Scientific journal
PHYSICAL AND MATHEMATICAL EDUCATION
Has been issued since 2013.

Науковий журнал
ФІЗИКО-МАТЕМАТИЧНА ОСВІТА
Видається з 2013.

ISSN 2413-158X (online)
ISSN 2413-1571 (print)

http://fmo-journal.fizmatsspu.sumy.ua/

Безуглий Д.С. Інформаційна безпека України: огляд останніх тенденцій. Фізико-математична освіта. 2018. Випуск 2(16). С. 13-17.

Bezuhlyi D. Information Security Of Ukraine: Review Of Recent Trends. Physical and Mathematical Education. 2018. Issue 2(16). P. 13-17.

УДК 378.147:004

Д.С. Безуглий
Сумський державний педагогічний університет імені А.С. Макаренка, Україна
DOI 10.31110/2413-1571-2018-016-2-002

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ОГЛЯД ОСТАННІХ ТЕНДЕНЦІЙ[1]

Анотація. *У статті розглянуті основні положення та тенденції функціонування та розвитку інформаційної безпеки України. Обґрунтована необхідність інформаційної безпеки як складової частини національної безпеки країни. Розглянуті основні нормативно-правові документи, які регламентують та уточнюють поняття та структурні компоненти інформаційної безпеки. Виділені три основні рівні надання інформаційної безпеки: рівень особи, суспільний рівень та державний рівень. Зазначені суттєві ознаки інформаційної безпеки (конфіденційність, цілісність, доступність, відмовостійкість) та головні загрози інформаційної безпеки (поширення недостовірної інформації, зовнішні впливи на суспільну свідомість, інформаційні впливи стосовно недоторканності, прояви сепаратизму в засобах масової інформації). Проаналізовано та описано головні цілі атак з метою несанкціонованого доступу до секретної інформації. Описано наймасштабніші кібератаки з використанням вірусів WannaCry та Petya.A. Закцентовано увагу на інноваціях, мета яких попередити, зашкодити та передбачити будь-які посягання на інформаційну та національну безпеку країни.*

Ключові слова: *інформаційна безпека, національна безпека країни, ознаки інформаційної безпеки, загрози інформаційної безпеки.*

Стрімкі темпи розвитку комп'ютеризації, поширення інформаційних систем і бурхливий розвиток інформаційного суспільства обумовлюють виникнення питання щодо інформаційної безпеки. З кінця XX-го століття інформація виступає стратегічним ресурсом будь-якої держави. Від її ефективного використання залежить не лише розвиток країни, а у більшій мірі національна безпека країни, її інформаційна безпека, яка необхідна для:

- підтримки територіальної цілісності;
- економічної, політичної та соціальної стабільності;
- формування демократичного суспільства, де реалізуються всі конституційні права та свободи громадян, серед яких право на вільний пошук інформації; отримання інформації; передачу інформації; виробництво та розповсюдження інформації будь-яким законним шляхом [1].

Усі вищезгадані питання в Україні регулює Концепція національної безпеки України. Концепцію національної безпеки України щодо інформаційної сфери підтримує та розвиває Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», яке затверджене Указом Президента України від 25 лютого 2017 року № 47/2017 [2].

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу з боку потенційно негативно налаштованих країн.

У самій Доктрині зазначено, що інформаційна сфера перетворилася на ключову арену протиборства в усіх сферах. Зазначається також, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Доктрина базується на принципах додержання прав і свобод людини й громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України.

[1] Робота виконувалася за рахунок бюджетних коштів МОН України, наданих на виконання науково-дослідного проекту №0117U003855 «Інституційно-технологічне проектування інноваційних мереж для системного забезпечення національної безпеки України» (Наказ МОН України від 10 жовтня 2017 р. №1366)

Під *інформаційною безпекою держави* слід розуміти рівень інформаційної захищеності держави, при якому всі негативні та незаконні акти стосовно інформації (несанкціоноване поширення, порушення цілісності інформації, несанкціонований доступ до інформації, порушення конфіденційності) не завдають шкоди національним інтересам та соціуму [3].

