

УДК 338.24

ОЛЬШАНСЬКА О.В.

Київський національний економічний університет
ім. В. Гетьмана

ОСНОВНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЇЇ СТАН В СУЧАСНИХ УМОВАХ РОЗВИТКУ В УКРАЇНІ

Мета. Дослідження та огляд основних положень управління інформаційною безпекою в сучасних умовах.

Методика. Використані наступні загальновідомі методи аналізу та синтезу, метод дедукції та порівняння.

Результати. В роботі проаналізовано стан інформаційної безпеки в Україні.

Наукова новизна. Досліджено поняття інформаційної безпеки сто совно економіки та розглянуто рекомендації, щодо покращення управління інформаційною безпекою.

Практична значимість. Раціональне управління інформаційною безпекою сприяє зростанню рівня конкурентоспроможності країни на світовому ринку, а також зростанню економічного потенціалу держави.

Ключові слова: інформаційна безпека, управління інформаційною безпекою, інформаційні впливи.

Вступ. Рівень сучасних технологій та виробництв сприяє стрімкій глобалізації та розвитку інформаційних та комунікаційних технологій, що у свою чергу налагоджує процес міжнародної співпраці у різних сферах. Проте виникає велика кількість загроз та зростає потреба забезпечення інформаційної безпеки.

Актуальність цієї теми обумовлена тим, що в сучасних умовах саме розвиток інформаційних технологій та рівень інформаційної безпеки будуть визначати місце держави на міжнародній арені. Що також є важливим, це те, що найближчим часом залежність всіх сфер діяльності суспільства та держави від інформаційних систем буде тільки зростати і вимагати підвищення якості новітніх технологій.

Питання забезпечення інформаційної безпеки як складової національної безпеки та безпеки підприємства у техніко-економічному контексті розглядають зарубіжні та вітчизняні вчені. Це: Данільян О.Г., Гурковський В.І., Литвиненко О.В., Дзьобань О.П., Панов М.І.Харченко Л.С., Левченко Є.Г., Швець В.А., Демчишин М.В., Ross Anderson, Bruce Schneier, Лоуренс А. Гордон, Мартін П. Лоеб, Алессандро Акісті та багато інших.

У своїх роботах вони здебільшого приділяють увагу таким питанням як: безпека комп'ютерних та інформаційних систем; забезпечення міжнародної інформаційної безпеки; забезпечення інформаційної безпеки держави та підприємств; ефективність інформаційної безпеки. Проте невирішеними залишаються питання зв'язку інформаційної безпеки та економіки, а саме: вплив інформаційних факторів на розвиток економіки.

Постановка завдання. Стрімка глобалізація суспільства сприяє зростанню значення інформаційної безпеки як для міжнародної спільноти, держави в цілому, так і окремо для секторів економіки, для підприємств та особистості. А в умовах розвитку економіки знань на

пріоритетні позиції виходять наукоємні виробництва та інформаційні технології, що складають пріоритетний сектор розвитку економіки, який в при раціональному регулюванні може вивести державу на якісно новий рівень розвитку.

Результати дослідження. Сьогодні інфомація перестала бути лише технічною категорією. Впровадження та поповсюдження новітніх технологій посприяло тому, що інформація перетворилася на економічну категорію, стала одним з найважливіших елементів ринку та фактором, що регулює рівень розвитку не тільки виробництв, а й економіки загалом, адже переважна більшість економічних звязків набувають форми обміну інформацією. У ринковій економіці інформація стає товаром і її отримання, збереження, передача та використання повинні підпорядковуватися законам товарно-грошових відносин, тобто інформація стає об'єктом та інструментом управління. Інформаційні впливи можуть спричиняти результат не відразу, а через тривалий час. Визначальним фактором життєдіяльності сучасного суспільства стає глобалізація інформаційних ресурсів. Тому важливими на цей час є питання, що належать до інформаційної сфери та їх впливи на економіку.

А отже виникає необхідність забезпечення та регулювання інформаційної безпеки різних сфер діяльності. Найчастіше інформаційну безпеку визначають як різновид соціальної діяльності, який полягає в створенні державними і недержавними інституціями необхідних умов для розвитку національних інтересів в інформаційній сфері.

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].

На рисунку 1 наведено види безпеки та рівні на яких здійснюється управління інформаційною безпекою.

