DOI: 10.35774/app2020.01.103
УДК 351.86:659.3/.4:004](477)

Володимир Панченко,
доктор економічних наук, доцент,
доцент кафедри педагогіки та менеджменту
освіти Центральноукраїнського державного
педагогічного університету імені В. Винниченка
ORCID: https://orcid.org/ 0000-0002-4927-0330

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ ТА ПІДПРИЄМСТВ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ

Розглянуто складові державної інформаційної політики щодо забезпечення інформаційної безпеки країни і визначено основні напрямки діяльності органів державної влади у цій сфері. Проаналізовані внутрішні та зовнішні інформаційні загрози національній безпеці України та шляхи гарантування інформаційної безпеки країни. Інформаційна безпека розглядається, як складова національної безпеки країни, а також як глобальна проблема захисту інформації, інформаційного простору, інформаційного суверенітету країни та інформаційного забезпечення прийняття урядових рішень.

Розглянуто підходи до сутності загроз інформаційній безпеці та політико-правовому аналізу загроз інформаційній безпеці України на сучасному етапі. Загрози інформаційній безпеці аналізуються в контексті системи загроз національній безпеці.

На основі аналізу стану нормативно-правового регулювання інформаційної безпеки України визначено основні здобутки та недоліки у нормативно-правовому полі держави щодо забезпечення інформаційної безпеки.

Наведено визначення поняття інформаційної безпеки підприємства.

Виявлено основні цілі, завдання, принципи побудови та види загроз. На їх основні сформовано методичний підхід до формування системи інформаційної безпеки промислових підприємств.

На основі проведеного аналізу сучасних підходів до визначення сутності інформаційної безпеки, на основі узагальнення теоретичних положень та досвіду функціонування організацій запропоновано систему інформаційної безпеки підприємства розглядати, як модель інформаційного протиборства з факторами внутрішнього та зовнішнього середовища.

Використання розробленого підходу в практиці господарювання промислових підприємств допоможе підвищити ефективність розробки, впровадження та використання системи інформаційної безпеки та запобігти системних або методичних помилок на кожному з етапів.

Ключові слова: *інформаційна безпека держави, управління інформаційною безпекою, організаційно-правові засади інформаційної безпеки, інформаційні загрози, захист інформації підприємства.*

Бібл.: 12.

Панченко В.

Управление информационной безопасностью государства и предприятий: правовые и организационные аспекты

Рассмотрены составляющие государственной информационной политики по обеспечению информационной безопасности страны и определены основные направления деятельности органов государственной власти в этой сфере. Проанализированы внутренние и внешние информационные угрозы национальной безопасности Украины и пути обеспечения информационной безопасности страны. Информационная безопасность рассматривается как составляющая национальной безопасности страны, а также как глобальная проблема защиты информации, информационного пространства, информационного суверенитета страны и информационного обеспечения принятия правительственных решений.

Статья посвящена обзору подходов к сущности угроз информационной безопасности и политико-правовому анализу угроз информационной безопасности Украины на современном этапе. Угрозы информационной безопасности анализируются в контексте системы угроз национальной безопасности.

На основе анализа состояния нормативно-правового регулирования информационной безопасности Украины определены основные достоинства и недостатки в нормативно-правовом поле государства по обеспечению информационной безопасности.

Приведено определение понятия информационной безопасности предприятия.

Выявлены основные цели, задачи, принципы построения и виды угроз. На их основные сформирован методический подход к формированию системы информационной безопасности промышленных предприятий.

На основе проведенного анализа современных подходов к определению сущности информационной безопасности, на основе обобщения теоретических положений и опыта функционирования организаций предложена система информационной безопасности предприятия рассматривать как модель информационного противоборства с факторами внутренней и внешней среды.

Использование разработанного подхода в практике хозяйствования промышленных предприятий поможет повысить эффективность разработки, внедрения и использования системы информационной безопасности и предотвращения системных или методических ошибок на каждом из этапов.

Ключевые слова: *информационная безопасность государства, управление информационной безопасностью, организационно-правовые основы информационной безопасности, информационные угрозы, защита информации предприятия*

Panchenko V.

State and enterprise information security management: legal and organizational aspects

The components of the state information policy on information security and the basic activities of public authorities in this field are reviewed in the article. The internal and external information challenges facing Ukraine and ways of ensuring information security are analyzed. Information security is seen as a component of national security, as well as a global problem of information security, information space, information sovereignty and information support decision-making.