Відповідно до *Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»* поняття «*інформаційна безпека*» більш деталізоване і тлумачиться як «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 поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [4].

Іншими словами, на рівні держави усвідомлено проблему інформаційної безпеки, що додатково підкреслено у Доктрині інформаційної безпеки України, яка акцентує увагу на визначенні інноваційних методів і підходів до формування захисту інформаційної сфери і всієї системи в цілому; головним завданням ставить розвиток політики стосовно руйнівного інформаційного впливу негативно налаштованих сторін.

З розвитком інформаційних технологій постає питання оновлення та модернізації засобів, що підтримують та забезпечують інформаційну безпеку. Відокремлюють наступні рівні надання інформаційної безпеки [5]:

1. Рівень особи. *Рівень особи* передбачає формування раціонального, критичного мислення на основі принципів свободи вибору кожного окремого громадянина.

2. Суспільний рівень. *Суспільний рівень* передбачає формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам.

3. Державний рівень. *Державний рівень* передбачає інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, систему захисту інформації з обмеженим доступом, протидію правопорушенням в інформаційній сфері, комп'ютерним злочинам.

Відповідно до Доктрини інформаційної безпеки України є наступний перелік принципів забезпечення інформаційної безпеки (рис. 1).

До суттєвих ознак поняття інформаційної безпеки відносять конфіденційність (стан інформації, при якому доступ до неї отримують тільки суб'єкти, які мають на це право), цілісність (запобігання несанкціонованій або незаконній модифікації інформації) та доступність (запобігання тимчасового або постійного приховування інформації від користувачів, які отримала право на доступ) (рис. 2). Також виділяють й інші категорії моделі, які не є обов'язковими, а саме: відмовостійкість (здатність посвідчити дію, яка мала місце або подію так, що ці події або дії не могли бути пізніше відкинуті), підзвітність, достовірність, автентичність.

