

УДК 330

РЗАЄВ Г. І.,
ДЖУС О. С.

Хмельницький національний університет

НОРМАТИВНО – ЗАКОНОДАВЧА ПІДТРИМКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІДПОВІДНО ДО ПОТРЕБ ЕКОНОМІЧНОГО АНАЛІЗУ

В статті досліджено сутність інформаційної безпеки у розрізі площин її вивчення. Окреслено основні його характеристики та обґрунтовано їх значення. Запропоновано досліджувати інформаційну безпеку підприємства в залежності від виду загроз її рівню. Розглянуто нормативно – законодавчу підтримку інформаційної безпеки підприємства у розрізі Законів України та окреслено сферу їх регулювання. Важливе значення для підтримки інформаційної безпеки займає мінімізація рівня загроз, а в окремих випадках розробка системи заходів їх попередження. Наголошено на доцільності дослідження загроз, що пов'язані з навмисними помилками.

Ключові слова: інформаційна безпека, нормативно-законодавче регулювання, інформаційний простір, мінімізація загроз.

RZAIEV H.,
DZHUS O.

Khmelnitsky National University

NORMATIVELY - LEGISLATIVE SUPPORT FOR INFORMATION SECURITY RELATING TO THE NEEDS OF ECONOMIC ANALYSIS

In the article the essence of information security in the context of the planes of its study is explored. Its main characteristics are described and their significance is substantiated. It is proposed to investigate information security as a state of information space security. The information security as a condition of the information environment is determined by the timeliness, accuracy and impartiality of information of all levels and divisions of the enterprise. It is proposed to study information security as a complexity of information resources that determine the state of the enterprise. Security as the effectiveness of information and analytical bases that determine the performance of the entity. Information security is proposed to be investigated as a basis for the formation and forecasting of the enterprise's activities in the future. It is proposed to investigate information security depending on the type of threats and level, namely: as information rights and freedoms of man and citizen; as ensuring the state of protection of personality, society, state from the influence of poor-quality information; information and information resources from unlawful influence of unauthorized persons. Compliance with the relevant information collection, storage and processing regime will enable us to achieve and maintain an appropriate level of information security and, accordingly, improve the performance of the enterprise.

It is stressed that in the conditions of unfair competition there is a danger of appearance of threats to information security of the enterprise. There is a need to protect economic competition through the support of an appropriate level of information security. It is proposed to investigate the information security of the enterprise depending on the type of threats and level. Regulatory and legislative support of information security of the enterprise in the context of the Laws of Ukraine is considered and the scope of their regulation is outlined. It is important to maintain information security to minimize the level of threats, and in some cases, the development of a system of measures to prevent them. It is emphasized on the expediency of researching the threats associated with intentional mistakes. The main threats under protection of commercial secrets and commercial interests are considered. The main stages of formation of a secure information system of the subject of economic activity are considered, which is based on the relevant regulatory and legislative provision. The main measures to increase the level of information security at the level of the economic entity are proposed and substantiated.

Key words: information security, normative-legislative regulation, information space, minimization of threats.

Вступ. Підтримка інформаційної безпеки є основою забезпечення рівня економічної безпеки на всіх рівнях господарювання. Інформаційна безпека як стан захищеності інформаційного середовища забезпечує його формування, використання і розвиток в інтересах господарюючих суб'єктів. На рівні підприємства, на сучасному етапі розвитку методів управління, на всіх рівнях управління інформаційну безпеку доцільно вивчати як провідний інструмент здійснення ефективної господарської діяльності. Стан та рівень інформаційної безпеки значною мірою залежить від її нормативно-законодавчої підтримки. Відповідна нормативно-законодавча підтримка

Аналіз останніх досліджень. У сучасних дослідженнях науковці розглядають актуальні проблеми, пов'язані зі створенням, перетворенням і споживанням інформації. Авторами досліджуються питання щодо створення і розповсюдження вихідної та похідної інформації. Останнім часом є актуальними проблеми, які потребують подальшого вирішення, що пов'язані з формуванням інформаційних ресурсів, підготовкою інформаційних продуктів, надання інформаційних послуг та ін. Окремі питання та проблеми оцінки та розуміння інформаційної безпеки розглядали В.М. Богущ, В.Л. Бурячок, В.П. Горбулін, Г.М. Гулак, С.Ф. Гуцу, О.Г. Додонов, О.І. Крюков, М.І. Зубок, Д.В. Ланде, А.І. Марущак, О.А. Сороківська, М.Ю. Танцюра., В.Б. Толубко, О. Юдін, В.С. Цимбалюк, Ю.О. Шпак та ін.

