3. Кісіль М.І. Про необхідність усунення міжгалузевих диспропорцій з метою інвестиційного забезпечення розвитку сільського господарства // Наукові праці КНТУ: Економічні науки. – Кіровоград : КНТУ, 2004. – Вип. 6. – С. 226-233.
4. Матеріали Прес-служби Мінагрополітики [Електронний ресурс]. – Режим доступу : http://minagro.gov.ua/uk/node/2888.
5. Офіційний сайт Київської обласної ради [Електронний ресурс] – Режим доступу : http://kor.gov.ua/node/5802.
6. Саблук П.Т. Структурно-інноваційні зрушення в аграрному секторі України як фактор його соціально-економічного зростання / П.Т. Саблук // Економіка АПК. – 2004. – № 6. – С. 3-9.
7. Статистичний щорічник України в цифрах у 2011 році / Державний комітет статистики України ; за ред. О.Г. Осауленка – Київ, 2012. – 250 с.
8. Статистичний щорічник Київської області за 2011 рік / Державний комітет статистики України ; за ред. С.І. Коханчук. – Київ, 2012. – 503 с.

УДК 330:004

Діброва О.В.
аспірант кафедри економічної кібернетики та маркетингу
Київського національного університету технологій та дизайну

АНАЛІЗ ІНФОРМАЦІЙНОГО ПРОСТОРУ НА МІЖНАРОДНІЙ АРЕНІ ТА В УКРАЇНІ

Стаття присвячена аналізу стану інформаційного простору в Україні у сучасних умовах глобальної інформатизації держави та суспільства. Досліджуються взаємозв'язок та вплив формування інформаційного простору, а саме його такої складової, як інформаційна безпека на сферу економіки. Детально розглядається динаміка кіберзлочинності у світі та в Україні. Також у статті розглянуто основні проблеми сучасного інформаційного простору України. Обґрунтовується необхідність здійснення реформ у сфері інформатизації держави задля покращення економічного добробуту та підвищення рівня конкурентоспроможності національної економіки.
Ключові слова: інформаційна безпека, безпека інформації, вплив інформаційної безпеки на економіку, динаміка кіберзлочинності, правове регулювання інформаційної безпеки, інформаційний простір.

Диброва О.В. АНАЛИЗ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА НА МЕЖДУНАРОДНОЙ АРЕНЕ И В УКРАИНЕ
Статья посвящена анализу состояния информационного пространства в Украине в современных условиях глобальной информатизации государства и общества. Исследуются взаимосвязь и влияние на формирование информационного пространства, а именно его такой составляющей, как информационная безопасность на сферу экономики. Подробно рассматривается динамика киберпреступности в мире и в Украине. Также в статье рассмотрены основные проблемы современного информационного пространства Украины. Обосновывается необходимость осуществления реформ в сфере информатизации государства для улучшения экономического благосостояния и повышения уровня конкурентоспособности национальной экономики.
Ключевые слова: информационная безопасность, безопасность информации, влияние информационной безопасности на экономику, динамика киберпреступности, правовое регулирование информационной безопасности, информационное пространство.

Dibrova O.V. ANALYSIS OF THE INFORMATION SPACE ON THE INTERNATIONAL STAGE AND IN UKRAINE
The article analyzes the state of information space in Ukraine in modern conditions of global informatization of society and of the state. Researched the relationship and influence on the information space, namely its following part as information security in the sphere of economy. Regarded in details dynamics of cybercrime in the world and in Ukraine. Also the article analyzes the main problems of modern Ukraine's information space. Considered the necessity of reforms in informatization area of the state to improve the economic prosperity and improve the competitiveness of the national economy.
Keywords: information security, information security, information security impact on the economy, dynamics of cybercrime, legal regulation of information security, information space.

Постановка проблеми. Головною тенденцією розвитку світу та суспільства у сучасних умовах є широка інформатизація усіх сфер діяльності як держави, так і окремих підприємств та людини. В умовах стрімкого розвитку інформаційних технологій категорія «інформація» перестає бути суто технічною чи філософською. Інформація відтепер досить часто є категорією економічною – товаром, а також важелем впливу як на сферу економіки, так і на інші сфери діяльності. Проте формування інформаційного простору відбувається набагато повільніше ніж впроваджуються в повсякденне життя новітні інформаційні технології та розробки. Але інформаційний простір є дуже важливим для держави і має бути пріоритетним у питаннях державної політики після державної незалежності, адже інформаційний простір є ключем до економічного добробуту. А тому виникає гостра необхідність у забезпеченні інформаційної безпеки на всіх рівнях: від національного до безпеки окремої особи.

