УДК 338.242

Глушко А.Д., к.е.н., доцент
Скриль В.В., к.е.н., доцент
Каленіченко Є.С., магістрант
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(м. Полтава, Україна)

СВІТОВИЙ ДОСВІД ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА МОЖЛИВОСТІ ЙОГО ЗАСТОСУВАННЯ В УКРАЇНІ

В умовах дуального впливу процесів діджиталізації, які, з одного боку, виступають інструментом реалізації й захисту національних економічних інтересів, забезпечення зміцнення безпеки національної економіки, а з іншого, – джерелом виникнення внутрішніх і зовнішніх дестабілізуючих чинників, інформація стає одним із найважливіших ресурсів, а її захист – головним завданням загальнодержавного рівня [1].

Інформаційна безпека є невід'ємною складовою кожної сфери національної безпеки й покликана захищати життєво важливі інтереси особистості, суспільства і держави, мінімізувати збитки через недостовірну та неповну інформацію, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив на суспільство. В реаліях сьогодення, забезпечення інформаційної безпеки кожного окремого громадянина, суспільства та держави в цілому є першочерговим завданням та набуває стратегічного значення [2, 3]. У цьому контексті доцільно розглянути позитивний світовий досвід в напрямку забезпечення високого рівня захищеності інформаційних ресурсів.

Лідером у сфері захисту інформаційних ресурсів правомірно визначити Сполучені Штати Америки, законодавство яких налічує майже півтисячі нормативно-правових актів у сфері інформаційної безпеки. Більшість американських підприємців користуються послугами охоронно-детективних агентств. Активний та успішний бізнес, співпрацюючи з такими структурами та маючи на меті зменшення підприємницьких ризиків, може заснувати власну службу безпеки. Варто зазначити, що в США особливою рисою у створенні зазначених вище зазначених структур є участь осіб з ФБР та ЦРУ. Це дає можливість використовувати власну базу даних, досвід відбору працівників та створювати спеціалізовані підрозділи зі співробітниками спеціальних служб. Враховуючи, що діяльність відділів безпеки знаходиться на особистому контролі президента, а рівень підготовки кадрів – одним із найвищих у світі, Сполучені Штати Америки є дійсно однією з передових країн світу у контексті захисту інформації [4].

Заслуговує на вивчення досвід організації захисту інформації Німеччини, як однієї з найбільш розвинутих країн Західної Європи в галузі інформаційної безпеки. Ще в 50-х рр. XIX ст. в країні почали активно розроблятися заходи забезпечення безпеки персональних даних. Як наслідок, в 1970 р. був прийнятий перший у світі нормативно-правовий акт, котрий регулював питання захисту таких даних. Зокрема, суб'єкти господарювання, навіть з чисельність працюючих 5-10 осіб, обов'язково мають мати у штатному розписі посаду уповноваженого із захисту особистих даних. З метою забезпечення високого рівня технічного захисту інформаційних ресурсів уряд Німеччини в 1993 р. створив спеціальне відомство із забезпечення безпеки у сфері інформаційної техніки. До його компетенції належить не лише технічний захист інформації, але й надання консультаційних послуг громадськості, сертифікація й стандартизація відповідних засобів безпеки, а також популяризація заходів захисту інформаційних ресурсів на підприємствах [5].

Досвід Великої Британії в контексті захисту інформації є незвичним та водночас схожим із практикою США. У сфері захисту інформаційних ресурсів активно проваджують діяльність приватні агентства. Водночас система захисту інформації країни містить ряд недоліків. Основу нормативно-правового забезпечення безпеки державних інформаційних

ресурсів складають Закони «Про державні документи» та «Про державну таємницю». Поряд з цим, захищеність інших видів інформації регламентується лише Кримінальним кодексом і низкою правових актів. Щодо захисту комерційної таємниці, то це питання взагалі законодавчо не регулюється і належить виключно до компетенції суб'єктів господарювання.

Донедавна Франція не вирізнялася з-поміж європейських країн специфікою у формуванні системи захисту інформаційних ресурсів. Останнім часом власники промислово-торговельних і фінансово-кредитних організацій посилюють інформаційну безпеку за допомогою створення власних або залучення детективно-охоронних агентств. Ці послуги невдовзі стали поширеними і в сфері страхування, юридичних структурах, закладах освіти. Кваліфіковані спеціалісти агентств, тісно контактуючи з правоохоронними органами, спрямовують зусилля на протидію зловживанню торговою маркою, недобросовісній конкуренції, промисловому шпигунству тощо [6].

Заслуговує на увагу практика країн Азії у сфері захисту інформаційних ресурсів, а саме Японії та Китаю. Японією накопичено значний юридичний досвід у відносинах щодо захисту комерційної таємниці. Відповідно до чинного законодавства, роботодавці мають змогу через укладення договорів зобов'язати найманих працівників не розголошувати комерційні дані, як під час дії трудової угоди, так і після її закінчення. Крім того, в Японії актуальним є питання захисту ділових секретів.

Китай лідирує в масштабах захисту інформаційних ресурсів та протидії кібератакам. Зокрема, сформована дієва система забезпечення безпеки комп'ютерних систем, в тому числі ґрунтовне законодавче забезпечення. Ще в 2001 р. китайський уряд прийняв Положення «Про охорону комп'ютерних програм». Цей юридичний акт став базисним у сфері охорони безпеки комп'ютерних систем Китаю. Забезпечення захисту інформаційних ресурсів в країні покладено на орган громадської безпеки [7].

Таким чином, питання захисту інформаційних ресурсів в умовах посилення процесів діджиталізації є актуальним у всіх країнах світу. В Україні напрацьовано ґрунтовну законодавчу базу, яка регулює відносини володіння, користування, збереження, розповсюдження інформаційних ресурсів та комерційної таємниці. Проте рівень інформаційної безпеки залишається недостатнім. про що свідчать успішні кібератаки. Використання світового досвіду, зокрема впровадження нових методів захисту інформаційних ресурсів, дозволить зменшити ризики кібератак та кіберзлочинів, забезпечити безпеку інформаційних ресурсів на всіх рівнях.

Список використаних джерел

1. Онищенко С.В., Глушко А.Д. Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації. *Соціальна економіка*. ХНУ, 2020. Вип. 59. С. 14–24.

2. Варналій З.С. Державна політика забезпечення інформаційної безпеки України. ІІІ Всеукраїнська науково-практична Інтернет-конференція з міжнародною участю «Економічна безпека: держава, регіон, підприємство» (1 грудня 2016 р. – 10 січня 2017 р.). Полтава: ПолтНТУ, 2016. С.79-84.

3. Onyshchenko S., Hlushko A., Yanko A. Role and importance of information security in a pandemic environment. *Economics and Region*. 2020. №2 (77). P.103–108.

4. Олійник О.Г. Інформаційна безпека США. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. Вип. 1. С. 280–288.

5. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Київ: Кондор, 2008. 384 с.

6. Низенко Е.І., Калепяк В.П. Забезпечення інформаційної безпеки підприємництва: навчальний посібник. Київ: МАІП, 2006. 134 с.

7. Лапінська Є. І. Зарубіжний досвід захисту інформації у сфері підприємництва та його використання в Україні. *Держава та регіони*. 2019. № 3 (65). С. 174–177.