The article is devoted to the review of approaches to the essence of threats to information security and politico-juridical analysis of threats to information security of Ukraine at the present stage. The threats of information security are analysed in the context of the system of threats of national security.

On base of the analysis of the condition normative-legal regulation to information safety of the Ukraine are determined main value and defect in normative field state on provision of information security.

The definition of information security of the enterprise is given.

The basic goals, objectives, principles and types of threats. At their core formed methodical approach to developing the information security systems of industrial enterprises.

The proposed enterprise information security system is regarded as a model of information warfare with the factors of internal and external environment, based on the analysis of modern approaches to the definition of information security, and on a synthesis of theoretical positions and experience of functioning of the organizations.

The use of the developed approach the Holy Practice of management of industrial enterprises will help to increase the efficiency of development, implementation and use of information security and prevent system or methodological errors at each stage.

Keywords: *information security of the state, management of information security, organizational and legal principles of information security, information threats, protection of information of the enterprise.*

Постановка проблеми. З розвитком і поширенням інформаційно-комунікаційних технологій у всі галузі промисловості та сфери державного управління гострої значимості набувають питання забезпечення інформаційної безпеки, що визнано однією із складових національної безпеки.

Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою для України, яка часто є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення [2, с. 27–28].

Увага до проблем гарантування інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі і є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави [2, с. 28].

Аналіз останніх досліджень і публікацій. Окремі питання законодавчого регулювання в інформаційній сфері розглянуто у працях: К. Бєлякова, Б. Кормича, В. Конах, Е. Демського, Й. Мастяниці та ін.

Проблеми створення системи інформаційної безпеки на підприємствах намагалися вирішити у своїх наукових пошуках В. В. Андріанова, А. А. Гладких, Ю. А. Гатчин, Є. В. Климової, А. І. Моїсеєва, В. А. Ромака та ін.

Проте поза увагою вчених залишилися правові та організаційні аспекти управління інформаційною безпекою, що вимагає проведення додаткових досліджень щодо вирішення цієї актуальної проблеми.

Мета дослідження – охарактеризувати правові та організаційні аспекти управління інформаційною безпекою держави та підприємств.

Виклад основного матеріалу дослідження. Правове регулювання інформаційних правових відносин в Україні забезпечується низкою нормативних актів, у тому числі: Конституцією України,

Кримінальним кодексом України, Цивільним кодексом України, законами України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII, «Про науково-технічну інформацію» від 25 червня 1993 р. № 3322-XII, «Про державну таємницю» від 21 січня 1994 р. № 3855-XII, «Про авторське право і суміжні права» від 23 грудня 1993 р. № 3792-XII, «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР, «Про доступ до публічної інформації» від 13 січня 2011 р. № 2939-VI та іншими нормативними документами.

У системі загальноправових норм умовно виокремлюють комплекс публічно правових норм, що регулюють інформаційні відносини у сфері інформатизації, у т. ч. технічні засоби комунікації. До них належать такі системоутворювані закони України: «Про телекомунікації», «Про Національну програму інформатизації», «Про систему Суспільного телебачення і радіомовлення України», «Про Концепцію Національної програми інформатизації».

Принципи, пріоритети та напрями забезпечення кібербезпеки України визначені Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 р. № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» [12].

У зв'язку з рішенням Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» від 21 березня 2008 р., введеним у дію Указом Президента України від 23 квітня 2008 р. № 377, було затверджено Доктрину інформаційної безпеки України (Указ Президента України від 8 липня 2009 р. № 514/2009).

У Доктрині наголошується, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, соціальної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки [9, с. 76].

Наведемо визначення «інформаційна безпека» та «загрози інформаційній безпеці», які трактує Концепція інформаційної безпеки України (від 30.09.2015 р.).

Інформаційна безпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, за якого запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [3, с. 3–4].

Загрози інформаційній безпеці – наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері [3, с. 3–4].

Загрозами національній безпеці України в інформаційній сфері вважають такі:

– загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації;

– загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору [3, с. 7].

Під національним інформаційним простором розуміють усю сукупність інформаційних потоків як національного походження, так і іноземних, що доступні на території держави.