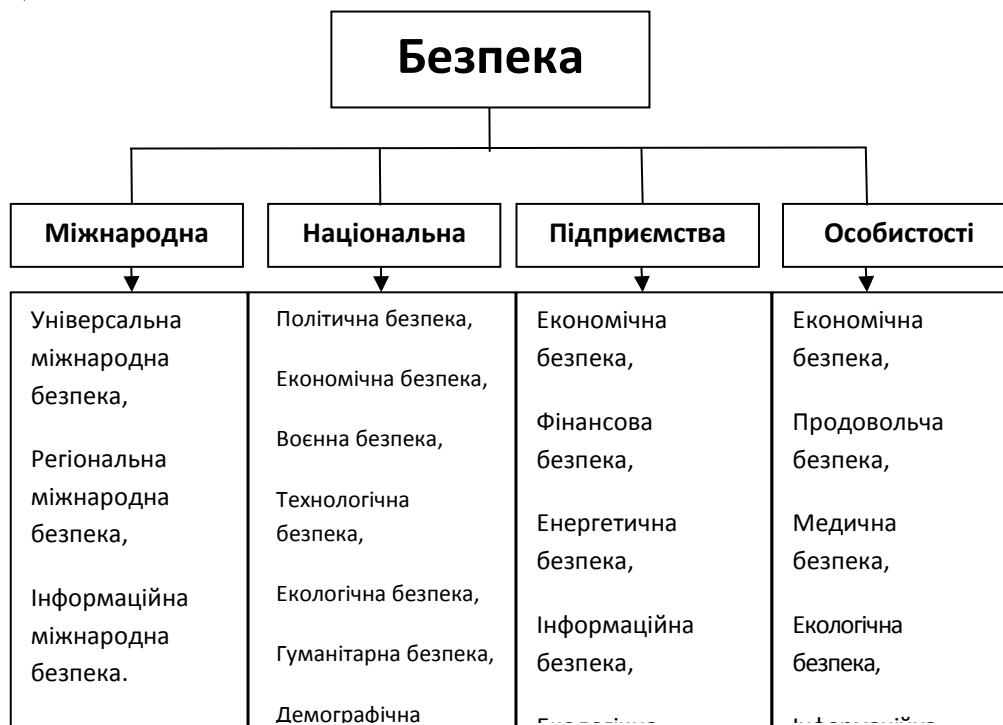


Рис.1. Види безпеки

Міжнародна інформаційна безпека - характеризується, як взаємодія учасників міжнародних відносин для підтримання тривалого миру на основі захисту світового кіберпростору разом із засобами масової інформації, глобальної інфраструктури та суспільної свідомості від реальних інформаційних загроз [2].

Інформаційна безпека, як складова національної безпеки - стан захищеності життєво важливих інтересів людини, суспільства і держави, коли 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 - діяльність керівництва підприємства з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує нормальне функціонування розвитку підприємства [3].

Інформаційна безпека, як складова особистої безпеки особи - характеризується як стан захищеності особистості, 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 [3].

Але інформаційна безпека на сьогодні це не лише забезпечення безпеки інформації, яка зберігається на електронних носіях, серверах чи персональних пристроях. Це, перш за все, раціональна інформаційна політика на рівні держави та підприємства, що не обмежує прав людини і громадянина на доступ до інформації, але й у свою чергу якісно виконує свої регулюючі функції у сфері інформаційних відносин.

В Україні регулювання інформаційної безпеки здійснюється за допомогою таких 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. Також інформаційна безпека регулюється рядом наступних міжнародних стандартів та норм: CoBiT (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library), ISO/IEC 27001:2005, ISO/IEC 17799, ISO/IEC 15408.

Варто зазначити, що механізми управління інформаційною безпекою суттєво відстають у розвитку від сучасного рівня інформатизації, що сприяє зростанню рівня кіберзлочинності, яка у свою чергу спричиняє важкі, 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 в комп'ютері, а також злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних систем [5, с. 8].

Також слід зазначити, що головною сферою кіберзлочинності є економіка.

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.

Наприклад, за даними Ради Європи шахрайство з кредитними картками коштує близько 400 млн. дол. збитків щорічно, тоді як вірусні загрози 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 [10]. На рисунках 2 та 3 наведено статистику скоєння кіберзлочинів у США за 2014 рік за галузями промисловості та статистику основних мотивів скоєння злочинів, пов'язаних з інформацією. Розглянемо їх детальніше.

