

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА

Правові горизонти



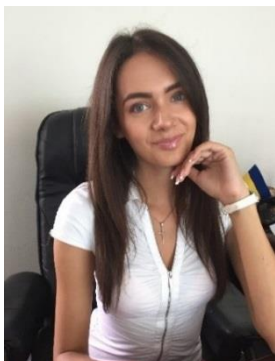
Legal horizons

ВИПУСК 14 (27)

Суми – 2019

DOI: <http://www.doi.org/10.21272/legalhorizons.2019.i14.p75>

КІБЕРБЕЗПЕКА ЯК ФАКТОР ЗАБЕЗПЕЧЕННЯ ЕКОНОМІНОЇ БЕЗПЕКИ⁴



Павленко Богдана Олегівна,
*аспірант, викладач-стажист кафедри адміністративного,
господарського права та фінансово-економічної безпеки,
Навчально-науковий інститут права,
Сумський державний університет*



Рева Максим Валерійович,
*Навчально-науковий інститут права,
Сумський державний університет*

Висока економічна залежність держави, проблеми її внутрішнього та зовнішнього характеру та інші дестабілізуючі фактори стають причинами зниження економічної та, відповідно, національної безпеки. Тому необхідною умовою для нормального стійкого розвитку країни стає забезпечення захисту життєво важливих інтересів громадян, суспільства та держави.

Процес постійної зміни внутрішніх та зовнішніх факторів розвитку національної економіки актуалізує дослідження питання забезпечення економічної безпеки країни в сфері високих технологій. Визначення стану її складових елементів в сьогоdnішніх умовах має важливе значення, оскільки дозволяє своєчасно вжити заходів з організаційно-правового забезпечення економічної безпеки країни.

У цій статті проаналізовано поняття кібербезпеки в системі забезпечення економічної безпеки в державі та суспільстві в цілому. Досліджено правову природу кібербезпеки. Здійснено аналіз положень законодавства, точок зору теоретиків та практиків та визначено його як окремий сектор забезпечення економічної безпеки. Розкрито питання кібербезпеки як поняття тотожне інформаційній безпеці, його функції та правову природу.

Визначено механізм забезпечення безпеки в кіберпросторі та функції і завдання покладені на відповідний орган «Департамент кіберполіції». Проаналізовано роботу вище вказаного органу та виявлено основну проблематику в реформі.

Проаналізовано проблематику та можливі загрози економічній безпеці в секторі кібербезпеки. Визначено проблематику проведення реформування та процес удосконалення системи забезпечення безпеки інформації в кіберпросторі. Визначено зміст понять кіберпростір, кібербезпека та інформаційна безпека. Досліджено небезпеку розповсюдження дезінформації в медіа ресурсах та мережі інтернет загалом, як основної загрози економічній безпеці та підбурення населення до повалення чинної системи та проблематику невизначеності ринку крипто валюти на ринку України як основного чинника економічної небезпеки.

⁴ Робота виконана в рамках проекту № 0118U003582

Ключові слова: кібербезпека, економічна безпека, кіберпростір, інформація, інформаційна безпека, інтернет, медіа ресурси, кіберполіція.

Pavlenko B.O., Reva M.V. Cyber security as a factor to improve economic life. The economic benefits of the economy, the pockets of its internal and external хapatikupu and other deceptive factors give rise to a decrease in the cost of the economy, in other words, to the national level. That non-existent intelligence for the most important part of the life of a person is due to the fact that life is vital to all kinds of people, both social and spiritual.

The process of constant change inside and out of the factors of development of the national economism actuals docling of patients for concerning the examination of the examination of the quality of high technologies. The recognition of the complexity of its cyclical abilities in the contemporary sense of mind is intrinsic to the knowledge, since it makes it possible to use the sources from the op-exoneration of the equivalent emotion of the country.