Основними цілями інформаційної політики України є забезпечення:

– захисту інформаційного суверенітету держави, особливо захисту національного інформаційного простору з інформаційним ресурсом і системи формування масової суспільної свідомості;

– рівня інформаційної достатності для прийняття рішень державними органами, підприємствами і громадянами;

– реалізації конституційних прав і свобод громадян, суспільства і держави [9, с. 71–72].

Організаційно-правовий механізм державної політики інформаційної безпеки – це впорядкована сукупність органів держави, задіяних у процесі формування, забезпечення і провадження політики інформаційної безпеки, а також внутрішні та зовнішні суспільні відносини, які регулюються системою правових норм та принципів у сфері інформації.

Реалізація організаційно-правового механізму державної політики інформаційної безпеки здійснюється:

– через сукупність державних інституцій, задіяних у процесі формування і впровадження політики інформаційної безпеки;

– шляхом ролей та правових відносин, що виникають у процесі проведення політики інформаційної безпеки, та специфічні ролі, форми і методи діяльності суб›єктів проведення політики інформаційної безпеки;

– через сукупність правових норм та принципів, що регулюють зміст та процес проведення політики інформаційної безпеки.

Інформаційна безпека є пріоритетним завданням також і для виробничих підприємств та інших суб'єктів господарювання, а не тільки органів державної влади.

Сучасні інформаційні системи призначені для забезпечення працездатності інформаційної інфраструктури підприємства, надання різних видів інформаційних сервісів, автоматизації фінансової та виробничої діяльності, а також бізнес-процесів організації, що дають змогу скоротити як фінансові, так і трудові витрати. В інформаційних системах зберігаються і обробляються значні обсяги інформації різного ступеня секретності, тому гостро постає питання про захищеність цих інформаційних систем підприємства від різних загроз безпеці інформації [5, с. 81].

Науковець М. В. Верескун, провівши аналіз результатів розвитку провідних промислових підприємств України, дійшов висновку, що «керівництво постійно приймає та удосконалює заходи щодо захисту корпоративної інформації, проте ці дії не носять системного характеру, оскільки спрямовані на усунення локальних конкретних загроз, які найчастіше одного разу вже були реалізовані» [1, с. 55].

Під інформаційною безпекою (ІБ) промислового підприємства М. В. Верескун розуміє «всі елементи системи управління підприємством, пов'язані з визначенням, досягненням конфіденційності, цілісності, доступності, неспростовності, підзвітності, автентичності та достовірності інформації або засобів її обробки» [1, с. 55].

Підприємницька інформація, що створює суб'єктові вигідні умови для прийняття оперативних рішень і досягнення ефективного результату, вважається корисною. Для її захисту від сторонніх осіб, щоб не втратити очікування, як правило, застосовується комплекс методів технічного й організаційного характеру [7, с. 6].

Науковці А. Печенюк [8], О. А. Сороківська і В. Л. Гевко [10] розглядали особливості організації інформаційної безпеки сучасного підприємства і дійшли висновку, що інформаційна безпека є невід'ємною складовою системи економічної безпеки суб'єкта господарювання.

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. З огляду на це безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами [8].

Основні завданняі нформаційної безпеки такі:

- організація доступності інформації;
- забезпечення цілісності інформації;
- гарантування конфіденційності інформації;
- забезпечення вірогідності інформації;
- забезпечення юридичної значимості інформації, поданої у вигляді електронного документа;
- здійснення невідстежуваності дій користувача [4, с. 11].

Інформаційна безпека в рамках забезпечення роботоздатності інформаційної системи повинна забезпечувати захист від:

порушення функціонування інформаційної системи шляхом впливу на інформаційні канали, канали сигналізації, керування і віддаленого завантаження баз даних, комутаційного устаткування, системне і прикладне програмне забезпечення;

– несанкціонованого доступу до інформаційних ресурсів і від намагань використання ресурсів мережі, що призводить до витоку даних, порушення цілісності мережі й інформації, зміни функціонування підсистем розподілу інформації, доступності баз даних;

– руйнування вбудованих та зовнішніх засобів захисту;

– неправомірних дій користувачів і персоналу з обслуговування мережі [4, с. 13].

З погляду державних структур захисні заходи насамперед мають забезпечити конфіденційність, цілісність і доступність інформації.