Аналіз останніх досліджень і публікацій. Вітчизняними науковцями В.О. Бондаренко, О.В. Литвиненко було сформульовано основні цілі політики інформаційної безпеки та напрями забезпечення інформаційної безпеки. В.А. Ліпкан досліджує інформаційну безпеку як складову національної безпеки та її нормативно-правове забезпечення. О.В. Карпенко розглянуто проблеми сучасного функціонування інформаційної політики у контексті національної безпеки. О.В. Соснін дослідив інформаційну політику України та проблеми правового регулювання. В. Хімей розглянув основні проблеми інформаційної безпеки в Україні та визначив головні негативні чинники, які впливають на інформаційний простір України. А зарубіжними науковцями, такими як Лоуренс А. Гордон, Мартін П. Лоеб, Алессандро Акісті, Брюс Шнайер та Росс Андерсон охарактеризовано економічну необхідність у забезпеченні інформаційної безпеки. Зокрема, оцінено необхідність інвестицій у сферу інформаційної безпеки підприємства та висунуто

тезу, згідно з якою більшість проблем безпеки належать не до технічної сфери, а до економічної.

Постановка завдання. На основі викладеного та беручи до уваги швидкі темпи розвитку інформаційних технологій і доволі повільний розвиток засобів та механізмів забезпечення інформаційної безпеки, варто проаналізувати особливості інформаційного простору та його впливи на сферу економіки, а отже, можна сформулювати дослідження, яке полягає в аналізі сучасного стану інформаційної безпеки, визначенні поняття інформаційної безпеки та її рівнів, дослідженні динаміки кіберзлочинності та її впливу на економічну сферу діяльності як держави, так і підприємств та громадян, і проаналізувати діяльність держави щодо створення умов для розвитку інформаційного простору та забезпечення захисту від інформаційних впливів, які можуть нашкодити.

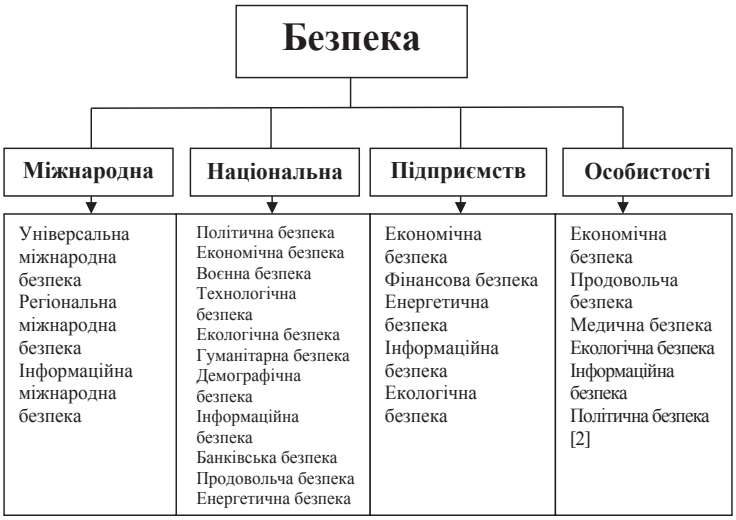

Рис. 1. Види безпеки

Виклад основного матеріалу дослідження. В умовах глобалізаційних процесів та щодня зростаючого впливу інформаційних технологій на формування інформаційного простору на міжнародній арені та в Україні питання інформаційної безпеки постає на першому місці, адже інформація стає однією із головних категорій, що впливають практично на всі сфери діяльності держави: від політики до економіки та культури. Тому важливими на цей час є питання, що належать до інформаційної сфери та їх впливи на економіку. Розглянемо детальніше поняття інформаційної безпеки.

Об'єктами інформаційної безпеки можуть бути: свідомість, психіка людей; інформаційні системи різного масштабу і різного призначення. До соціальних об'єктів інформаційної безпеки звичайно відносять особистість, колектив, суспільство, державу, світове товариство [1].

Найчастіше інформаційну безпеку визначають як різновид соціальної діяльності, який полягає у створенні державними і недержавними інституціями необхідних умов для розвитку національних інтересів в інформаційній сфері.

