ЗАГРОЗИ ТА ФОРМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Любохинець Л. С.
кандидат економічних наук,
доцент кафедри економічної теорії
Хмельницький національний університет

Міхалець А. В.
студентка
Хмельницький національний університет
м. Хмельницький, Україна

Впровадження інформаційних технологій в різні сфери суспільного розвитку, формування інформаційного суспільства *призводить до швидкого зростання інформації, яку необхідно захищати з метою збереження її конфіденційності. Інформація стала чинником, під впливом якого зростає потенційна вразливість суспільних процесів, відбувається дезорганізація державного управління, можуть виникати великомасштабні аварії, військові конфлікти, стихійні лиха.* У сучасному суспільстві одним із найважливіших показників рівня цивілізованості держави є ступінь розвитку її інформаційного простору.

До сфери інформаційної безпеки держави віднесені конкретні дії щодо забезпечення безпечних умов існуючих інформаційних процесів та безпечного розвитку їх у майбутньому. Це охоплює регулювання питань захисту самої інформації, інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов розвитку інформаційних процесів. Все це досягається проведенням необхідної державної політики інформаційної безпеки та створенням необхідних правових та організаційних засад її реалізації.

Інформаційна безпека посідає особливе місце в системі національної безпеки, тому загрози інформаційного характеру можуть спрямовуватись до будь-яких структурних складових національної безпеки, однак їх негативний вплив завжди опосередковуватиметься завданням шкоди інформаційній безпеці держави. Система загроз інформаційній безпеці має комплексний характер і в загальному вигляді включає в себе загрози безпеці інформації та інформаційної інфраструктури, безпеці суб'єктів інформаційної сфери й соціальних зв'язків між ними від інформаційних впливів, загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери. Таким чином, загрози інформаційній безпеці держави виступають сукупністю умов і факторів, які становлять небезпеку життєво важливим інтересам держави, суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру [1, с. 183]. Варто сказати, що недосконаліть, мало-

розвиненість та вплив різних негативних факторів зменшують ефективність забезпечення інформаційної безпеки.

У 2017 році Україна зазнала найбільших інформаційних втрат і входить до країн з найбільшим рівнем ураження (рис. 1). Так, за звітом відомої компанії «Panda Security» в 1 кварталі 2017 року в Україні діяли невідомі кібератаки, які пошкодили 3,73 % інформаційного обладнання.

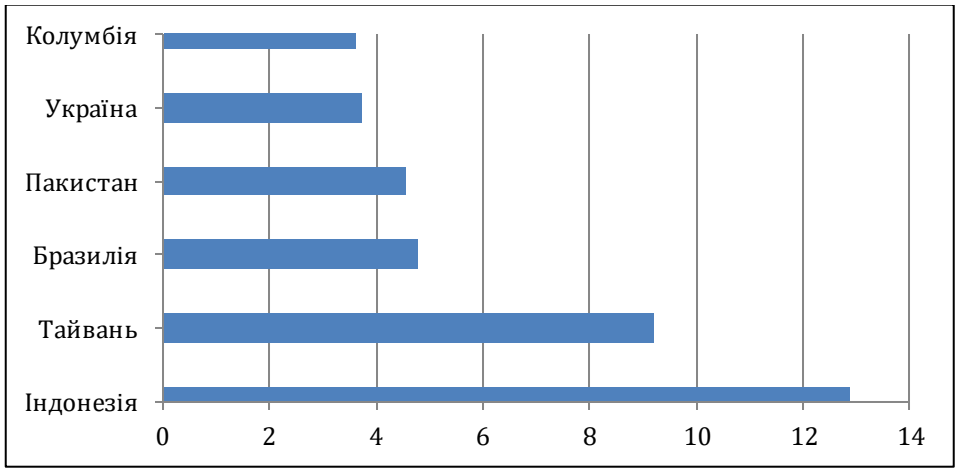

Рис. 1. Країни з найбільшим рівнем ураження в 1 кварталі 2017 року [2]

Другий квартал 2017 року з точки зору інформаційної безпеки став найжахливішим за всю історію атак. Були проведені дві самі великі кібер-атаки WannaCry та GoldenEye/Petya, від яких постраждали майже всі країни світу і велика кількість компаній, більше 230 000 комп'ютерів. За різними оцінками експертів, втрати від цих атак склали від 1 до 4 млрд. дол. США, тобто від 4300 до 17000 дол. в розрахунку на кожний комп'ютер[3]. Ці атаки тісно пов'язані з кібер-війнами і зусиллями різних країн в боротьбі з ними. Дві атаки скористались вразливістю виявленою АНБ, яка була викрадена групою хакерів Shadow Brockers ще в квітні 2017 року. Також відомо, що існує ряд доказів, які вказують на те, що джерелом атаки WannaCry є КНДР, а атака GoldenEye/Petya була спрямована тільки на Україну, тобто на українські компанії. За звітом компанії «Panda Security» у 2 кварталі 2017 року Україна також увійшла в ТОП-10 найбільш атакуючих країн і її показник становив уже 8,96% (рис. 2).