Для комерційних структур, ймовірно, найважливішими є цілісність і доступність даних і послуг. На відміну від державних, комерційні організації більш відкриті і динамічні, тому ймовірні загрози для них відрізняються не тільки кількістю, а й якістю [4, с. 13]

Науковці В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович [4] для вирішення завдань щодо забезпечення безпеки в інформаційних системах пропонують такі заходи:

– захистити інформацію під час її зберігання, оброблення і передавання мережею;

– підтвердити дійсність об'єктів даних і користувачів;

– знайти і попередити порушення цілісності об'єктів даних;

– захистити технічні пристрої і приміщення;

– захистити конфіденційну інформацію від витоку вбудованими електродними пристроями зняття інформації;

– захистити програмні засоби від приєднання програмних закладок і вірусів;

– захистити від несанкціонованого доступу до інформаційного ресурсу і технічних засобів мережі, зокрема до засобів керування, щоб запобігти зниженню рівня захищеності інформації і самої мережі;

– організувати заходи, що спрямовані на забезпечення збереження конфіденційних даних [4, с. 14].

Науковець А. Ю. Нашинець-Наумова [6] характеризує рівні забезпечення інформаційної безпеки в державі.

На законодавчому рівні розрізняють дві групи заходів: ті, що спрямовані на створення і підтримку в суспільстві негативного (у т. ч. із застосуванням покарань) ставлення до порушень і порушників інформаційної безпеки (назвемо їх заходами обмежувальної спрямованості); направляючі і координуючі заходи, що сприяють підвищенню освіченості суспільства в галузі інформаційної безпеки, що допомагають у розробці та поширенні засобів забезпечення інформаційної безпеки (заходи творчої спрямованості). Найважливіше (і, ймовірно, найважче) на законодавчому рівні – створити механізм, що дає змогу узгодити процес розробки законів з реаліями і прогресом інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, оскільки на практиці, крім інших негативних моментів, це веде до зниження інформаційної безпеки.

До адміністративного рівня інформаційної безпеки відносяться дії загального характеру. Головна мета заходів адміністративного рівня – сформувати програму робіт у галузі інформаційної безпеки та забезпечити її виконання, виокремивши необхідні ресурси і контролюючи стан справ. Основою програми є політика безпеки, що відображає підхід організації до захисту своїх інформаційних активів. Керівництво кожної організації має усвідомити необхідність підтримки режиму безпеки і виділення на ці цілі значних ресурсів. Політика безпеки будується на основі аналізу ризиків, які визнаються реальними для інформаційної системи організації. Коли ризики проаналізовані та стратегія захисту визначена, складається програма забезпечення інформаційної безпеки. «Політика безпеки» (є не зовсім точним перекладом англійського словосполучення «security policy»), має на увазі не окремі правила або їх набори, а стратегію організації в галузі інформаційної безпеки. Політика безпеки – сукупність документованих рішень, прийнятих керівництвом організації і спрямованих на захист інформації та асоційованих з нею ресурсів.

Процедурний рівень орієнтований на людей, а не на технічні засоби. Саме люди формують режим інформаційної безпеки і водночас становлять головну загрозу, тому «людський фактор» заслуговує особливої уваги. Слід усвідомити ту ступінь залежності від комп'ютерної обробки даних, в яку потрапило сучасне суспільство. Акцент слід робити не на військовому чи кримінальному боці справи, а на цивільних аспектах, пов'язаних з підтриманням нормального функціонування апаратного та програмного забезпечення, тобто концентруватися на питаннях доступності та цілісності даних.

Програмно-технічний рівень, тобто рівень, спрямований на контроль комп'ютерних сутностей – обладнання, програм та/або даних, утворюють останній і найважливіший рубіж інформаційної безпеки. Наголошуємо, що збиток наносять переважно дії легальних користувачів, щодо яких процедурні регулятори малоефективні. Головні вороги – некомпетентність і неакуратність під час виконання службових обов'язків, і тільки програмно-технічні заходи здатні їм протистояти [6, с. 33–34].

Діяльність державних органів у сфері забезпечення інформаційної безпеки зосереджується на двох напрямах:

– забезпечення сталого розвитку інформаційного простору України з метою досягнення ним такого рівня, який завдяки своїм властивостям міг би протистояти зовнішнім та внутрішнім загрозам;

– організація створення і функціонування системи захисту процесу розвитку інформаційного простору від загроз.