Інформаційна безпека є складовою загальної проблеми інформаційного забезпечення розвитку людини, держави і суспільства. Вона орієнтована на захист важливих об'єктів інформаційних ресурсів, законних інтересів [1, с. 18].

Розглядаючи класифікацію безпеки на рисунку 1, ми бачимо, що управління інформаційною безпекою здійснюється на кожному із рівнів: на міжнародному, національному, рівні підприємства та особи, що ще раз доводить про широкі масштаби інформатизації сучасного світу.

Міжнародна інформаційна безпека визначається як взаємодія учасників міжнародних відносин з операції підтримання сталого миру на основі захисту міжнародної іоносфери (кіберпростору разом із засобами масової інформації), глобальної інфраструктури та суспільної свідомості світової спільноти від реальних інформаційних загроз [2].

Інформаційна безпека як складова національної безпеки – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [3].

Інформаційна безпека як складова безпеки підприємства – це захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Крім того, під інформаційною безпекою розуміють захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може виявитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктури [4].

Інформаційна безпека як складова особистої безпеки особи характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору [5].

Але інформаційна безпека у сучасних умовах – це не лише забезпечення безпеки інформації, яка міститься чи зберігається на електронних носіях, серверах чи персональних пристроях. Це також раціональна інформаційна політика на рівні держави та підприємства, що не порушує обмежує законних прав людини і громадянина на доступ до інформації, але й у свою чергу регулює інформаційні відносини.

В Україні регулювання інформаційної безпеки на державному рівні здійснюється за допомогою наступних нормативно-правових актів: Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», Закон України «Про інформацію», Закон України «Про Національну програму інформатизації», Указ Президента України «Про Доктрину інформаційної безпеки України», Концепція національної безпеки України та Конституція України.

Чинне правове підґрунтя має доволі розвинений характер, адже більшість нормативно-правових актів відповідають міжнародним стандартам, принципам і нормам забезпечення прав громадян на свободу слова, отримання та розповсюдження інформації. Але водночас нормативно-правова база у сфері інформаційної безпеки вимагає вдосконалення [6, с. 16]. Також інформаційна безпека регулюється рядом наступних міжнародних стандартів та норм: CoBiT (Control Objectives for Information and Related Technology),

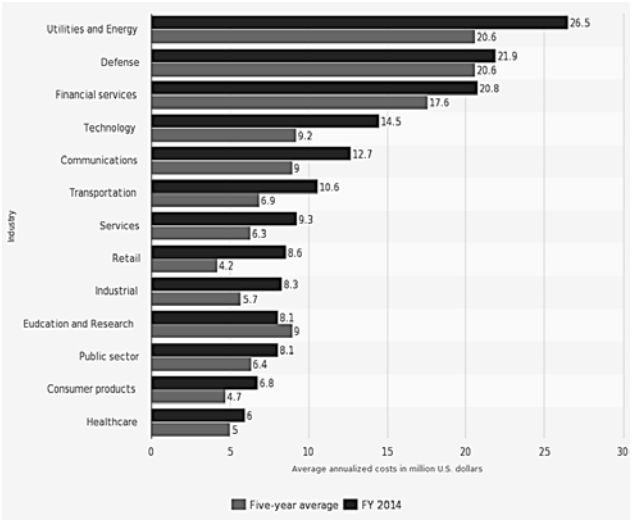

Рис. 2. Середньорічні витрати, пов'язані з кіберзлочинністю, у США за 2014 рік (у млн дол. США) [10]

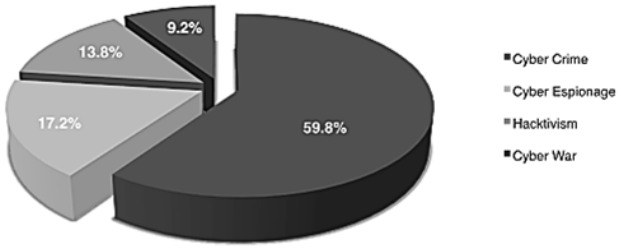

Рис. 3. Мотиви скоєння кіберзлочинів у США за 2014 рік [10]

Top 15 der Ursprungsländer von Angriffen (2014-05)

