Адміністративне право і процес; фінансове право; інформаційне право
УДК 34.096+321.01

Скриньковський Руслан Миколайович
кандидат економічних наук, доцент,
професор кафедри економіки підприємств та інформаційних технологій
Львівський університет бізнесу та права
Скрыньковский Руслан Николаевич
кандидат экономических наук, доцент,
профессор кафедры экономики предприятий и информационных технологий
Львовский университет бизнеса и права
Skrynkovskyy Ruslan
PhD (Economics), Associate Professor,
Professor of the Department of Business Economy and Information Technology
Lviv University of Business and Law
ORCID: 0000-0002-2180-8055

Малашко Олександр Євгенійович
викладач кафедри адміністративного права та процесу,
фінансового і інформаційного права
Львівський університет бізнесу та права
Малашко Александр Евгеньевич
преподаватель кафедры административного права и процесса,
финансового и информационного права
Львовский университет бизнеса и права
Malashko Oleksandr
Lecturer of the Department of Administrative Law and Process,
Financial and Information Law
Lviv University of Business and Law
ORCID: 0000-0001-8676-5837

СТРУКТУРНО-КЛАСИФІКАЦІЙНА ХАРАКТЕРИСТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
СТРУКТУРНО-КЛАССИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
STRUCTURAL AND CLASSIFICATION CHARACTERISTICS OF PROVIDING INFORMATION SECURITY

Анотація. *У статті розкрито основні аспекти структурно-класифікаційної характеристики забезпечення інформаційної безпеки. В контексті розкриття мети наукового дослідження опрацьовано ряд джерел, окремі статті Конституції України, Указ Президента України "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України", деякі статті Закону України "Про концепцію Національної програми інформатизації", Закону України "Про інформацію", Закону України "Про державну таємницю" та Закону України "Про доступ до публічної інформації". Визначено, що інформаційна безпека являє собою стан та рівень захищеності інформаційної сфери та проявляється за результатами формування, використання та розвитку інтересів як громадян, так і суспільства, у тому числі держави, загалом. Встановлено, що інформаційна безпека носить міждисциплінарний характер, а саме охоплює правові, технічні, технологічні, психологічні основи та зумовлює неабияку складність і багаторівневість взаємозв'язків між складовими елементами забезпечення інформаційної безпеки. Доведено, що застосування підходів до класифікації забезпечення інформаційної безпеки, які використовуються у науковій статті, виступає одним із способів здійснення структурного аналізу процесу забезпечення інформаційної безпеки, при цьому не порушуючи взаємозв'язків між його складовими. Визначено, що ключові ознаки кожної із складових процесу забезпечення*

дозволяють у перспективі комплексно провести процес забезпечення інформаційної безпеки та сформувати тактичні і стратегічні напрямки такої діяльності. З'ясовано, що розгляд та врахування всіх основних питань комплексного забезпечення інформаційної безпеки дозволяє гармонізувати українське законодавство у інформаційній сфері, а це у перспективі сприятиме формуванню ефективної державної політики у інформаційній сфері.

Ключові слова: *інформаційна безпека, забезпечення інформаційної безпеки, державна інформаційна політика, захист інформації.*

Аннотация. *В статье раскрыты основные аспекты структурно-классификационной характеристики обеспечения информационной безопасности. В контексте раскрытия цели научного исследования обработаны ряд источников, отдельные статьи Конституции Украины, Указ Президента Украины "О решении Совета национальной безопасности и обороны Украины от 29 декабря 2016 года "О Доктрине информационной безопасности Украины", некоторые статьи Закона Украины "О концепции Национальной программы информатизации", Закона Украины "Об информации", Закона Украины "О государственной тайне" и Закона Украины "О доступе к публичной информации". Определено, что информационная безопасность представляет собой состояние и уровень защищенности информационной сферы и проявляется по результатам формирования, использования и развития интересов как граждан, так и общества, в том числе государства, в целом. Установлено, что информационная безопасность носит междисциплинарный характер, а именно охватывает правовые, технические, технологические, психологические основы и обуславливает большую сложность и многоуровневость взаимосвязей между составляющими элементами обеспечения информационной безопасности.*