Інформаційна безпека України забезпечується шляхом захисту національного інформаційного простору від інформаційних загроз та через сприяння його сталому розвитку задля реалізації життєво важливих інтересів та потреб громадянина, суспільства і держави в інформаційній сфері [3, с. 5].

Науковець В. Ю. Степанов зазначає, що «організація сучасної інформаційної безпеки держави є, безперечно, складним, системним, багаторівневим феноменом, на стан, динаміку й перспективи розвитку якого безпосередньо впливають багато зовнішніх і внутрішніх чинників, найважливішими з яких є: політична обстановка у світі; наявність потенційних зовнішніх і внутрішніх загроз; стан і рівень інформаційно-комунікаційного розвитку країни; внутрішньополітична ситуація» [11, с. 5].

Висновки. Інформаційна безпека є невід'ємним складником системи комерційної безпеки суб'єктів господарювання, а також політичної та економічної безпеки держави загалом.

Визначено, що інформаційна безпека є станом захищеності життєвих інтересів громадянина, суспільства і держави, за якого запобігається можливе завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації, умисне спричинення негативних наслідків застосування інформаційних технологій.

Організаційно-правовий механізм державної політики інформаційної безпеки є впорядкованою сукупністю органів держави, задіяних у процесі формування, забезпечення і провадження політики інформаційної безпеки, а також внутрішні та зовнішні суспільні відносини, які регулюються системою правових норм та принципів у сфері інформації.

Встановлено, що загрози інформаційній безпеці поділяються на наявні та потенційно можливі явища і чинники, які можуть створити певну небезпеку інтересам людини, суспільства і держави в інформаційній сфері.

Охарактеризовано рівні забезпечення інформаційної безпеки в державі: законодавчий, адміністративний, процедурний, програмно-технічний рівень.

Виокремлено основні завдання у сфері інформаційної безпеки для суб'єктів господарювання: організація доступності інформації; забезпечення цілісності інформації; гарантування конфіденційності інформації; забезпечення вірогідності інформації; забезпечення юридичної значимості інформації, поданої у вигляді електронного документа; здійснення невідстежуваності дій користувача.

Доведено, що пріоритетними завданнями державної інформаційної політики є такі: створення, розвиток і вдосконалення системи кібербезпеки; захист незалежності ЗМІ і прав громадян на свободу слова; забезпечення суверенітету та інформаційної безпеки органів держави та суб'єктів господарювання; запобігання злочинам у сфері інформаційних технологій.

Однак одержані результати дослідження не вичерпують усіх аспектів управління інформаційною безпекою, зокрема перспективами подальших пошуків можуть бути економічні та політичні аспекти інформаційної безпеки держави.

Список використаних жерел

1. Верескун М. В. Методичне забезпечення системи інформаційної безпеки промислових підприємств. *Економіка і організація управління.* 2014. № 1 (17). С. 54–60.
2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision*. 2016. Vol. 2, Num. 1. С. 27–32. URL : http://nbuv.gov.ua/UJRN/hv_2016_2_1_7 (дата звернення: 15.01.2020).
3. Концепція інформаційної безпеки України. URL : http://mip.gov.ua/files/banners/Final%20Проект%20концепції%20(Текст)%20-%2030.09.15.pdf (дата звернення: 15.01.2020).
4. Лужецький В. А., Кожухівський А. Д,, Войтович О. П. Основи інформаційної безпеки : навч. посіб. Вінниця : ВНТУ, 2013. 221 с.
5. Маркіна І. А., Дячков Д. Н. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва.* 2016. № 3(1). С. 80–88.
6. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Видав. дім «Гельветика», 2017. 168 с.
7. Низенко Е. І., Каленяк Е. І. Забезпечення інформаційної безпеки підприємництва : навч. посіб. Київ : МАУП, 2006. 134 с.
8. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. URL : http://sophus.at.ua/publ/2014_04_17_18_kampodilsk/sekcija_4_2014_04_17_18/osoblivosti_organizaciji_informacijnoji_bezpeki_suchasnogo_pidpriemstva/54-1-0-931 (дата звернення: 17.01.2020).