Постановка завдання. Метою статті є дослідження сутності категорії «інформаційна безпека» та окреслення основних його особливостей, у розрізі наукових підходів, з урахуванням нормативно-законодавчої підтримки.

Результати дослідження. Успішна підприємницька діяльність значною мірою залежить від уміння розпоряджатися таким найціннішим товаром, як інформація. Підприємницька (комерційна) діяльність тісно пов'язана з отриманням, зберіганням, накопиченням, обробкою і використанням різноманітної інформації. Однак захисту підлягає не вся інформація, а лише та, яка є цінною (своєчасною, об'єктивною, неупередженою) для підприємства. При визначенні цінності підприємницької інформації необхідно керуватися такими критеріями, як корисність, своєчасність і достовірність даних та ін.

Щоб ефективно функціонувати за умов нестабільної економіки, необхідно постійно отримувати повну та достовірну інформацію, що комплексно характеризує процеси діяльності підприємства. Якість інформаційного забезпечення гарантує певна послідовність дій та етапів, логічність яких ґрунтується на науковому підході. Ефективність інформаційного забезпечення обумовлюється системністю та комплексністю інформаційних потоків. Поетапний збір, обробка, групування, аналіз, діагностика дадуть змогу забезпечити повноту, точність, своєчасність та об'єктивність інформації, що групується відповідно до визначених цілей та завдань діяльності суб'єкта господарювання. Дотримання зазначених принципів дасть змогу підтримувати рівень інформаційної безпеки на достатньому рівні. Останнім часом все більше науковців приділяють увагу інформаційній безпеці підприємства і наголошують на її важливості для підприємства.

Важливо підкреслити, що у сучасних дослідженнях відсутній єдиний підхід до змісту поняття «інформаційна безпека». Сучасні підходи до розуміння зазначеного поняття представлено у табл. 1.

Таблиця 1.

Визначення інформаційної безпеки у сучасних дослідженнях

Автор (джерело)	Визначення поняття «інформаційна безпека»
Богуш В.М. [1, ст.35]	це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.
Гуцу С.Ф. [3, ст.30]	стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз
Крюков О.І. [7, ст.3]	це суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільні правовідносини пов'язані з організацією технологій створення, розповсюдження, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави.
Марущак А.І. [8, ст.94]	це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.
Сороківська О.А. [10, ст.32]	суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності.
Танцюра М.Ю. [11, ст.452]	збереження конфіденційності, цілісності та доступності інформації; доступність – це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність – це властивість захищеності точності та повноти даних; конфіденційний – це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами.
Цимбалюк В.С. [14, ст.88]	це суспільні відносини щодо створення та підтримання на належному (бажаному, можливому) рівні життєдіяльності відповідної інформаційної системи, у тому числі підприємництва.
Додонов О.Г. [5, ст.65]	стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави
Панарін І.М. [9, ст.87]	стан інформаційного середовища суспільства і політичної еліти, який забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства
Тер-Акопов А.А. [13, ст. 9]	стан захищеності інформації, яка забезпечує життєво важливі інтереси людини

У попередніх дослідженнях, нами було досліджено, існуючі теоретичні підходи до розуміння інформаційної безпеки, що на основі узагальнення дало змогу виділити такі його характеристики:

- стан захищеності інформаційного простору; стан інформаційного середовища
- своєчасність, точність та неупередженість інформації всіх рівнів та підрозділів підприємства;
- комплексність інформаційних ресурсів, що визначають стан діяльності підприємства;
- ефективність інформаційно-аналітичних баз, що зумовлюють результативність діяльності суб'єкта господарювання;

– основа формування та прогнозування діяльності підприємства на перспективу.