This article analyzes the concept of cybersecurity in the system of ensuring economic security in the state and society as a whole. The legal nature of cybersecurity is investigated. The analysis of the provisions of the law, points of view of theorists and practitioners has been analyzed and defined as a separate sector of ensuring economic security. The issue of cybercafe as a notion identical to information security, its functions and legal nature is disclosed.

The mechanism of security in the cyberspace is determined and functions and tasks are assigned to the appropriate body of the Department of Cyberpolicies. The article analyzes the above mentioned body and reveals the main problems in the reform.

The problems and possible threats to economic security in the cybersecurity sector are analyzed. The problems of the reformation and the process of improving the information security system in the cyberspace were determined. The content of the concepts of cyberspace, cybersecurity and information security was determined. The danger of dissemination of misinformation in media resources and the Internet in general as a major threat to economic security and incitement of the population to overthrow the current system and the problems of uncertainty of the crypto currency market in the Ukrainian market as the main factor of economic danger is investigated.

Key words: cybersecurity, economic security, cyberspace, information, information security, internet, media resources, cyberpolice.

Висока економічна залежність держави, проблеми її внутрішнього та зовнішнього характеру та інші дестабілізуючі фактори стають причинами зниження економічної та, відповідно, національної безпеки. Тому необхідною умовою для нормального стійкого розвитку країни стає забезпечення захисту життєво важливих інтересів громадян, суспільства та держави.

Процес постійної зміни внутрішніх та зовнішніх факторів розвитку національної економіки актуалізує дослідження питання забезпечення економічної безпеки країни в сфері високих технологій. Визначення стану її складових елементів в сьгоднішніх умовах має важливе значення, оскільки дозволяє своєчасно вжити заходів з організаційно-правового забезпечення економічної безпеки країни. [1,2]

На сьгоднішній день в світ розпочато період високих технологій, а разом з ним і період витоку інформації з електронно обчислювальних машин. 90% всієї інформації у світі зберігається на носіях інформації які мають технічну природу.

Забезпечення належного рівня кібернетичної безпеки стало необхідною умовою розвитку інформаційного суспільства. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру.

У багатьох зарубіжних країнах світу вже створені та загалом сформовані загальнодержавні системи кібернетичної безпеки – як найбільш позитивні організаційні структури, що здатні в короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам.

В Україні також відбувається процес формування системи кібернетичної безпеки. Складову такої системи варто розглядати єдину загальнодержавну систему протидії кіберзлочинності, як складову одиницю такої системи, пропозиції щодо створення якої ще у 2011

році доручалося розробити Кабінету Міністрів України за участю Служби безпеки України.

Відповідно до проведення реформи щодо удосконалення правоохоронних органів, 13 жовтня 2015 року Кабінетом міністрів України було опубліковано постанову №831 «Про утворення територіального органу Національної поліції», а саме Департаменту Кіберполіції підпорядковану Національній поліції України. [3]

До основних функцій які покладено на даний структурний підрозділ можливо віднести:

- визначає, розробляє та забезпечує реалізацію комплексу заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності;

- у межах своїх повноважень уживає необхідних оперативних-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності;

- уживає передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів, у тому числі об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень;

- організує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності;

- проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті;

- забезпечує формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності;

- організує виконання, у межах компетенції, доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях;

В той же час, недосконалість національного законодавства у сфері забезпечення кібернетичної безпеки значно підвищує ймовірність реалізації таких загроз, що негативно впливає на загальний рівень національної та економічної безпеки України.

Правову основу кібернетичної безпеки України становлять Конституція України, закони України "Про основи національної безпеки", "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про Основні засади розвитку інформаційного

суспільства в Україні на 2007–2015 роки" та інші закони, Конвенція Ради Європи про кіберзлочинність [4], інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також видані на виконання законів інші нормативно-правові акти. Необхідно додати, що в секторі інформаційної безпеки України визначено життєво важливі інтереси в економічній сфері.