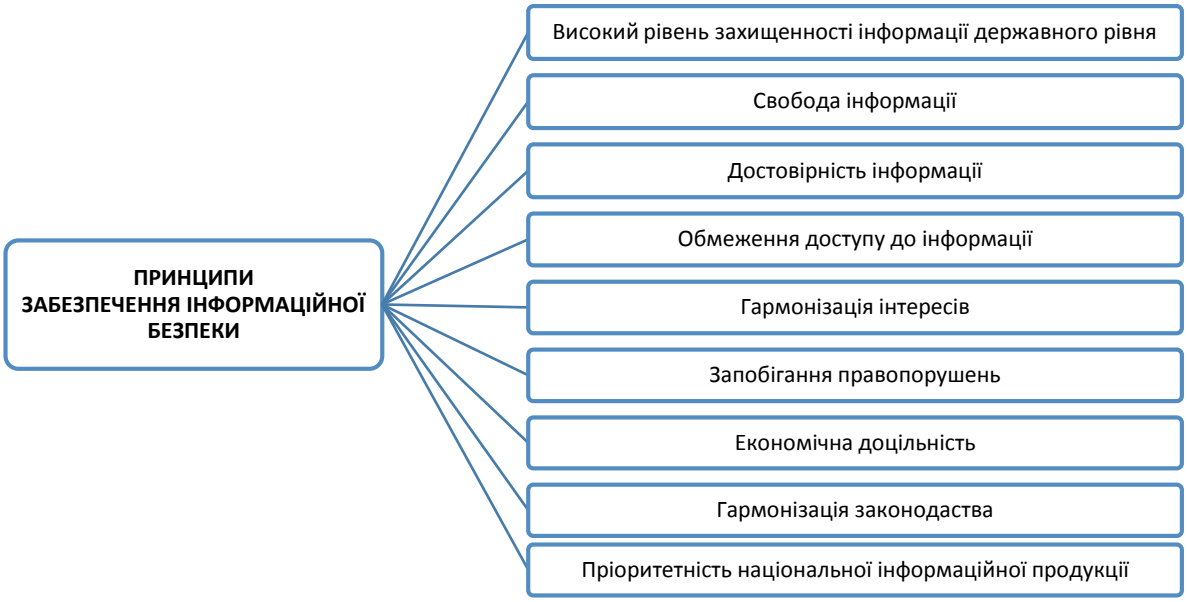

Рис. 1. Принципи інформаційної безпеки

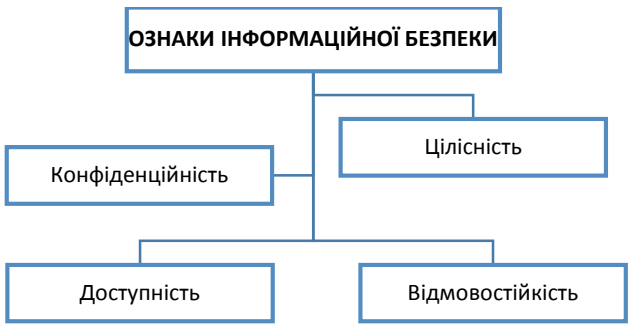

Рис. 2. Ознаки інформаційної безпеки

В офіційних правових документах виділяють наступні загрози інформаційної безпеки країни (рис. 3).

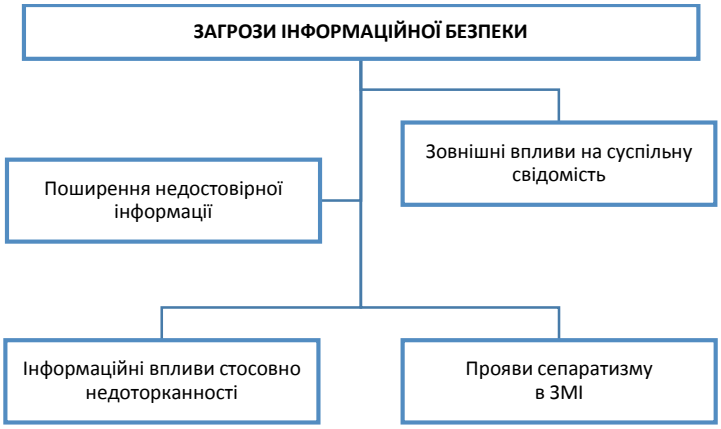

Рис. 3. Загрози інформаційної безпеки

Більшість загроз інформаційної безпеки реалізується шляхом несанкціонованого проникнення до сховищ інформації (комп'ютерів та серверів певних користувачів або організацій та установ).

Головні цілі таких атак:

– заміна достовірної інформації на недостовірну;
– викрадення конфіденційної інформації та подальше її нелегальне використання або вимагання за неї грошових еквівалентів;
– порушення стабільності роботи інфраструктури організацій та країни в цілому;
– внесення соціальної, політичної та економічної дестабілізації.

Одним із прикладів порушення інформаційної безпеки та подальшого прояву всіх негативних наслідків цього явища є подія 27 липня 2017 року, коли відбулася наймасштабніша в історії України кібератака, яку деякі ЗМІ класифікують як кібертеракт: відбулося інфікування великої кількості комп'ютерів різних організацій через програму для обліку Me.Doc комп'ютерним вірусом під назвою Petya.A (або mbr locker 256 – вірус-шифрувальник) [6]. Вірус схожий на свого попередника під назвою WannaCry (рис. 3), який вимагав грошових сплат від користувачів ПК [7]. Вірус Petya.A безповоротно шифрував дані на користувацьких комп'ютерах, після чого було неможливо відновити зашифровану інформацію.

Рис. 3. Екран блокування, викликаний вірусом Wannacry з детальною інструкцією вимог

У списку організацій, які зазнали шкоди, – найкрупніші банки (включаючи НБУ); комунальні та енергетичні підприємства; підприємства інфраструктури (серед яких Укрзалізниця); провідні оператори мобільного зв'язку; автозаправні станції; поштові компанії (Укрпошта, Нова Пошта та ін.); ЗМІ; влада та державні підприємства (Кабмін, ГСЧС, ЧАЕС та ін.).

