цій галузі. У процесі становлення інформаційного суспільства в умовах глобалізації, нових викликів і загроз порушення сталого функціонування інформаційної інфраструктури потребують уточнення напрями розвитку національного законодавства, відбуваються зміни і на міжнародній арені, що вимагають адекватного правового регулювання. Це очевидно на прикладі розвитку Інтернету і використання його в протиправних цілях.

Аналіз міжнародних актів показує, що починаючи з 2000 р. прийняті такі найважливіші акти, як Окінавська хартія глобального інформаційного суспільства, підсумкові документи Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства в грудні 2003 р. в Женеві та в листопаді 2005 р. в Тунісі, спрямовані на прискорення формування постіндустріальних тенденцій в економічній, соціально-політичній і духовній сферах життя суспільства. Декларація принципів із питань інформаційного суспільства, прийнята в Женеві в 2003 р., проголосила побудову інформаційного суспільства глобальним завданням у новому тисячолітті і визначила принцип забезпечення підвищення довіри і безпеки під час використання інформаційних технологій одним із ключових [6, с. 125].

Для побудови інформаційного суспільства важливе значення мають розвиток інфраструктури, створення людського потенціалу, інформаційна безпека у дотриманні принципу верховенства права, протидія новим викликам і загрозам. Просування ініціатив у сфері міжнародної інформаційної безпеки має позитивний характер і в рамках Міжнародного Центру наукової та технічної інформації (далі – МЦНТІ). Про це свідчить Заява глав держав-членів МЦНТІ щодо проектів національних і міжнародних ініціатив у сфері розвитку системи наукової та технічної інформації, а також безпеки та захисту цієї інформації від 19 вересня 2018 р. в місті Мінськ (Республіка Білорусь) під час проведення 69-го засідання Комітету представників. Проблеми правового регулювання в цій галузі викликають заклопотаність у всіх держав-учасників цього Центру у зв'язку з глобалізацією викликів і загроз. Питання встановлення відповідальності за зміст інтернет-сайтів та інтернаціоналізації управління Інтернетом також мають міжнародний характер, потребують додаткового вивчення для вироблення взаємоузгоджених пропозицій і їх реалізації. На основі вивчення міжнародно-правових актів, що стосуються протидії новим викликам і загрозам в інформаційній сфері, а також впливу глобалізації на визначення національної стратегії розвитку інформаційного

суспільства, обґрунтовується висновок про необхідність подальшої імплементації положень міжнародних правових актів, що стосуються, зокрема, забезпечення доступу до публічної і судової інформації, боротьби з корупцією, тероризмом і екстремізмом, кіберзлочинністю і гармонізації законодавства держав.

Водночас слід відзначити позитивний досвід міжнародної співпраці на прикладі проведення Форуму інформаційної безпеки «Age of Security Forum», присвяченого міжнародним аспектам інформаційної безпеки, в Резолюції якого визначена роль забезпечення інформаційної безпеки як ключового елемента національної безпеки у становленні глобального інформаційного суспільства. Транснаціональність загроз і рівень шкоди у їх реалізації змушують ставити проблему забезпечення інформаційної безпеки як глобальну, що вимагає зусиль всього світового співтовариства. За даними організації «Ukrainian Information Security Center», близько 100 держав нині мають окремі закони про право на інформацію в складі національного законодавства.

Дослідження зарубіжного законодавства показує, що особливо важливим є облік у національному законодавстві принципів, закріплених у міжнародних правових актах (таких як Резолюція 2450 (XXIII) від 12 грудня 1968 р. Генеральної Асамблеї ООН): принципу свободи обміну інформацією, принципів і процедур інформування громадськості про діяльність державних структур, а також принципу контролю держав над комунікаційною діяльністю, здійснюваною під їх юрисдикцією, регламентації порядку діяльності та здійснення контролю за комунікаціями, включаючи комплексну розробку державної політики в цій сфері. За останні 20 років закони про доступ громадян до інформації прийняті у Франції, Греції, Данії, Голландії, Бельгії, Португалії, Іспанії, Фінляндії та Італії. Для зарубіжних країн із різними правовими традиціями характерний підхід до проблеми інформаційної безпеки з урахуванням таких загальних понять, як «автентичність», «доступність», «цілісність», «конфіденційність» [7, с. 69].