9. Правові засади інформаційної безпеки України : монографія / П. Д. Біленчук, Л. В. Борисова, І. М. Неклонський., В. О. Собина ; за ред. П. Д. Біленчука. Харків : 2018. 289 с.
10. Сороківська О. А., Гевко Л. В, Інформаційна безпека підприємства : нові загрози та перспективи. *Вісник Хмельницького нац. ун-ту.* 2010. № 2, т. 2. С. 32–35.
11. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики. *Державне будівництво.* 2016. № 2. С. 19.
12. Про Доктрину інформаційної безпеки України : Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. URL : https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 19.01.2020).

References

1. Vereskun, M. V. (2014) Metodychne zabezpechennia systemy informatsiinoi bezpeky promyslovykh pidpryiemstv [Methodical provision of information security system of industrial enterprises] (2014) *Ekonomika i orhanizatsiia upravlinnia - Economics and organization of management, 1 (17), 54–60* [in Ukrainian].
2. Ilnytska, U. (2016). Informatsiina bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnym informatsiino-psykholohichnym vplyvam [Information security of Ukraine: current challenges, threats and mechanisms of countering negative information-psychological impacts]. *Humanitarian vision - Humanitarnyi ohliad, 2 (1),* 27–32. [in Ukrainian].
3. The concept of information security of Ukraine. [Online], Available at: http://mip.gov.ua/files/banners/Final%20Проект%20Концепції%20 (Текст)%20-%2030.09.15.pdf
4. Luzhetskyi, V. A., Kozhukhivskyi, A. D., Voitovych, O. P. (2013) *Osnovy informatsiinoi bezpeky. [Fundamentals of Information Security].* Vinnytsia: VNTU [in Ukrainian].
5. Markina, I. A., Diachkov, D. V. (2016). Osnovy formuvannia systemy menedzhmentu informatsiinoi bezpeky pidpryiemstva [Fundamentals of formation of enterprise information security management system]. *Problemy i perspektyvy rozvytku pidpryiemnytstva - Problems and prospects of entrepreneurship development, 3(1),* 80-88. URL: http://nbuv.gov.ua/UJRN/piprp_2016_3(1)__18 [in Ukrainian].
6. Nashynets-Naumova, A. Yu. (2017), *Informatsiina bezpeka: pytannia pravovoho rehuliuvannia: monohrafiia [Information security: issues of legal regulation]*. Kyiv: Helvetyka [in Ukrainian].
7. Nyzenko, E. I., Kaleniak, V. P. (2006). *Zabezpechennia informatsiinoi bezpeky pidpryiemnytstva: Navch. posib. [Ensuring information security of entrepreneurship]*. Kyiv: MAUP [in Ukrainian].
8. Pecheniuk, A. (2014). *Osoblyvosti orhanizatsii informatsiinoi bezpeky suchasnoho pidpryiemstva [Features of organization of information security of the modern enterprise]*. URL: http://sophus.at.ua/publ/2014_04_17_18_kampodilsk/sekcija_4_2014_04_17_18/osoblivosti_organizaciji_informacijnoji_bezpeki_suchasnogo_pidpriemstva/54-1-0-931 [in Ukrainian].
9. Bilenchuk, P. D., Borysova, L. V., Neklonskyi, I. M., Sobyna, V. O. (2018). *Pravovi zasady informatsiinoi bezpeky Ukrainy: monohrafiia [Legal basis of information security of Ukraine]*. Kharkiv [in Ukrainian].
10. Sorokivska, O.A. and Gevko, V.L. (2010). Informatsiina bezpeka pidpryiemstva : novi zahrozy ta perspektyvy. [Enterprise Information Security: New Threats and Prospects]. *Visnik Hmelnickogo nacionalnogo universitetu - Bulletin of Khmelnitsky National University, 2(2),* 32–35 [in Ukrainian].
11. Stepanov, V. Yu. (2016). Informatsiina bezpeka yak skladova derzhavnoi informatsiinoi polityky [Information security as a component of state information policy]. *Derzhavne budivnytstvo - State building, 2,* 1–9 [in Ukrainian].
12. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy» [Decree of the President of Ukraine On the decision of the National Security and Defense Council of December 29, 2016 «On the Doctrine of Information Security of Ukraine»].* Retrieved from https://zakon.rada.gov.ua/laws/show/47/2017 [in Ukrainian].

Стаття надійшла до редакції 04.02.2020.