	Quelle	Anzahl
	Russische Föderation	6.910.798
	China	3.247.727
	Vereinigte Staaten	930.059
	Deutschland	510.708
	Kanada	140.597
	Taiwan	113.441
	Palästinensische Gebiete	97.421
	Australien	96.623
	Frankreich	95.502
	Spanien	66.259
	Republik Korea	58.251
	Brasilien	45.230
	Vereinigtes Königreich	43.768
	Polen	39.705
	Japan	36.108

Top 15 der Ursprungsländer von Angriffen (2014-10)

	Quelle	Anzahl
	Russische Föderation	2.792.403
	Deutschland	1.427.451
	Vereinigte Staaten	1.230.475
	China	1.072.880
	Vietnam	793.615
	Frankreich	480.791
	Rumänien	420.216
	Taiwan	352.219
	Vereinigtes Königreich	203.092
	Niederlande	160.072
	Venezuela	147.887
	Australien	122.199
	Ukraine	116.182
	Litauen	86.941
	Indonesien	85.702

Рис. 4. Динаміка зміни країн за кількістю вихідних з країни кібер за травень та вересень 2014 року відповідно [8]

ITIL (Information Technology Infrastructure Library), ISO/IEC 27001:2005, ISO/IEC 17799, ISO/IES 15408.

Проте механізми управління інформаційною безпекою відстають у розвитку від сучасного рівня інформатизації, що сприяє зростання рівня кіберзлочинності, яка спричиняє серйозні, а іноді й незворотні наслідки для держави, підприємства, суспільства, особи. У глобальному плані спостерігається широкий діапазон кіберзлочинів, які включають злочини, що здійснюються в цілях отримання фінансової вигоди, злочини, пов'язані з використанням інформації, яка міститься у комп'ютері, а також злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних систем [7, с. 8].

Боротьбу з кіберзлочинністю регулює Будапештська Конвенція, згідно з якою виділяють такі види кіберзлочинів:

1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (так звані «CIA-злочини»), зокрема: незаконний доступ, нелегальне перехоплення комп'ютерних даних; втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;втручання у систему, включаючи навмисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру; зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу з метою здійснення «CIA-злочинів» [10];

2. Правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, здійснені з використанням комп'ютерів [10];

3. Правопорушення, пов'язані зі змістом інформації [10].

4. Правопорушення, пов'язані з порушенням авторських і суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг [10].

Розглянемо статистику скоєння кіберзлочинів у США за 2014 рік за галузями промисловості на рисунку 2.

Як бачимо з наведеного рисунку, найбільше збитків отримують у сфері комунальних послуг та енергії (utilities and energy), оборони (defense) та фінансових послуг (financial services).

На рисунку 3 зображено статистику основних мотивів скоєння злочинів, повязаних з інформацією.

З рисунку 4 ми бачимо, що основними мотивами скоєння злочинів, повязаних з інформацією

є саме кіберзлочинність у 59,8% зафіксованих випадків, та кібершпигунство в 17,2% випадків, хакерство 13,8%, а лише 9,2% це ведення кібервійни.

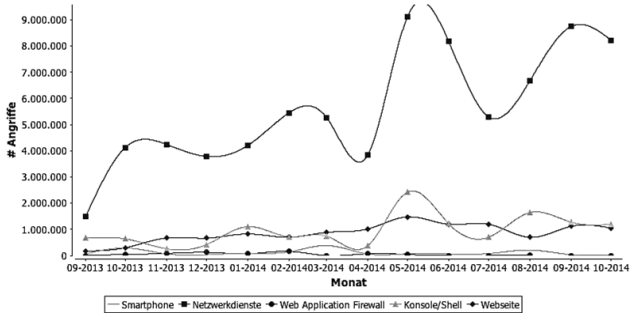

Рис. 5. Розподіл за типами атак за 2013 та 2014 роки [8]

З рисунку видно, що найбільша кількість атак здійснюється за допомогою мережевих служб (Netzwerkdienste).

Пояснити таке стрімке зростання рівня кіберзлочинності можливо швидкими темпами впровадження інформаційних технологій у повсякденне життя та усі сфери діяльності держави, наприклад впровадження електронного документообігу. У такому випадку викрадення чи пошкодження інформації може спричинити збитки, що можуть у кілька разів перевищити вартість самої інформації.

У 2012 році компанія Symantec представила доповідь «2012 Norton Cybercrime Report», у якій були опублікувані результати щорічного дослідження за статистикою кіберзлочинів, скоєних щодо користувачів.