У ряді країн Європи (Нідерландах, Іспанії, Португалії, Австрії, Угорщині, Естонії, Бельгії та Румунії) право громадян на доступ до офіційної інформації закріплено конституційно. У Франції, Греції та Італії це право закріплено законодавчо. Удосконалення законодавства в названій сфері активно йде у Великій Британії, Німеччині, Естонії, Молдові, Польщі та ряді інших країн. Положення про недоторканність приватного життя, про захист персональних даних містяться в різних законодавчих актах, особливо в законах, що регламентують ведення медичних записів, зберігання інформації про споживчі кредити та ін. Нині в багатьох державах розробляються і реалізуються концепції «електронного уряду», що ґрунтуються на створенні державних інформаційних ресурсів і на доступі до інформації про діяльність державних органів влади. Лідерами серед таких країн є США, Сінгапур, Австралія, Нова Зеландія. Правове регулювання інформаційної безпеки є найбільш ефективним, коли сформовані правові основи інформаційного суспільства, а інформаційна безпека в силу глобального характеру мереж зв'язку може бути забезпечена лише за умови міжнародної взаємодії. Удосконалення механізмів правового регулювання суспільних відносин, що виникають у сфері забезпечення інформаційної безпеки, повинно стати одним із пріоритетних напрямів державної політики у цій сфері. Розвиток законодавства в галузі забезпечення інформаційної безпеки України має базуватися на дотриманні не тільки загальних принципів (законності, справедливості, юридичної рівності громадян, гуманізму, демократизму, єдності прав і обов'язків), міжгалузевих (невідворотності відповідальності), але і таких принципів правового забезпечення інформаційної безпеки, як єдність інформаційного простору, дотримання балансу інтересів особистості, суспільства і держави та їх взаємної відповідальності, інтеграції в рамках системи міжнародної інформаційної безпеки [8, с. 21].

Отже, правове забезпечення інформаційної безпеки – це невід'ємна і найважливіша складова частина забезпечення системи національної безпеки; проблема створення або вдосконалення сучасної системи інформаційної безпеки на національному рівні – це насамперед прерогатива держави та її інститутів. І тому на національному та міжнародному рівнях у цьому складному, довготривалому, дуже витратному і делікатному процесі, яким є

забезпечення інформаційної безпеки, повинні брати участь відповідні органи виконавчої влади та провідні наукові інститути.

**Висновки.** Провідні держави в сучасних міжнародних відносинах використовують інформацію як стратегічний ресурс для реалізації своїх геополітичних завдань. Тому інформаційна безпека сьогодні є одним із пріоритетних напрямів зовнішньої політики. Могутність країни на зовнішньополітичній арені визначається її можливостями впливати на міжнародне інформаційне поле, а отже, і на інформаційне середовище інших держав.

Таким чином, для успішного розвитку нашої держави в XXI ст. було б доцільно:

1. Удосконалити систему інформаційної безпеки.
2. Сформувати і реалізовувати концепцію забезпечення інформаційної безпеки, засновану на технології інформаційного управління.
3. Побудувати гармонійне інформаційне суспільство, засноване на саморегуляції.
4. Впливати на міжнародне інформаційне середовище, просуваючи і лобіюючи інтереси України в світі.
5. Удосконалювати та реалізовувати проекти інформаційно-технічного й інформаційно-психологічного забезпечення безпеки країни, виходячи з пріоритетів, цілей і завдань.

**Список використаних джерел:**

1. Нашинець-Наумова А.Ю. Інформаційна безпека суб'єктів господарювання: проблеми теорії та практики правозастосування: монографія / під заг. ред. В.І. Курила. Херсон: Видавничий дім «Гельветика», 2017. 386 с.
2. Миротворча місія на Донбасі – це тест для ООН, – Порошенко. URL: https//24tv.ua/.
3. Шерстюк В.П. Проблемы обеспечения безопасности информационного общества. Стратегічна панорама. 2003. № 2. С. 52–53.
4. Сучасні методики розробки політик безпеки. URL: https://infopedia.su/7xba99.html.
5. Крылов Г.О. Международные проблемы информационного права: учеб. пособ. М.: РПА Минюста России, 2013. 122 с.
6. Полякова Т.А. Информационная безопасность в условиях построения информационного общества. М.: РПА Минюста России, 2007. 165 с.
7. Павлов И.Ю. Доступ к информации: Государственная тайна и права человека. Экология и право. 2004. № 15. С. 68–72.
8. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий: учеб. пособ. М.: МИФИ, 1995. 96 с.