Доказано, что применение подходов к классификации обеспечения информационной безопасности, используемых в научной статье, выступает одним из способов осуществления структурного анализа процесса обеспечения информационной безопасности, при этом не нарушая взаимосвязей между его составляющими. Определено, что ключевые признаки каждой из составляющих процесса обеспечения позволяют в перспективе комплексно провести процесс обеспечения информационной безопасности и сформировать тактические и стратегические направления такой деятельности. Установлено, что рассмотрение и отражение всех основных вопросов комплексного обеспечения информационной безопасности позволяет гармонизировать украинское законодательство в информационной сфере, а это в перспективе будет способствовать формированию эффективной государственной политики в информационной сфере.

Ключевые слова: *информационная безопасность, обеспечение информационной безопасности, государственная информационная политика, защита информации.*

Summary. *The article reveals the main aspects of the structural and classification characteristics of providing information security. In the context of revealing the purpose of scientific research processed a number of sources, separate articles of the Constitution of Ukraine, the Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Doctrine of Information Security of Ukraine", some articles of the Law of Ukraine "On the Concept of the National Informatization Program", the Law of Ukraine "On Information", the Law of Ukraine "On State Secrets" and the Law of Ukraine "On Access to Public Information". It is determined that information security is a state and level of protection of the information sphere and is manifested in the formation, use and*

development of the interests of both citizens and society, including the state as a whole. It is established that information security has an interdisciplinary nature, namely it covers the legal, technical, technological, psychological foundations and causes great complexity and multilevel relationships between the components of information security. It is proved that the application of approaches to the classification of information security, which are used in the scientific article, is one of the ways to carry out a structural analysis of the process of providing information security, without violating the relationships between its components. It has been determined that the key features of each of the components of the provisioning process allow in the future to carry out the process of ensuring information security in a comprehensive manner and form the tactical and strategic directions of such activities. It was found that consideration and reflection of all the main issues of comprehensive providing information security allows to harmonize the Ukrainian legislation in the information sphere, and this in the long run will contribute to the formation of an effective state policy in the information sphere.

Key words: *information security, providing information security, state information policy, information protection.*

Постановка проблеми. У наш час важливою інтегруючою базою життєздатності суспільства виступає інформаційна сфера, водночас забезпечення безпеки у інформаційній сфері є одним із ключових концептуальних аспектів гарантування безпеки інформаційної сфери. Саме у таких умовах відбувається формування державної політики у інформаційній сфері, яка, до того ж, базується на низці проведених наукових досліджень у інформаційній сфері із нахилом на забезпечення інформаційної безпеки.

З’ясовано, що проведення наукових досліджень стосовно забезпечення інформаційної безпеки вимагає глибокого аналізу

особливостей структури забезпечення. При цьому деталізація і виокремлення складових елементів системи забезпечення інформаційної безпеки відповідно до ознак дають можливість усвідомити характерні риси кожної з ознак і дозволять у перспективі сформувати адекватні заходи державного і недержавного регулювання сфери інформаційного розвитку України, а також інтеграцію України у сферу світового інформаційного простору.

Аналіз останніх досліджень і публікацій. Наукові дослідження стосовно забезпечення безпеки у інформаційній сфері на сьогодні проводять багато вчених та науковців, зокрема – О. Д. Довгань [1], С. Д. Гусарєв [2], О. М. Когосов [3], Ю. Є. Максименко [4], О. В. Черевко [5] та інші.

Однак, виходячи із аналізу наукових праць, які представлені вищезазначеними науковцями та вченими, не до кінця вивченою та такою, що потребує нагального дослідження, залишається актуальна проблематика з розкриття структурно-класифікаційної характеристики забезпечення інформаційної безпеки.

Мета статті. Метою статті є дослідити і розкрити основні аспекти структурно-класифікаційної характеристики забезпечення інформаційної безпеки.

Виклад основного матеріалу дослідження. В контексті розкриття тематики у даному напрямі, слід першочергово представити визначення поняття “інформаційна безпека”.

Так, опираючись на інформацію, представленої у праці [1], під інформаційною безпекою слід розуміти стан та рівень захищеності середовища інформаційної сфери суспільства, який дозволяє формувати, використовувати та розвивати інтереси не тільки громадян, але і організацій.