Побудова інформаційного суспільства в різних країнах світу, глобалізація інформаційних процесів, суттєве зростання ролі інформаційної інфраструктури в різних сферах суспільного життя з одного боку створюють підґрунтя для ефективного економічного розвитку держави, а з іншого дають змогу іншим державам отримати доступ до інформації у зв'язку з малоефективністю захисного програмного забезпечення.

Національна безпека України та її економічне становище все більше залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційними та комунікаційними технологіями, або в більш широкому розумінні - кіберпростором. Водночас, зростання залежності від інформаційно-комунікаційних технологій робить сучасне українське суспільство більш уразливим перед можливими негативними наслідками протиправного використання кіберпростору. В цих умовах головним завданням держави є вжиття заходів, що дозволять принципово зменшити (а подекуди - унеможливити повністю) негативні наслідки від кібератак. [5]

Інформація – це важливий елемент економічної безпеки. Інформація — відомості, знання. Інформація у широкому розумінні — результат відображення одного об'єкта в іншому, що використовується у подальшому для формування управлінських впливів. [6] Це відображення (інформаційна модель) об'єкта. Цільова функція інформації полягає в її здатності впливати на процеси управління. Взаємозв'язок понять "інформація" і "управління" базується на теоретичній аксіомі, відповідно до якої інформація є вираженням якоїсь відмінності. У практичному змісті інформація — це відомості про осіб, предмети, факти, події, явища або процеси безвідносно до форми їхнього подання.

Закон України "Про інформацію" від 2 жовтня 1992 р. визначає, що інформація — це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі. [7]

Інформація завжди відіграла в житті людини дуже велику роль. Але із середини ХХ ст. у результаті соціального прогресу та бурхливого розвитку науки і техніки роль інформації незмірно зросла. У світі відбувається лавиноподібне наростання маси різноманітної інформації, що одержало назву "інформаційного вибуху", який і призвів до зміни трактування поняття "інформація". Один із розповсюджених підходів до трактування поняття "інформація" розглядає інформацію як властивість певного класу матеріальних систем, яка виникає і збагачується у процесі становлення, розвитку цих систем, їхньої взаємодії між собою і зовнішнім середовищем. Інформація є основою для прийняття управлінських рішень.

Серед загроз щодо яких може призвести до настання блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об'єктів підвищеної небезпеки є кібернетична загроза.

Я правильно зауважує В.П. Шеломенцев, в законодавстві відсутнє визначення не тільки поняття "кібернетична безпека (кібербезпека)", а й таке поняття, як "кібернетична загроза (кіберзагроза)". [2]

Проаналізувавши наукові роботи, на мою думку найбільш вдалі визначення надав Діордіца І., а саме:

Кібернетична загроза (кіберзагроза) – наявній потенційно можливі явища та чинники, що створюють небезпеку інтересам людини, суспільства й держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури [8].

Але окрім критичної інфраструктури та кіберзагроз існують безліч видів процедур які «підривають» економічну безпеку країни. Як ми знаємо на сьогоднішній день у світі набувають розвитку та закріплення на законодавчому рівні такого терміну як «криптовалюта». На сьогоднішній день їх налічують близько 60 одиниць.

Як зауважив начальник Департаменту кіберполіції Демедюк С.В. [9], коментуючи виступ Турчинова А.В. що правовий вакуум на ринку криптовалют через відсутність в Україні відповідної законодавчої і нормативної бази "створює загрози для економіки та безпеки

держави" так як набирає обертів створення фішингових сайтів з обміну криптовалютою. Так люди та держава втрачають величезні кошти. Відсутня оперативна допомога через не визначений статус криптовалют. В Україні вони не заборонені і не дозволені. Важко встановити склад злочину через відсутність механізму верифікації власника криптогаманця та не можливість контролювати обігу коштів. Таким чином тіньова економіка країни одразу перейшла до системи розрахунку крипто валютою.