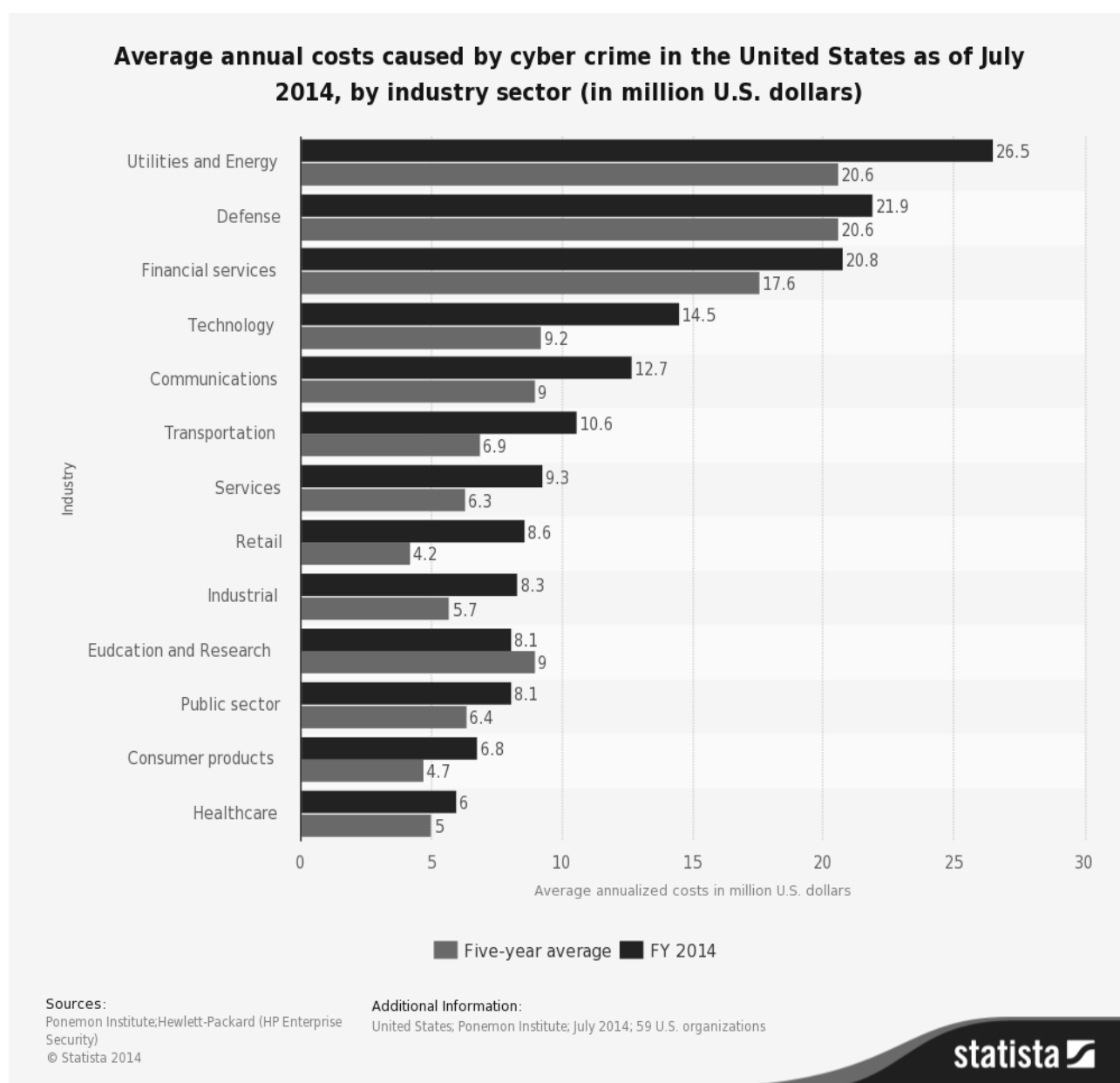


Рис.2. Середньорічні витрати, пов'язані з кіберзлочинністю в США за 2014 рік (в млн. дол. США) [8]

Як бачимо з наведеного рисунку найбільше збитків отримують у сфері комунальних послуг та енергії (utilities and energy), оборони (defense) та фінансових послуг (financial services), а найменше у медичній сфері (healthcare) та роздрібній торгівлі (retail).

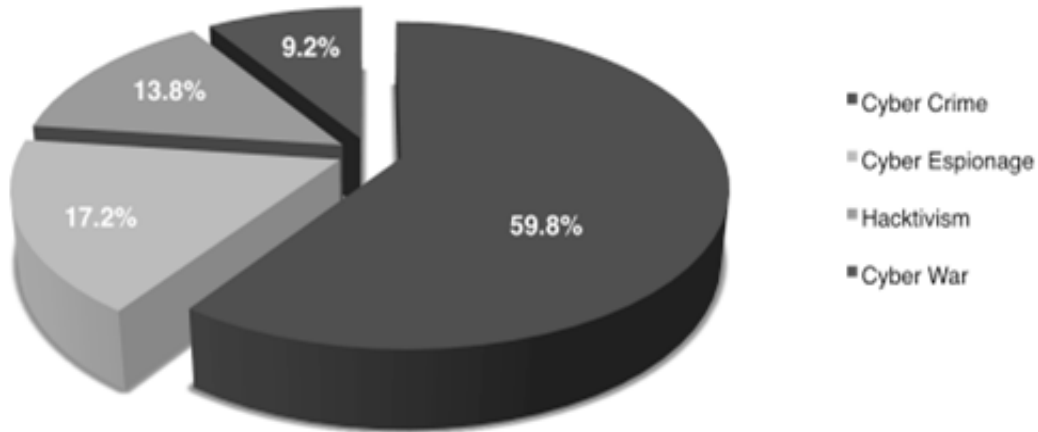


Рис.3. Мотиви скоєння кіберзлочинів в США за 2014 рік [8]

Як можемо бачити, основними мотивами скоєння злочинів, пов'язаних з інформацією є саме кіберзлочинність, у 59,8% зафіксованих випадків, та кібер шпигунство в 17,2% випадків, хакерство 13,8%, а лише 9,2 % це ведення кібервійни.