Відповідно до статті 17 Конституції України [6], однією із визначальних функцій держави, а також важливим завданням Українського народу виступає забезпечення інформаційної безпеки в контексті забезпечення захисту суверенітету і територіальної цілісності України.

Базуючись на зазначеному вище, варто відмітити, що процес забезпечення інформаційної безпеки слід трактувати як цілеспрямовану та одну із провідних функцій держави. Опираючись на цьому, слід зазначити, що синергетична динаміка розвитку суспільства на сучасному етапі повинна відповідати теорії держави та права, а функції держави в цьому контексті повинні базуватися на напрямках та видах державної діяльності.

Термін "забезпечення" загалом тлумачиться як [7, с. 375]:

– процес надання і створення засобів та умов, якими гарантується захист;

– засоби чи система засобів захисту.

Своєю чергою, виходячи із теорії діяльності, тлумачення поняття "забезпечення" є не рівнозначним, оскільки засоби діяльності часто проявляються у вигляді змістовних елементів, які, до того ж, визначають незмінну складову цієї діяльності [2, с. 89].

Що стосується системи забезпечення інформаційної безпеки, то основними її завданнями виступають [1]:

– розроблення та впровадження на практиці планів і інших заходів стосовно захисту інтересів інформаційної сфери;

– створення та забезпечення функціонування і розвитку належних органів, засобів та сил для захисту безпеки інформаційної сфери;

– відновлення об'єктів, якими забезпечується захист інформаційної сфери.

Своєю чергою, цілі системи забезпечення інформаційної безпеки спрямовуються на виявлення, запобігання, нейтралізацію, усунення, локалізацію, відбиття та знищення інформаційних загроз [1].

Базуючись на характерних особливостях кожного із видів діяльності, варто відмітити, що засоби захисту у багатьох випадках виступають самостійними елементами, через які виражається мета, завдання і результати діяльності. При цьому організаційна діяльність держави виражається як, по-перше – процес формування потрібних засобів, через які забезпечується діяльність суб'єктів, а, по-друге – процес використання цих засобів суб'єктами, в контексті досягнення ними поставленої мети. З огляду на те, засоби слід вважати як такі, в контекст яких покладено досягнення завдань та отримання очікуваних результатів від них у ході реалізації окресленої мети.

Інформаційна безпека, виходячи із своїх особливостей, носить системний характер, оскільки характеризується як складний та сукупний процес забезпечення діяльності відповідно до поставлених вимог. Наукові дослідження довели, що на сьогодні ще не вироблено ефективного механізму, через який забезпечувалася б безпека у інформаційній сфері. Тому для виділення окремих складових цього механізму прийнято використовувати такі поняття як "механізми", "напрями", "шляхи". При цьому, суть забезпечення інформаційної безпеки виражається як комплексна діяльність, до реалізації якої повинен застосовуватися спеціальний діяльнісний підхід.

Результати дослідження доводять, що в наш час недостатньо розробленою та систематизованою виступає структура ключових елементів процесу забезпечення інформаційної безпеки. Що стосується нормативно-правового рівня регулювання забезпечення інформаційної безпеки, то напрямки регулювання цього процесу опираються на традиційні сфери життєдіяльності.

До прикладу, в основу Доктрини інформаційної безпеки України [8] покладено саме традиційний підхід до забезпечення безпеки у інформаційній сфері.

У ході представлення класифікації забезпечення безпеки інформаційної сфери варто зазначити, що кожен із критеріїв слід інтерпретувати, базуючись при цьому на спеціальних ознаках. Використання такого підходу дозволить представити багатоаспектну класифікацію процесу забезпечення інформаційної безпеки.

Базуючись на інформації, поданій у літературних джерелах [8; 9]: забезпечення інформаційної безпеки відбувається у таких сферах суспільного життя, як: економічна сфера, політична сфера, оборонна сфера, екологічна сфера, соціальна сфера та інші.

Відповідно до українського законодавства, процес забезпечення інформаційної безпеки виступає невід'ємною складовою забезпечення національної безпеки.

