Микола Слободянюк,
студент 1 СТН курсу спеціальності 208 «Агроінженерія»
Науковий керівник: ***Мушеник Ірина Миколаївна,***
канд. екон. наук, доцент кафедри математичних дисциплін, інформатики і моделювання,
Подільський державний аграрно-технічний університет,
м. Кам'янець-Подільський

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Забезпечення інформаційної безпеки держави – це досить нова державна функція, яка характеризується відсутністю сталих та визначених механізмів та методів, правового інструментарію їх реалізації. Її формування обумовлене необхідністю захисту суспільства і держави від інформаційних загроз, пов'язаних з розвитком новітніх інформаційно-комунікаційних технологій. Масштаби негативних наслідків цих загроз для держав, організацій, прав і свобод людини і громадянина вже усвідомлені світовою спільнотою, тому найважливішим завданням держави є розробка системи заходів по їх запобіганню і нейтралізації [3].

Під **інформаційною безпекою** розуміється захищеність інформації та підтримує її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктурі [1].

Інформаційна безпека організації це – стан захищеності інформаційного середовища організації, що забезпечує її формування, використання і розвиток.

У сучасному соціумі інформаційна сфера має дві складові: інформаційно-технічну (штучно створений людиною світ техніки, технологій тощо) та інформаційно-психологічну (природний світ живої природи, що включає і самої людини).

Відповідно, в загальному випадку загальну безпеку суспільства можна представити двома складовими частинами: інформаційно – технічною безпекою і інформаційно-психологічної (психофізичної) безпекою.

У якості стандартної моделі безпеки часто призводять модель з трьох категорій:

– конфіденційність – стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на нього право;

– цілісність – уникнення несанкціонованої модифікації інформації;

– доступність – уникнення тимчасового або постійного захування інформації від користувачів, що отримали права доступу.

Виділяють і інші не завжди обов'язкові категорії моделі безпеки:

– неспростовності або апелліруємість – неможливість відмови від авторства;

– підзвітність – забезпечення ідентифікації суб'єкта доступу та реєстрації його дій;

– достовірність – властивість відповідності передбаченому поведінки чи результату;

– автентичність або справжність – властивість, що гарантує, що суб'єкт або ресурс ідентичні заявленим.

Визначення мети, принципів забезпечення інформаційної безпеки країни сприяє формуванню інформаційної системи і вирішення пов'язаних з нею проблем. Інформаційна безпека, як правило, є сполучною ланкою між політикою національної безпеки і інформаційною політикою країни. Небезпека, яка може виникати в інформаційній сфері, – це незбалансованість інтересів суб'єктів суспільних відносин. Причина криється, перш за все, в недостатній діяльності державних інститутів щодо підвищення рівня інформаційної безпеки України [4].

Отже, національний інформаційний простір України, на жаль, зазнає суттєвих загроз, викликів, які становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури. Загрози національній безпеці України в інформаційній сфері це – сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства і особи через

можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [3].

Таким чином, в сучасних умовах наявність розвиненої системи інформаційної безпеки стає одним з найважливіших умов конкурентоспроможності і навіть життєздатності будь-якої компанії.

Фахівці кажуть, що головна причина проникнення в комп'ютерні мережі - безтурботність і непідготовленість користувачів. Це характерно не лише для пересічних користувачів, але і для фахівців в області комп'ютерної безпеки. Разом з тим, причина не тільки в халатності, але й у порівняно невеликому досвіді фахівців з безпеки у сфері інформаційних технологій. Пов'язано це зі стрімким розвитком ринку мережевих технологій і самої мережі Інтернет [2].

За даними лабораторії Касперського, близько 90% від загального числа проникнень на комп'ютер шкідливих програм використовується за допомогою Інтернет, через електронну пошту і перегляд Web-сторінок.

У сучасному глобалізованому інформаційному суспільстві, де кіберпростір перетворюється на поле боротьби, вагомими загрозами інформаційній безпеці держави (і України, зокрема) є комп’ютерна злочинність, кібертероризм, кібервійни, які передбачають протистояння національних інтересів у просторі Інтернету, застосування комп’ютерних та інтернет-технологій для нанесення шкоди супротивнику. Найчастіше технології кібервійни, кібертероризму спрямовані на сферу державної безпеки й оборони і становлять реальну загрозу суверенітету держави. Отже, проти України широко використовують сучасні технології негативних інформаційно-психологічних впливів, які стають загрозою українському національному інформаційному простору та суверенітету держави [1].

Варто зазначити, що з метою захисту національного інформаційного простору, створення ефективної системи забезпечення інформаційної безпеки, з 8 боку української влади здійснюються певні заходи. Зокрема, 14 січня 2015 року Кабінет Міністрів України ухвалив Постанову, згідно з якою створено

Міністерство інформаційної політики України, пріоритетними завданнями якого є протидія інформаційній агресії з боку Російської федерації; розроблення ефективної стратегії інформаційної політики держави та Концепції інформаційної безпеки України; узгодженість та координація функціонування і діяльності органів державної влади і інформаційній сфері [4].

Отже, в умовах сучасних інформаційних протистоянь, національний інформаційний простір України є недостатньо захищеним від зовнішніх негативних пропагандистських інформаційно-психологічних впливів, загроз. Тому захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки України, розроблення дієвих стратегій і тактик протидії медіа загрозам повинні стати пріоритетними завданнями органів державної влади та недержавних інститутів.

Список використаних джерел:

1. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. №1. С. 68-75.

2. Микитенко Т. В., Петровська І. О., Рогов П. Д. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2014. №1. С. 24-31.

3. Степанов В. Ю. Інформаційна безпека в інформаційній сфері державного управління. *Теорія та практика державного управління*. 2016. №4 (55). С. 24-28.

4. Ясінецька І., Мушеник І. Інформаційні системи і технології в управлінні діяльністю підприємства. *Збірник наукових праць ΛΌГОΣ*. 2020. С. 66-67.