На жаль, в Україні інформація щодо динаміки кіберзлочинів та рівня збитків від таких злочинів практично відсутня в статистичній інформації, що свідчить про недостатню увагу, якак приділяється питанням інформаційної безпеки з боку держави. Але навіть з тими наявними даними можливо зробити висновок, що кількість злочинів та збитки від злочинів пов'язаних з інформацією постійно збільшуються.

Згідно з 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 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 [9].

Висновки. В умовах глобалізаційних процесів та щохвилини зростаючому впливу інформаційних технологій на формування інформаційного простору на міжнародній арені та в Україні питання інформаційної безпеки постає на першому місці, адже інформація дійсно стала однією з 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. Для активного формування, розвитку та захисту національного інформаційного простору та ресурсів мають використовуватися адекватні методи і засоби, які базуються на відповідних сучасних 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.

Список використаних джерел

1. Політична наука в Україні: стан і перспективи: матеріали всеукраїнської наукової конференції (Львів, 10-11 травня 2007 року) /Укл. Поліщук М., Скочиляс Л., Угрин Л. – Львів, ЦПД, 2008. - 308 с.
2. Кашпрук Н Міжнародна інформаційна безпека як актуальна проблема сучасності. [Електронний ресурс]. – Режим доступу: <http://naub.org.ua/?p=1050>
3. Сашук Г. Інформаційна безпека в системі забезпечення національної безпеки [Електронний ресурс]. – Режим доступу: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php
4. Борисенко П.А. Методичні підходи до визначення поняття „наукоємне виробництво” (на прикладі авіаційної промисловості)//Схід. – 2008. – №4. – с.27;
5. Державна служба фінансового моніторингу України [Електронний ресурс]: Кіберзлочинність та відмивання коштів Режим доступу: www.minfin.gov.ua/file/link/396800/file/tipolog2013.pdf
6. Україна у цифрах у 2013 році: статистичний збірник/ [за ред. О.Г. Осауленка]. –К. : Державний комітет статистики України, 2014. – 239 с
7. Обсяг виконаних наукових та науково-технічних робіт [Електронний ресурс]. – Режим доступу: <http://www.ukrstat.gov.ua>
8. Конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу:
9. http://zakon1.rada.gov.ua/laws/show/994_575
10. Баринов А. Информационный суверенитет или информационная безопасность? // Национальная безопасность и оборона. – 2001. – № 1. – С. 70-76
11. Рада Європи [Електронний ресурс]: шахрайство з кредитних карток. – Режим доступу: www.coe.int

ОСНОВНЫЕ ПОЛОЖЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ СОСТОЯНИЕ В СОВРЕМЕННЫХ УСЛОВИЯХ РАЗВИТИЯ В УКРАИНЕ

ОЛЬШАНСКАЯ О.В.

Киевский национальный экономический университет им. Вадима Гетьмана

Цель. Исследования и обзор основных положений управления информационной безопасностью в современных условиях.

Методика. Используются следующие общеизвестные методы анализа и синтеза, метод дедукции и сравнения.

Результаты. В работе проанализировано состояние информационной безопасности в Украине.

Научная новизна. Исследовано понятие информационной безопасности относительно экономики и рассмотрены рекомендации по улучшению управления информационной безопасностью.

Практическая значимость. Рациональное управление информационной безопасностью способствует росту уровня конкурентоспособности страны на мировом рынке, а также росту экономического потенциала государства.

Ключевые слова: информационная безопасность, управление информационной безопасностью, информационные воздействия.

MAIN PROVISIONS OF OF INFORMATION SECURITY AND ITS STATE IN MODERN CONDITIONS OF DEVELOPMENT IN UKRAINE

OLSHANSKA O.

Kiev National Economics University named after Vadym Hetman

Purpose. Research and overview of the main provisions of information security management in modern conditions.

Methodology. Used the known methods of analysis and synthesis, the method of deduction and comparison.

Findings. The paper analyzes the state of information security in Ukraine.

Originality. Explored the concept of information security on the economy and reviewed recommendations for improving information security management.

Practical value. The rational management of information security promotes the growth of a country's level of competitiveness in the global market and increase the economic potential of the state.

Key words: *information security, information security management, information exposure.*