Що стосується розуміння інформаційної безпеки, то відповідно до інформації, поданої у праці [4, с. 57], процес забезпечення інформаційної безпеки поділяється на:

1) забезпечення інформаційно-психологічної безпеки;
2) забезпечення інформаційно-технологічної (технічної) безпеки;
3) забезпечення інформаційної безпеки у системі прав та свобод людини.

У Законі України "Про інформацію" [10] зазначено, що суть забезпечення інформаційної безпеки полягає у:

1) забезпеченні можливостей для використання інформації;
2) забезпеченні належного рівня зберігання інформації;
3) забезпеченні захисту інформації;
4) забезпеченні отримання інформації у визначеному порядку;
5) забезпеченні легітимного (законного) поширення інформації.

Базуючись на комплексності підходів до визначення забезпечення інформаційної безпеки і пов'язаних із цим проблем, слід наголосити на обов'язковому виділенні особливих видів діяльності, в які закладено інноваційні (інтелектуальні) основи результативного розвитку інформаційних систем. До прикладу, такими діяльностями виступають професійна освіта, а також проведення наукових досліджень у сфері інформаційної діяльності, як визначені положеннями статті 15 "Науково-технічна інформація" та статті 16 "Податкова інформація" Закону України "Про інформацію" [10].

Варто також зазначити, що основними етапами діяльності по протидії загрозам у інформаційній сфері виступають:

1) етап моніторингування наявних та потенційних загроз у інформаційній сфері (зокрема проводиться аналіз чинників впливу на стан інформаційної сфери та виявляються загрози);

2) етап ранжування загроз у інформаційній сфері (зокрема встановлюються пріоритетні загрози, тобто ті, нейтралізація яких є першочерговою);

3) етап профілактики та попередження виникнення загроз, а також їх негативного впливу на стан інформаційної сфери;

4) етап безпосередньої протидії загрозам.

Розглядаючи загрозу як чинник негативного впливу, варто відмітити, що усунення цієї загрози передбачається пріоритетними напрямками державної діяльності. Разом з тим, процес забезпечення інформаційної безпеки можна горизонтально структуризувати. Водночас за видами забезпечення, які формуються відповідно до основних етапів діяльності по протидії загрозам у інформаційній сфері представляється вертикальна структуризація забезпечення інформаційної безпеки.

Державне забезпечення інформаційної безпеки відповідно до змісту поділяється на:

1) процес інформування (відповідно до якого суб'єктам надається певна якісна інформація для забезпечення та підтримання на належному рівні їх функціонування і життєздатності);

2) процес інформатизації (відповідно до якого держава провадить цілеспрямовану діяльність, націлену на формування економічних, політичних, технічних і інших умов, необхідних для забезпечення інформаційного розвитку суб'єктів, оптимізації обміну інформацією, а також для розвитку державних інформаційних ресурсів);

3) процес приведення до норми поведінку суб'єктів у інформаційній сфері (зокрема передбачається правова регламентація відносин у інформаційній сфері);

4) процес боротьби із правопорушеннями, які виникають та здійснюються у інформаційній сфері.

У частих випадках державне забезпечення інформаційної безпеки визначається як комплекс державних гарантій у інформаційній сфері, які прямим чи опосередкованим чином впливають на правове регулювання процесу забезпечення інформаційної безпеки, і виступають базою розроблення нових та удосконалення існуючих нормативно-правових актів. До прикладу, це Доктрина інформаційної безпеки України [8], Закон України "Про концепцію Національної програми інформатизації" [9], Закон України "Про інформацію" [10].

У Доктрині інформаційної безпеки України [8] зазначається, що процес забезпечення інформаційної безпеки класифікується за такими ключовими ознаками, як:

1) за суб'єктами забезпечення інформаційної безпеки на:

а) міжнародне забезпечення інформаційної безпеки, яке базується на міжнародному співробітництву у сфері інформації, гарантуванні інформаційної незалежності держави, сприянні задоволенню потреб громадян у необхідній інформації);

б) державне забезпечення інформаційної безпеки, яке базується на діяльності державних органів, організацій та індивідів;

в) недержавне забезпечення інформаційної безпеки, яке базується на діяльності інститутів громадянського суспільства (у тому числі громадських організацій), та індивідів;

2) за об'єктами забезпечення інформаційної безпеки на:

а) забезпечення інформаційної безпеки держави;

б) забезпечення інформаційної безпеки суспільства;

в) забезпечення інформаційної безпеки індивіда;

3) за напрямками впливу загроз на:

а) опосередкований вплив загроз, який потрібно нейтралізувати (послабити) внаслідок підвищення інформаційного потенціалу суб'єктів, а також через сприяння їх самоорганізації;

б) безпосередній вплив загроз, який потрібно нейтралізувати (послабити) внаслідок формування сприятливих умов, необхідних для забезпечення життєдіяльності суб'єктів у інформаційній сфері;

4) за предметністю забезпечення інформаційної безпеки на:

а) трансформацію негативного впливу загроз у позитивний вплив;

б) посилення позитивних процесів у інформаційній сфері;

в) усунення (нейтралізацію) негативних процесів та/чи загроз;

5) за способами забезпечення інформаційної безпеки на:

а) контрольно-наглядову діяльність у інформаційній сфері;

б) інженерно-технічне забезпечення інформаційної сфери;

в) матеріально-технічне забезпечення інформаційної сфери;

г) правове регламентування взаємовідносин у інформаційній сфері.

Відповідно до положень Закону України "Про державну таємницю" [11] та Закону України "Про доступ до публічної інформації" [12], процес забезпечення інформаційної безпеки класифікується також за такими видами:

1) у відповідності до правового режиму інформації на:

а) процес забезпечення режиму доступу до інформації у ситуації обмеженого доступу;

б) процес забезпечення розповсюдження інформації на належному рівні;

в) процес забезпечення оптимального обміну інформацією, яка є відкритою;

2) відповідно до заходів захисту інформації (у тому числі секретної) на:

а) оперативно-розшукове забезпечення інформаційної безпеки;

б) організаційно-правове забезпечення інформаційної безпеки;

в) криптографічне забезпечення інформаційної безпеки;

г) інженерно-технічне забезпечення інформаційної безпеки.

Окрім того, О. Д. Довгань [1], вивчаючи проблематику правового забезпечення інформаційної безпеки України, виділяє такі пріоритетні напрямки процесу забезпечення як:

1) забезпечення наступальності різних способів досягнення інформаційної безпеки, виходячи із особливостей прояву загроз у інформаційній сфері;

2) формування інтегрованої системи оцінювальних індикаторів впливу загроз у інформаційній сфері, а також оперативного реагування на їх нейтралізацію чи послаблення;

3) розроблення і впровадження на практиці скоординованої інформаційної політики спеціально уповноваженим органами державної влади;

4) своєчасне реагування на інформаційні операції проти України, а також на маніпуляції із свідомістю суспільства;

5) формування, розвиток та результативне функціонування інститутів, націлених на забезпечення безпеки у інформаційній сфері України;

6) покращення підготовки спеціально уповноважених осіб у сфері інформаційної безпеки.

Разом з тим, О. Д. Довгань [1] наголошує, що система забезпечення інформаційної безпеки включає: а) суб'єктів із інформаційно-аналітичними компетенціями, які проводять аналіз інформаційних загроз; б) суб'єктів із організаційно-управлінськими компетенціями, якими приймаються рішення, а також розробляються та впроваджуються заходи із протидії загроз; в) суб'єктів, за якими закріплені виконавчі функції.

Своєю чергою, О. М. Косогов [3], в контексті аналізування сучасних методів забезпечення безпеки у інформаційній сфері, наголошує, що на сьогодні досить поширеними методами забезпечення інформаційної безпеки виступають:

1) однорівневі методи, які націлені на конкретному завданні процесу забезпечення інформаційної безпеки;

2) багаторівневі методи, які націлені на кількох завданнях процесу забезпечення інформаційної безпеки;

3) комплексні методи, які базуються на аналізі впливу загроз на інформаційну безпеку;

4) інтегровані високоінтелектуальні методи, в основу яких закладено використання багатокомпонентних технологій із використанням автоматизованих інтелектуальних засобів.