Окремі автори пропонують досліджувати інформаційну безпеку в залежності від виду загроз її рівню, а саме: як інформаційних прав і свобод людини і громадянина; як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб.

При дослідженні проблем оцінки та підтримки інформаційної безпеки є доцільним розуміти її сутність, але при тому, ґрунтуючись на таких основних аспектах, а саме: концепції інформаційної безпеки держави; зацікавленість та підтримка інформаційної безпеки; інформаційне середовище суспільства. Можливі загрози інформаційній безпеці, об'єкти та суб'єкти інформаційної безпеки є основою розв'язання проблем підтримки інформаційної безпеки. Важливе місце посідають види інформаційної безпеки і відповідно форми і принципи її забезпечення.

Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок — обґрунтованість рішень та дій, що приймаються.

В інформаційному праві інформаційна безпека – це одна зі сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [6, ст. 26].

Важливе значення для підтримки рівня інформаційної безпеки на належному рівні належить відповідному нормативно-законодавчому забезпеченні. Визначне місце в забезпеченні інформаційної безпеки належить закону про інформацію, що регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Важливе місце займають закони стосовно формування концепції національної програми інформатизації, що дають характеристику сучасного стану інформатизації, окреслюють стратегічні цілі та основні принципи інформатизації, очікувані наслідки її реалізації тощо. Основні нормативно-законодавчі акти щодо підтримки інформаційної безпеки та сфера їх регулювання представлено у табл.2.

Важливе значення для підтримки інформаційної безпеки займає мінімізація рівня загроз, а в окремих випадках розробка системи заходів їх попередження. Існує дві групи загроз щодо інформаційної безпеки підприємства, таких як випадкові або ненавмисні дії, що виражаються в неадекватній підтримці механізмів захисту та помилках в управлінні, та навмисні загрози – несанкціонований доступ до інформації і несанкціонована маніпуляція даними, ресурсами і самими системами. Окремо необхідно виділити загрози, пов'язані з навмисними помилками, що виникають за межами бізнесу. До таких загроз відносять доцільно віднести [2, с. 242]:

- несанкціонований доступ до інформації, що зберігається в системі;
- заперечення дій, пов'язаних із маніпулюванням інформацією (наприклад, несанкціонована модифікація, яка веде до порушення цілісності даних);
- введення в програмні продукти і проекти «логічних бомб», які спрацьовують за виконання певних умов або після закінчення певного періоду часу і частково або повністю виводять з ладу комп'ютерну систему;
- розроблення і поширення комп'ютерних вірусів;
- зміна комп'ютерної інформації і підробка електронних підписів;
- недбалість у розробленні, підтримці та експлуатації програмного забезпечення, що приводить до краху комп'ютерної системи;
- заперечення дій або послуги;
- розкрадання інформації;
- перехоплення інформаційних потоків;
- відмова в наданні послуги [2, с. 242].

Заслугує на увагу нормативно-законодавче регулювання доступу до публічної інформації. Зазначене законодавство визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених законодавством та інформації, що становить суспільний інтерес.

За умов недобросовісної конкуренції виникає небезпека появи загроз інформаційній безпеці підприємства. Виникає потреба захисту економічної конкуренції через підтримку відповідного рівня інформаційної безпеки.

Йдеться про наявність загроз посягання на інформацію суб'єктів підприємництва. В той же час, враховуючи, що суб'єкти підприємництва у ході конкурентних відносин не лише утворюють нову інформацію, яка є об'єктом посягань з боку конкурентів, а і самі досить часто вдаються до заходів отримання чужої інформації, в т. ч. і з метою поповнення власного інформаційного ресурсу. Враховуючи, що інформаційне середовище наповнене не лише об'єктивною інформацією, а отримання чужої інформації може мати негативні наслідки, у інформаційній діяльності суб'єктів підприємництва можуть виникати певні ризики [4, с.60].