Така атака вплинула на стабільність державних і приватних організацій, і призвела до негативних та подекуди панічних настроїв у суспільстві.

Це обумовлює актуалізацію досліджень в галузі забезпечення інформаційної безпеки, які зорієнтовані на активне використання інноваційних технологій та аналіз досвіду інших країн. Зокрема, цікавим є Ізраїльський досвід [8]: великі компанії, такі як Cisco, Microsoft, Google, IBM відкрили на території країни свої центри кіберрозробок, результати яких були ефективно впроваджені і використані в роботі органів державного управління та інституцій для забезпечення безпеки (інформаційної та кібербезпеки). Саме тому пріоритетним напрямом інноваційного розвитку в галузі інформаційної безпеки для України є залучення власних та закордонних спеціалістів з кіберсфери для розвитку і впровадження систем захисту від кібератак.

На думку організації Fortinet [1], головними інноваціями з переліку є широке використання та підвищення безпеки контейнерів, таких як Docker (в операційних системах на ядрі Linux, програмне забезпечення для автоматизації розгортання і управління програмним забезпеченням в середовищі віртуалізації на рівні операційної системи. Дозволяє «упакувати» програмне забезпечення з усім його оточенням і залежностями в контейнер, який може бути перенесений на будь-яку Linux-систему з підтримкою cgroups в ядрі, а також надає середовище з управління контейнерами.) та підтримка розвитку та розгортання корпоративних мереж SD-WAN (Software-Defined Wide Area Network – програмно-конфігуровані глобальні мережі, технологія, яка дозволяє спростити шифрування трафіку, в оперативному режимі відслідковувати атаки та розділяти мережу на сегменти з метою ізоляції негативного впливу атак на мережу).

Отже, суб'єкти реалізації державної інформаційної політики у взаємодії з інститутами громадянського суспільства в межах компетенції забезпечують реалізацію Доктрини, а також за необхідності вносять обґрунтовані пропозиції щодо корегування її положень.

Важливою проблемою в рамках реалізації політики інформаційної безпеки є правильний підбір методів та цілей задля протидії можливим небезпекам в галузі інформаційної безпеки України.

Також для підтримки відповідного рівня інформаційної безпеки в Україні доцільно розробити стратегію захисту інформаційної сфери в умовах нових інформаційно-військових викликів. В подальшому потрібно вдосконалювати цю систему, враховуючи всі можливі чинники і фактори, як внутрішні, так і зовнішні.

Список використаних джерел

1. Пять инноваций в сфере ИБ в 2017 г. | ChannelForIT. URL: http://channel4it.com/publications/Pyat-innovaciy-v-sfere-IB-v-2017-g-24929.html#. (дата звернення 24.05.2018)
2. "УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017 — Офіційне інтернет-представництво Президента України". *Офіційне інтернет-представництво Президента України.* 2017. URL: http://www.president.gov.ua/documents/472017-21374. (Дата звернення: 24.05.2018).
3. Інформаційна безпека України. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8. (дата звернення 24.05.2018)
4. "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки", Офіційне інтернет-представництво Президента України. 2017. URL: http://zakon0.rada.gov.ua/laws/show/537-16. (Дата звернення: 24.05.2018).
5. Бондар І. Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. Суми. 2014. URL : http://www.lac.lviv.ua/fileadmin/www.lac.lviv.ua/data/kafedry/MEV/Bodnar/Bodnar_Vyb_Pub_9.pdf. (Дата звернення 24.05.2018).
6. Кібератака вірусу Petya: що відомо | Політичні новини з Європи: аналітика, прогнози, коментарі | DW | 28.06.2017. URL : https://www.dw.com/uk/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0-%D0%B2%D1%96%D1%80%D1%83%D1%81%D1%83-petya-%D1%89%D0%BE-%D0%B2%D1%96%D0%B4%D0%BE%D0%BC%D0%BE/a-39452258. (дата звернення 24.05.2018)
7. Вірус Wannacry: все, що потрібно знати про кібератаку / Новое время. URL: https://nv.ua/ukr/world/countries/svit-zaznav-bezpretsedentnoju-kiberatatsi-shcho-take-virus-wannacry-jak-z-nim-borotisja-i-hto-vinen-1138770.html. (дата звернення 24.05.2018)
8. Израильские инновации в области информационной безопасности – в чем секрет? – STMEGI. URL: https://stmegi.com/posts/34937/izrailskie-innovatsii-v-oblasti-informatsionnoy-bezopasnosti-v-chem-sekret/. (дата звернення 24.05.2018)