Таким чином, слід наголосити на тому, що в рамках аналізу існуючих класифікацій забезпечення інформаційної безпеки, варто також звернути увагу на класифікацію загроз у інформаційній безпеці, на усунення та послаблення впливу яких спрямовано забезпечення

інформаційної безпеки. Так, загрози у інформаційній безпеці класифікуються за такими ключовими ознаками [5]:

1) за особливостями порушення (розкриття конфіденційної інформації, протиправне втручання у діяльність інформаційних систем, виведення інформаційних систем із ладу, спотворення та знищення інформації тощо);

2) за можливими наслідками (серйозний злочин, дрібне хуліганство, незначні помилки);

3) за характером дій правопорушників (умисне втручання у процес порушення інформаційної безпеки, неумисне втручання у процес порушення інформаційної безпеки);

4) за мотивованістю здійснення порушення (зловмисне порушення, незловмисне порушення);

5) за місцем виникнення (зовнішні загрози в інформаційній безпеці, внутрішні загрози в інформаційній безпеці (здебільшого провокуються інсайдерами);

6) за кінцевим результатом (реалізовані загрози, нереалізовані загрози);

7) за об'єктивністю впливу загроз (загрози, які спрямовані на усю інформаційну систему, загрози, які спрямовані на деякі компоненти інформаційної системи);

8) за причинами виникнення (загрози, які виникають в контексті недосконалого рівня технічного захисту інформаційної безпеки, загрози, які виникають внаслідок браку організаційних мір);

9) за каналом проникнення (загрози, які виникають через слабкість програмного забезпечення, загрози, які виникають через прогалини у системі авторизації, зокрема провокують, тим самим, ряд недоліків системи зберігання документів;

10) за реалізацією загроз (загрози у вигляді впливу шкідливих програм, хакерських атак, програмних закладок, загрози, які спричиняють уразливі процедури для авторизації тощо);

11) за особливостями походження загроз (загрози через стихійні лиха, антропогенні, техногенні та природні явища);

12) загрози за характером збитку (критичні, значні, незначні).

Висновки. За результатами опрацювання літературних джерел, окремих статей Конституції України, Указу Президента України "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України", окремих статей Закону України "Про концепцію Національної програми інформатизації", Закону України "Про інформацію", Закону України "Про державну таємницю", Закону України "Про доступ до публічної інформації" [1–15] у науковій статті розкрито основні аспекти структурно-класифікаційної характеристики забезпечення інформаційної безпеки.

Встановлено, що інформаційна безпека носить міждисциплінарний характер, а саме охоплює правові, технічні, технологічні, психологічні основи та зумовлює неабияку складність і багаторівневість взаємозв'язків між складовими елементами забезпечення інформаційної безпеки. Доведено, що застосування підходів до класифікації забезпечення інформаційної безпеки, які використовуються у науковій статті, виступає одним із способів здійснення структурного аналізу процесу забезпечення інформаційної безпеки, при цьому не порушуючи взаємозв'язків між його складовими.

Визначено, що ключові ознаки кожної із складових процесу забезпечення дозволяють у перспективі комплексно провести процес забезпечення інформаційної безпеки та сформувати тактичні і стратегічні напрямки такої діяльності. З'ясовано, що розгляд всіх основних питань комплексного забезпечення інформаційної безпеки дозволяє гармонізувати

українське законодавство у інформаційній сфері, а це у перспективі сприятиме формуванню ефективної державної політики у інформаційній сфері.

Література

1. Довгань О. Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України // Інформаційна безпека людини, суспільства, держави. 2015. № 3(19). С. 6–17. URL: http://nbuv.gov.ua/UJRN/iblsd_2015_3_3
2. Гусарєв С. Д. Юридична діяльність: методологічні та теоретичні аспекти: монографія. К.: Знання, 2005. 375 с.
3. Когосов О. М. Методи забезпечення безпеки інформаційної інфраструктури держави // Збірник наукових праць Харківського національного університету Повітряних Сил. 2016. № 2(47). С. 38–41. URL: http://www.hups.mil.gov.ua/periodic-app/article/16818
4. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. ... канд. юрид. наук: 12.00.01 / Київський національний університет внутрішніх справ. К., 2007. 186 с.
5. Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системи інформаційного захисту // Ефективна економіка. 2014. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2014_5_103
6. Конституція України: прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. (із змінами та доповненнями). URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр
7. Великий тлумачний словник сучасної української мови (з дод., допов. та CD) / уклад. і голов. ред. В. Т. Бусел. К.; Ірпінь: ВТФ “Перун”, 2009. 1736 с.
8. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України”:

Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

9. Про концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/75/98-вр#Text
10. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII (із змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
11. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII (із змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
12. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI (із змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text
13. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія / заг. ред. Р. А. Калюжний. Центр навчально-наукових та науково-практичних видань Національної академії Служби безпеки України, 2014. 196 с.
14. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім “Гельветика”, 2017. 168 с.
15. Тихомиров О. О. Забезпечення інформаційної безпеки як функція держави: автореф. дис. ... канд. юрид. наук: 12.00.01 / Національна академія внутрішніх справ. Київ, 2011. 19 с.

References

1. Dovhan O. D. Pravovi zasady formuvannia i rozvytku systemy zabezpechennia informatsiinoi bezpeky Ukrainy // Informatsiina bezpeka liudyny, suspilstva, derzhavy. 2015. № 3(19). S. 6–17. URL:

http://nbuv.gov.ua/UJRN/iblsd_2015_3_3

2. Husariev S. D. Yurydychna diialnist: metodolohichni ta teoretychni aspekty: monohrafiia. K.: Znannia, 2005. 375 s.
3. Kohosov O. M. Metody zabezpechennia bezpeky informatsiinoi infrastruktury derzhavy // Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl. 2016. № 2(47). S. 38–41. URL: http://www.hups.mil.gov.ua/periodic-app/article/16818
4. Maksymenko Yu. Ye. Teoretyko-pravovi zasady zabezpechennia informatsiinoi bezpeky Ukrainy: dys. ... kand. yuryd. nauk: 12.00.01 / Kyivskyi natsionalnyi universytet vnutrishnikh sprav. K., 2007. 186 s.
5. Cherevko O. V. Teoretychni zasady poniattia informatsiinoi bezpeky ta klasyfikatsiia zahroz systemy informatsiinoho zakhystu // Efektyvna ekonomika. 2014. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2014_5_103
6. Konstytutsiia Ukrainy: pryiniata na piatii sesii Verkhovnoi Rady Ukrainy 28 chervnia 1996 r. (iz zminamy ta dopovnenniamy). URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр
7. Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy (z dod., dopov. ta CD) / uklad. i holov. red. V. T. Busel. K.; Irpin: VTF “Perun”, 2009. 1736 s.
8. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku “Pro Doktrynu informatsiinoi bezpeky Ukrainy”: Ukaz Prezydenta Ukrainy vid 25.02.2017 r. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text
9. Pro kontseptsiiu Natsionalnoi prohramy informatyzatsii: Zakon Ukrainy vid 04.02.1998 r. № 75/98-VR. URL: https://zakon.rada.gov.ua/laws/show/75/98-вр#Text
10. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 r. № 2657-XII (iz zminamy ta dopovnenniamy). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

11. Pro derzhavnu taiemnytsiu: Zakon Ukrainy vid 21.01.1994 r. № 3855-XII (iz zminamy ta dopovnenniamy). URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
12. Pro dostup do publichnoi informatsii: Zakon Ukrainy vid 13.01.2011 r. № 2939-VI (iz zminamy ta dopovnenniamy). URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text
13. Tykhomyrov O. O. Zabezpechennia informatsiinoi bezpeky yak funktsiia suchasnoi derzhavy: monohrafiia / zah. red. R. A. Kaliuzhnyi. Tsentr navchalno-naukovykh ta naukovo-praktychnykh vydan Natsionalnoi akademii Sluzhby bezpeky Ukrainy, 2014. 196 s.
14. Nashynets-Naumova A.Iu. Informatsiina bezpeka: pytannia pravovoho rehuliuvannia: monohrafiia. Kyiv: Vydavnychyi dim “Helvetyka”, 2017. 168 s.
15. Tykhomyrov O. O. Zabezpechennia informatsiinoi bezpeky yak funktsiia derzhavy: avtoref. dys. ... kand. yuryd. nauk: 12.00.01 / Natsionalna akademiia vnutrishnikh sprav. Kyiv, 2011. 19 s.