За умов посилення конкуренції важливе значення у захисті комерційної таємниці та комерційних інтересів належить Закону України «Про захист від недобросовісної конкуренції» від 7 червня 1996 року № 236/96-ВР (гл. 4, 5) (статті 16, 17, 18, 19, 26).

Таблиця 2

Нормативно – законодавча підтримка інформаційної безпеки

Нормативно-правовий акт	Сфера регулювання
Закон України «Про інформацію» від 2 жовтня 1992р. №2658-ХІІ // Відомості Верховної Ради України. – 1992. – № 48/ - ст. 651	Регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації
Закон України «Про науково-технічну інформацію» від 25 червня 1993р. №3323-ХІІ// Відомості Верховної Ради України. – 1993. - №33. – ст.346.	Визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу України. Метою Закону є створення в Україні правової бази для одержання та використання науково-технічної інформації
Закон України «Про Концепцію національної програми інформатизації» від 4 лютого 1998р. №75/98-ВР// Відомості Верховної Ради України. – 1998. - №27-28. – ст.182.	Визначає характеристику сучасного стану інформатизації, стратегічні цілі та основні принципи інформатизації, очікувані наслідки її реалізації
Закон України «Про захист персональних даних» від 1 червня 2010р. №2297-VI// Відомості Верховної Ради України. – 2010. - №34. – ст.481.	Регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних
Закон України «Про доступ до публічної інформації» від 13 січня 2011р. №2939-VI// Відомості Верховної Ради України. – 2011. - №32. – ст.314.	Визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес
НП(С)БО 1 «Загальні вимоги до фінансової звітності», затверджене наказом Міністерства фінансів України від 31 березня 1999р. №87 зі змінами і доповненнями.	Визначає мету, склад і принципи підготовки фінансової звітності та вимоги до визнання і розкриття її елементів.

Згідно з ст.16 ЗУ «Неправомірне збирання комерційної таємниці» виникає загроза щодо добування протиправним способом відомостей, які відповідно до законодавства України, становлять комерційну таємницю, якщо це завдало чи могло завдати шкоди господарюючому суб'єкту (підприємцю).

Враховуючи інформацію ст.17 ЗУ «Розголошення комерційної таємниці» виникає загроза ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що, відповідно до чинного законодавства України, становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків, якщо це завдало чи могло завдати шкоди господарюючому суб'єкту (підприємцю).

За умов конкурентної боротьби виникає загроза схилення до розголошення комерційної таємниці (ст.18 ЗУ), що представляє собою спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків відомості, що, відповідно до чинного законодавства України, становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди господарюючому суб'єкту (підприємцю).

Згідно зі ст.19 ЗУ виникає загроза неправомірного використання комерційної таємниці, виникає загроза використання, без дозволу уповноваженої на те особи, неправомірно здобутих відомостей, що становлять відповідно до законодавства України, комерційну таємницю.

Важливим є формування безпечної інформаційної системи суб'єкта господарювання, що ґрунтується на відповідному нормативно-законодавчому забезпеченні. Основними етапами її формування є наступні:

1. Розробка програм формування інформаційного забезпечення відповідно до об'єктів виникнення небезпек.
2. Систематизація, класифікація та раціоналізація інформаційних потоків за різними джерелами надходження, що відповідають напрямам дослідження.

3. Збір, опрацювання, узагальнення та аналіз інформації відповідно до обраних напрямів дослідження та об'єктів виникнення загроз.

4. Аналітичне групування та обробка інформації відповідно до висунутих вимог та визначених завдань дослідження рівня безпеки.

5. Захист інформаційного середовища та його продукту на рівні підприємства і за його межами.

Основними напрямками підтримки безпеки інформації на рівні суб'єкта господарювання, можуть бути такі: раціоналізація документів та їх структури; систематизація та спрощеність документів; автоматизація обліку та його удосконалення шляхом використання останніх версій програмного забезпечення; комп'ютеризація, уніфікація, типізація та стандартизація; скорочення документообігу та ліквідація дублювання; розвиток інформаційних технологій та використання відеоінформаційних систем тощо.