Представлені дані показують, що понад 31 млн росіян стали жертвами, а кожну секунду в світі відбувається в середньому 18 кіберзлочинів, а в усьому світі за минулий рік число жертв досягло 556 млн. Загальний збиток користувачів від кіберзлочинів фахівці оцінили в 110 млрд дол, з них в Росії – близько 2 млрд дол. Збитки від кіберзлочинності наведені у таблиці 1.

Таблиця 1

Збитки від кіберзлочинності

	У світі (по 24 країнам)
Загальні чисті втрати / збиток від кіберзлочинів за останні 12 місяців	US $110 млрд
Середній збиток від одного кіберзлочину за останні 12 місяців	US $197

Отже, ми бачимо, що головною «жертвою» кіберзлочинності є сфера економіки. Економічні наслідки в інформаційному просторі досить важко підрахувати, тому що за розслідуванням таких випадків звертається лише третина постраждалих, а також тому що відсутні механізми оцінки фактичних наслідків та ймовірних наслідків певних інформаційних загроз та інформаційних впливів. За даними Ради Європи, шахрайство з кредитними картками обходиться в 400 млн дол. збитків щорічно, віруси за той же час спричиняють збитків на 12 млн дол., а прибутки від незаконного використання патентів та торгових марок складають 250 млн дол., що становить 5% від обсягів світової торгівлі [9].

На відміну від світової спільноти в Україні детальна інформація щодо динаміки кіберзлочинів та рівня збитків від таких злочинів практично відсутня, що свідчить про недостатню увагу цим питанням з боку держави. Але навіть з тими наявними даними можливо зробити висновок, що збитки від злочинів, пов'язаних з інформацією, збільшуються.

Так, за інформацією НБУ України, за 2012 р. загальна кількість шахрайських операцій з платіжними картами в нашій країні зросла відразу на 47% і з 35 до 57 збільшилася кількість банків, з рахунків яких пропали кошти. А станом на 1 жовтня 2013 року в Україні перебуває в обігу 68,1 млн платіжних карток, з яких 33,9 млн карток є активними. При цьому сума операцій, проведених з використанням платіжних карток, за 9 місяців 2013 року становить близько 650,0 млрд грн [6].

Висновки з проведеного дослідження. З наведеного вище можна зробити наступні висновки. Для активного формування, розвитку та захисту національного інформаційного простору й ресурсів мають використовуватися адекватні методи і засоби, які базуються на відповідних сучасних інформаційних та інформаційно-аналітичних технологіях, яким на сьогодні приділяється мало уваги на державному рівні.

Нинішня ситуація в Україні за умов недосконалої інформатизації та затримки з вирішенням проблем інформаційної безпеки та негативних інформаційних впливів призводить до величезних збитків, падіння економічного розвитку та конкурентоспроможності на світовому ринку. Для запобігання цьому необхідне як міжнародне співробітництво, зумовлене відсутністю досвіду розв'язання питання щодо створення сучасного інформаційного простору в Україні та системи його захисту, так і раціональні реформи у сфері інформатизації та інформаційної політики держави в цілому.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. – К. : КНТ, 2006. – 280 с. (Серія: Національна і міжнародна безпека).
2. Кашпрук Н Міжнародна інформаційна безпека як актуальна проблема сучасності [Електронний ресурс]. – Режим доступу : http://naub.org.ua/?p=1050.
3. Закон України про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки // Відомості Верховної ради України. – 2007. – № 12. – С. 511.
4. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия : учебное пособие. 2-е изд. – М. : Издательско-торговая корпорация «Дашков и К°». – 2005. – 336 с.
5. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки [Електронний ресурс]. – Режим доступу : http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.
6. Баринов А. Информационный суверенитет или информационная безопасность? // Національна безпека і оборона. – 2001. – № 1. – С. 70-76
7. Державна служба фінансового моніторингу України [Електронний ресурс]: Кіберзлочинність та відмивання коштів. – Режим доступу : www.minfin.gov.ua/file/link/396800/file/tipolog2013.pdf.
8. Deutche Telekom [Електронний ресурс]: віртуалізована карта країн –джерел кібератак. – Режим доступу : http://sicherheitstacho.eu/?lang=de.
9. Рада Європи [Електронний ресурс]: шахрайство з кредитних карток. – Режим доступу : www.coe.int.
10. Конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/994_575.