Також основним напрямком кібербезпеки є подолання дій іноземних спецслужб спрямованих на дестабілізацію економічної обстановки та безпеки в Україні. Для цього було створено спеціальні відділи інформаційно-аналітичної роботи з питань кібербезпеки в Департаменті кіберполіції та Службі безпеки України дії яких спрямовані на усунення ресурсів дезінформування та припинення інформаційної війни.

Не менш небезпечним, ніж шпигунство і тероризм, явищем є інформаційна дія спецслужб іноземних держав на українських радикально налаштованих громадян. На сьогодні інформаційна війна – це вже безпосередньо війна цивілізацій, це зіткнення різних базових цілей, знань, теорій [10]. Наприклад пропаганда у медіа просторі віртуальних переваг російської держави та хибне представлення українських реалій стало однією з причин втрати Україною Автономної Республіки. [11].

Висновки. Отже кібербезпека являється одним з найважливішим чинником який забезпечує економічну безпеку країни та громадян. На жаль даний напрямок потребує удосконалення, так як на даному етапі в Україні на приблизно 80 % відсутня інформація про рух коштів, ідентифікація персональних даних, номерів телефонів, банківських рахунків. Відсутня взаємодія об'єктів критичної інфраструктури та органів поліції, а інформація яка міститься в електронно-інформаційному вигляді в державних установах та інших об'єктах які мають економічне важливе значення кожного дня піддається хакерським атакам або витоку за допомогою віддалено доступу. Не менш важливе є удосконалення контролю медіа - обігу серед користувачів мережі Інтернет. Дезінформація та пропаганда певних цілей серед мережі, в якій користується кожний третій громадянин країни, являється основною загрозою економічної безпеки держави і не тільки.

Література :

1. Сак Т.В. Економічна безпека України: поняття, структура, основні тенденції / Т.В. Сак // Інформаційні технології та економічна безпека. – 2013. – № 6. – С. 330-340
2. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312–320.
3. Постанова Кабінету міністрів України № 831 від 13.10.2015 «Про утворення територіального органу Національної поліції» // [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF>
4. Конвенція про кіберзлочинність // [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/994_575
5. Стратегія забезпечення кібернетичної безпеки України/ Проект/ Національний інститут стратегічних досліджень// [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf
6. Економічна безпека: навч. посіб. / О. Є. Користін, О. І. Барановський, Л. В. Герасименко та ін.; за ред. О. М. Джужі. — К.: Алерта; КНТ ; Центр учбової літератури, 2010. — 368 с. [Електронний ресурс] – Режим доступу до ресурсу: https://pidruchniki.com/17910211/ekonomika/organizatsiya_diyalnosti_dsbez_schodo_protidiyi_ekonomichniy_zlochinnosti
7. Закон України «Про інформацію» від 02.10.1992, / Документ 2657-ХІІ, чинний, поточна редакція — Редакція від 01.01.2017, підстава - 1774-VIII/ [Електронний ресурс]. – Режим доступу : <http://zakon.rada.gov.ua/laws/show/2657-12>
8. Глава кіберполіції України виступає за врегулювання статусу крипто валют / [Електронний ресурс]. – Режим доступу : <https://gordonua.com/ukr/news/money/glava-kiberpolitsiji-ukrajini-vistupaje-za-vreguljuvannja-statusu-kriptovaljut-227123.html>
9. Інформаційна війна як форма ведення інформаційного протиборства [Електронний ресурс]. – Режим доступу: http://pidruchniki.ws/1212012436972/politologiya/informatsiyana_viyana_forma_vedennya_informatsiyного_protiborstva
10. Лейст О. Э. Сущность права. Проблемы теории и философии права Лейст О. Э. - М. : «ИКД Зерцало-М», 2002. - 288 с.
11. Інформаційна війна як форма ведення інформаційного протиборства [Електронний ресурс]. – Режим доступу: http://pidruchniki.ws/1212012436972/politologiya/informatsiyana_viyana_forma_vedennya_informatsiyного_protiborstva