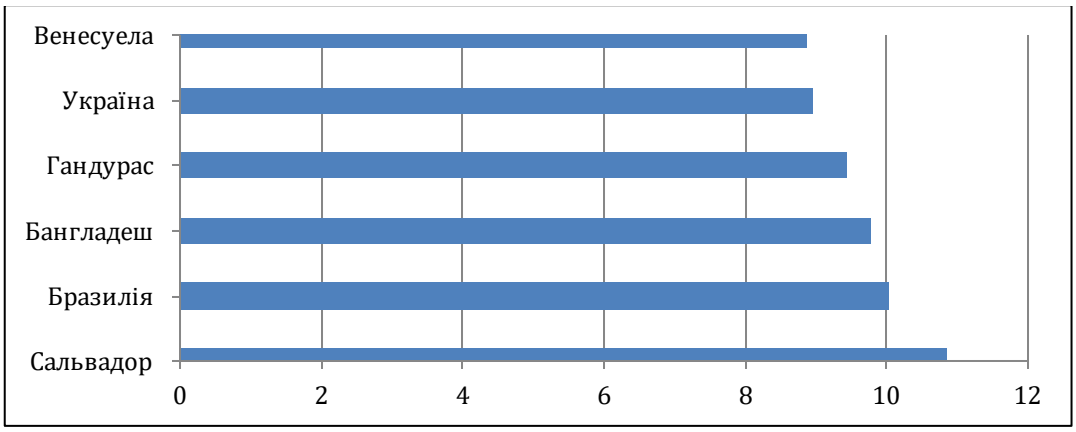

Рис. 2. Країни з найбільшим рівнем ураження в 2 кварталі 2017 року [3]

Таким чином, 2017 рік був найважчим для інформаційної безпеки України. Тому виникає потреба у створенні умов для забезпечення гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод, встановлення політичної і соціальної стабільності, економічного процвітання і т.д.

Кожній із загроз безпеці в різних сферах інформаційного життя необхідно протиставити певні заходи, способи, методи їх нейтралізації, захисту інформаційного ресурсу, баз даних, національного інформаційного простору. Забезпечення інформаційної безпеки – це сукупність методів, форм призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації. При цьому форми забезпечення інформаційної безпеки утворюють інструмент, за допомогою якого сили інформаційної безпеки вирішують увесь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави.

Забезпечення інформаційної безпеки здійснюється трьома формами (рис. 3).

Рис. 3. Форми забезпечення інформаційної безпеки держави [4, с. 100]

Інформаційним патронатом називається форма забезпечення інформаційної безпеки з боку держави фізичних і юридичних осіб та включає добування різноманітних відомостей про дестабілізуючі фактори та інформаційні загрози, обмін інформацією між органами управління та засобами системи інформаційної безпеки. Інформаційною кооперацією є форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу, який включає сукупність взаємоузгоджених дій, спрямованих на отримання відомостей про дестабілізацію інформаційної безпеки в країні, інформаційні загрози та методи боротьби з ними. Інформаційне протиборство – це форма суперництва соціальних систем в інформаційній сфері з приводу впливу на різні сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, в результаті якого одна з груп отримає переваги, які потрібні їм задля подальшого розвитку. Інформаційне протиборство відбувається між різними видами соціальних суб'єктів, але цілі ряди таких взаємодій утворюють окремі форми протиборства (інформаційні війни, злочинність, тероризм) [5, с. 96].

Отже, забезпечення інформаційної безпеки держави, сьогодні, є проблемою високої складності та потребує комплексного підходу. Вибір методів протидії конкретним загрозам та небезпекам у сфері інформаційної безпеки України становить важливу проблему і складову частину діяльності по реалізації основних напрямів державної політики інформаційної безпеки. Забезпечення інформаційної безпеки сьогодні вимагає пошуку перспективних шляхів тісної взаємодії й координації державних та недержавних структур у системі національної безпеки, посилення контролю та стратегії забезпечення інформаційної безпеки, насамперед, збоку держави для подальшого ефективного захисту інформації – як головної складової сучасного суспільства.

Література:

1. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право.* 2017. № 10. С. 182-186

2. Pandalabs – Отчет за 1 квартал 2017 года. URL: http://www.cloudav.ru/upload/iblock/3b3/Pandalabs%20-%20Отчет%20за%202%20квартал%202017.pdf.

3. Pandalabs – Отчет за 2 квартал 2017. URL: https://pandasecurity.bitrix24.ru/docs/pub/1c3e16b44b7eced067ca1ceb9ae381ce/default/?&

4. Лук'янова В.В., Лаутар А.Ю. Безпека в умовах розвитку інформаційної системи. *Вісник Хмельницького національного університету. Економічні науки.* 2013. № 2. Т. 3. С. 97-101.

5. Любохинець Л.С., Поплавська О.В. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі. *Бізнес-навігатор.* 2017. Випуск 4-1(43). С. 93-97