Висновки. Отже, у сучасних умовах інформаційна безпека є невід'ємною складовою економічної безпеки суб'єкта господарювання. В свою чергу, надійне забезпечення інформаційної безпеки є необхідною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Ринкове динамічне середовище вимагає постійної підтримки відповідного інформаційного середовища, що буде відповідати певному рівню інформаційної безпеки. Дотримання відповідного режиму збирання, збереження та обробки інформації дасть змогу досягти і підтримувати відповідний рівень інформаційної безпеки й відповідно покращити результати діяльності підприємства. Основними заходами щодо підвищення рівня інформаційної безпеки можуть бути наступні:

- посилення персональної відповідальності посадових осіб за збереження та обробку інформаційних масивів, порушення змісту яких може призвести до втрати комерційної таємниці;
- обмежити доступ до конфіденційної інформації широкого кола відповідальних осіб;
- позбавити можливості відповідних працівників безконтрольного, несвідомого користування та винесення різних носіїв інформації;
- створити умови забезпечення та підтримки необхідного режиму захисту інформаційного середовища;
- обмежити несанкціоноване користування системами обробки інформації і наявними там даними, а також лімітувати отримання дозволів на користування ними;
- ознайомлення посадових осіб з правилами діловодства та контроль за їх дотриманням;
- проведення профілактичних заходів, спрямованих на попередження режиму захисту інформаційного продукту;
- дотримання конфіденційності та встановленого порядку проведення нарад, переговорів, співбесід тощо;
- посилення контролю та пропускового режиму відповідних об'єктів та ін.

Таким чином, дотримання запропонованих заходів дасть змогу суб'єктам господарювання підтримувати рівень інформаційної безпеки відповідно до вимог часу. Саме функціонування підприємств у мінливому конкурентному середовищі потребує постійного моніторингу рівня інформаційної безпеки, що є гарантією підвищення відповідного стану економічної безпеки за умов загострення конкурентної боротьби.

Література

1. Богуш В.М. Інформаційна безпека держави
2. Бурачок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Підручник] / В.Л. Бурачок, Г.М Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с
3. Гуцу С.Ф. Правові основи інформаційної діяльності: навчальний посібник / С.Ф. Гуцу. – Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 48 с.
4. Зубок М.І. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – К.: ГНОЗІС, 2015 – 216 с.
5. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / О.Г. Додонов, В.П. Горбулін, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.
6. Копилов В.А. Информационное право / В.А. Копилов. – М. : Юрист, 2002 – с. 122.
7. Крюков О.І. Інформаційна безпека держави в умовах глобалізації / О. І. Крюков. // Державне будівництво. - 2007. - № 2. Режим доступу: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12 / В. Богуш, О. Юдін; [Гол. ред. Ю.О. Шпак]. – К.: «МК-Прес», 2005. – 432 с.
8. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки // Державна безпека України / А.І. Марущак. – 2011.
9. Панарин И.Н. Информационная безопасность / И.Н. Панарин [Електронний ресурс] / Режим доступу: http://panarin.com/info_voina/86-informacionnaya-bezopasnost.html.
10. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи [Текст] / О.А. Сороківська, В.Л. Гевко // Вісн. Хмельниц. нац. ун-ту. Сер.: Екон. науки. – 2010. – № 2. – Т. 2. – С. 32–35.
11. Тацюра М.Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства // Матеріали Другої наук.-практ. конф. «Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях» 23- 24 вересня 2010 р. м. Бахчисарай, НДІ сталого розвитку та природокористування,

РВПС України НАН України, Кримський інститут КНЕУ ім. Вадима Гетьмана / М.Ю. Тацюра. – Сімферополь: Фенікс, 2010. – С. 451–453.

13. Тер-Акопов А.А. Безопасность человека : Теоретические основы социально-правовой концепции / А.А. Тер-Акопов, Междунар. независимый экол.-политолог. ун-т (МНЭПУ). – М. : Изд-во МНЭПУ, 1998. – 196 с.

14. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації) // Підприємництво, господарство і право. – 2004. – № 3. – С. 88-91.

References

1. Bohush V.M. Informatsiyna bezpeka derzhavy / V. Bohush, O. Yudin; [Hol. red. YU.O. Shpak]. – K.: «MK-Pres», 2005. – 432 s.
2. Buryachok V.L. Informatsiynny ta kiberprostory: problemy bezpeky, metody ta zasoby borot'by [Pidruchnyk] / V.L. Buryachok, H.M. Hulak, V.B. Tolubko. – K.: TOV «SIK HRUP UKRAYINA», 2015. – 449 s.
3. Hutsu S.F. Pravovi osnovy informatsiynoy diyal'nosti: navchal'nyy posibnyk / S.F. Hutsu. – KH.: Nats. aerokosm. un-t «Khark. aviats. in-t», 2009. – 48 s.
4. Zubok M.I. Informatsiyna bezpeka v pidpryyemnyts'kiy diyal'nosti / M.I. Zubok. – K.: HNOZIS, 2015 – 216 s.
5. Informatsiynni operatsiyi ta bezpeka suspil'stva: zahrozy, protydiya, modelyuvannya: monohrafiya / O.H. Dodonov, V.P. Horbulin, D.V. Lande. – K.: Intertekhnolohiya, 2009. – 164 s.
6. Kopylov V.A. Ynformatsyonnoe pravo /V.A. Kopylov. – M. : Yuryst, 2002 – s. 122.
7. Kryukov O.I. Informatsiyna bezpeka derzhavy v umovakh hlobalizatsiyi / O. I. Kryukov. // Derzhavne budivnytstvo. - 2007. - № 2. Rezhym dostupu: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12
8. Marushchak A.I. Informatsiyno-pravovi napryamy doslidzhennya problem informatsiynoy bezpeky // Derzhavna bezpeka Ukrainy / A.I. Marushchak. – 2011.
9. Panaryn Y.N. Ynformatsionnaya bezopasnost' / Y.N. Panaryn [Elektronnyy resurs] / Rezhym dostupu: http://panarin.com/info_voina/86-informacionnaya-bezopasnost.html.
10. Sorokivs'ka O. A. Informatsiyna bezpeka pidpryyemstva: novi zahrozy ta perspektyvy [Tekst] / O. A. Sorokivs'ka, V. L. Hevko // Visn. Khmel'nyts. nats. un-tu. Ser.: Ekon. nauky. – 2010. – № 2. – Т. 2. – С. 32–35.
11. Tatsyura M.YU. Problemnii aspekty standartyzatsiyi u haluzi informatsiynoy bezpeky pidpryyemstva // Materialy Druhoyi nauk.-prakt. konf. «Stalyy rozvytok ta ekolohichna bezpeka suspil'stva v ekonomichnykh transformatsiyakh» 23- 24 veresnya 2010 r. m. Bakhchysaray, NDI staloho rozvytku ta pryrodokorystuvannya, RVPS Ukrainy NAN Ukrainy, Kryms'kyy instytut KNEU im. Vadyma Het'mana / M.YU. Tatsyura. – Simferopol': Feniks, 2010. – S. 451–453.
13. Ter-Akopov A.A. Bezopasnost' cheloveka : Teoretycheskye osnovy sotsyal'no-pravovoy kontseptsyy / A.A. Ter-Akopov, Mezhdunar. nezavysymyy ekol.-polytoloh. un-t (MNÉPU). – M. : Yzd-vo MNÉPU, 1998. – 196 s.
14. Tsymbalyuk V. Informatsiyna bezpeka pidpryyemnyts'koyi diyal'nosti: vyznachennya sutnosti ta zmistu ponyattya za umov vkhodzhennya Ukrainy do informatsiynoho suspil'stva (hlobal'ni kibertsyvilizatsiyi) // Pidpryyemnytstvo, hospodarstvo i pravo. – 2004. – № 3. – С. 88-91.

Рецензія/Peer review : 11.04.2018

Надрукована/Printed : 04.06.2018

Рецензент: д. е. н., проф. Лук'янова В. В.