References

1. Pyat innovatsiy v sfere IB v 2017 g. | ChannelForIT. URL: http://channel4it.com/publications/Pyat-innovaciy-v-sfere-IB-v-2017-g-24929.html# (in Russian).
2. "UKAZ PREZYDENTA UKRAINY №47/2017 — Ofitsiine internet-predstavnytstvo Prezydenta Ukrainy". Ofitsiine internet-predstavnytstvo Prezydenta Ukrainy. 2017. URL: http://www.president.gov.ua/documents/472017-21374 (in Ukrainian).
3. Informatsiina bezpeka Ukrainy. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8 (in Ukrainian).
4. "Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007-2015 roky", Ofitsiine internet-predstavnytstvo Prezydenta Ukrainy. 2017. URL: http://zakon0.rada.gov.ua/laws/show/537-16 (in Ukrainian).
5. Bondar I. R. Informatsiina bezpeka yak osnova natsionalnoi bezpeky. Mekhanizm rehuliuvannia ekonomiky. Sumy. 2014. URL : http://www.lac.lviv.ua/fileadmin/www.lac.lviv.ua/data/kafedry/MEV/Bodnar/Bodnar_Vyb_Pub_9.pdf (in Ukrainian).
6. Kiberataka virusu Petya: shcho vidomo | Politychni novyny z Yevropy: analityka, prohnozy, komentari | DW | 28.06.2017. URL : https://www.dw.com/uk/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0-%D0%B2%D1%96%D1%80%D1%83%D1%81%D1%83-petya-%D1%89%D0%BE-%D0%B2%D1%96%D0%B4%D0%BE%D0%BC%D0%BE/a-39452258 (in Ukrainian).
7. Virus Wannacry: vse, shcho potribno znaty pro kiberataku / Novoe vremia. URL: https://nv.ua/ukr/world/countries/svit-zaznav-bezpretsedentnoju-kiberatatsi-shcho-take-virus-wannacry-jak-z-nim-borotisja-i-hto-vinen-1138770.html
8. (in Ukrainian).
9. Izrailskie innovatsii v oblasti informatsionnoy bezopasnosti – v chem sekret? – STMEGI. URL: https://stmegi.com/posts/34937/izrailskie-innovatsii-v-oblasti-informatsionnoy-bezopasnosti-v-chem-sekret/ (in Russian).

INFORMATION SECURITY OF UKRAINE: REVIEW OF RECENT TRENDS

Dmytro Bezuhlyi

Makarenko Sumy State Pedagogical University, Ukraine

Abstract. *The article considers the main provisions and tendencies of functioning and development of information security of Ukraine. Described the thesis on the need for information security, as part of the national security of the country. The main legal documents regulating and clarifying the concept and structural components of information security are considered. Dedicated 3 basic levels of providing information security, including: the level of the person, the social level and the state level. The indicated essential features of information security (confidentiality, integrity, accessibility, fault tolerance) and the main threats to information security (dissemination of unreliable information, external influences on public consciousness, information influences for inviolability, manifestations of separatism in the media). The main purposes of attacks with the purpose of unauthorized access to classified information are analyzed and described.*

Also in the article are mentioned the most large-scale cyber attacks using the viruses WannaCry and Petya.A. Attention is focused on innovations, the purpose of which is to prevent, damage and provide for any encroachment on the information and national security of the country.

Keywords: *information security, national security of the country, signs of information security, threats of information security.*