2. Agriculture Resilience Initiative (AGRI) - Ukraine. – URL: https://www.usaid.gov/ukraine/agriculture-resilience-initiative-agri-ukraine

3. FAO stands ready to support Ukrainian farmers and rural population. – URL: https://www.fao.org/

4. Treasury Releases Fact Sheet on Food and Fertilizer-Related Authorizations Under Russia Sanctions; Expands General License Authorizing Agricultural Transactions. – URL: https://home.treasury.gov/news/press-releases/jy0868

5. Павлова Г, Абрамович І, М. Бальзан. Стратегічні заходи підвищення конкурентоспроможності аграрного сектору України на міжнародному ринку. *Вісник Хмельницького національного університету*. 2022. № 4. С. 62-67.

6. Аграрні відносини під час війни: як держава допомагає аграріям з регіонів, що постраждали від воєнних дій . – URL: https://cutt.ly/2K9evCm

7. Як виживають аграрії в умовах війни та чому їм доводиться відстоювати право на патріотизм. – URL: https://news.obozrevatel.com/ukr/economics/yak-vizhivayut-agrarii-v-umovah-vijni-ta-chomu-im-dovoditsya-vidstoyuvati-pravo-na-patriotizm.htm

Валерія КОЛЕНДЗЯН,
здобувач вищої освіти ОС «бакалавр»,
спеціальність «Фінанси, банківська справа та страхування»,
Заклад вищої освіти «Подільський державний університет»,
Андрій Печенюк,
кандидат економічних наук, доцент кафедри фінансів,
банківської справи, страхування та електронних платіжних систем,
Заклад вищої освіти «Подільський державний університет»,
Україна

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА ТА ОСНОВНІ СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Сьогодні підприємство стикається з багатьма проблемами, коли мова заходить про інформаційну безпеку. Зі зростанням залежності від технологій потреба в захисті даних та інформаційних активів ніколи не була більшою. У

сучасному діловому світі захист інформації компанії має вирішальне значення для успіху. Є багато небезпек, які можуть поставити дані під загрозу, тому важливо мати надійну систему безпеки.

Захист інформаційної інфраструктури організації відкриває нові ділові можливості, а наявні бізнес-процеси вимагають менше ресурсів для ефективної роботи. Надійний захист інформації дозволяє залучити до бізнесу нових партнерів. Чим вищий рівень довіри, тим більший рівень доступу безпечно можна надавати зовнішнім сторонам: клієнтам, діловим партнерам, співробітникам і підрядникам. Це допомагає розширити бізнес та одночасно спрощує виконання операцій, знижуючи витрати.

Поняття «інформаційна безпека» слід розглядати як стан захищеності систем обробки и зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення [1].

Під загрозою безпеки інформації слід розуміти події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів, програмних і апаратних засобів інформаційної системи підприємства.

В найбільш загальному вигляді інформаційна безпека може бути визначена як неможливість нанесення шкоди властивостям об’єкта безпеки, обумовлена інформацією і інформаційною інфраструктурою [2].

Основними загрозами інформаційної безпеки сучасного підприємства є: розкриття конфіденційної інформації, помилкове використання інформаційних ресурсів; несанкціоноване використання інформації; «злам» інформаційної системи; несанкціонований обмін інформацією.

У сьогоднішніх реаліях усе частіше застосовується робота співробітників поза офісами. З цієї причини виникає ризик крадіжки даних компанії та збільшення загроз інформаційної безпеки. Це відбувається тому, що бізнес не

готовий централізовано керувати своєю мережею або інфраструктура не достатньо готова, недостатньо інструментів для захисту інформації або відсутня налагодженість процесів і, що важливо, низька кваліфікація персоналу [3].

Зростаюча кількість загроз інформаційній безпеці бізнесу в умовах формування цифрової економіки обумовлює необхідність розробки та впровадження комплексного характеру дій, спрямованих на її захист. Варто щонайменше виокремлювати взаємопов'язані між собою технічний, організаційний та економічний напрями забезпечення інформаційної безпеки бізнесу.

Заходи технічного характеру пов'язані, в першу чергу, з використанням сучасних технічних засобів і технологій, які, з одного боку, дозволяють ефективно накопичувати, зберігати, обробляти і передавати інформацію, а, з іншого, – забезпечувати її високий рівень захищеності (розподілені бази даних, мережеві екрани, хмарні сервіси, захищені сервери, антивірусні програми тощо).

Дослідження, проведене у 2017 році американським Центром інтернет безпеки (CIS), переконливо довело, що головною дієвою особою і найслабшою ланкою в системі інформаційної безпеки є якраз не технічні системи і використовувані технології, а працівники самого підприємства [4]. Саме через навмисні або ненавмисні дії персоналу здійснюється найбільший відсоток витоку конфіденційної інформації, відбувається втручання в захищені мережі і системи. Відповідно одним з пріоритетних напрямів забезпечення інформаційної безпеки бізнесу має стати постійне підвищення рівня інформаційної (цифрової) грамотності працівників та усебічне організаційно-документальне врегулювання процесів збору, накопичення, обробки використання і зберігання інформації в системі положень і інструкцій поводження з інформацією, які можуть імплементуватися в їх посадові інструкції.

Важливою складовою забезпечення інформаційної безпеки сучасного підприємства є також застосування низки відповідних економічних заходів. Адже проблема захисту інформації має витратний аспект, який необхідно враховувати, порівнюючи потенційний ефект від захищеності інформаційних ресурсів і обсяг витрат, які мають бути здійснені на забезпечення такого захисту. Реалізація окремих заходів має проводитися на підставі співставлення вигід від захисту інформації і можливих втрат, які можуть бути понесені в результаті відсутності такого захисту. Крім того, економічні методи забезпечення інформаційної безпеки бізнесу мають передбачати мотиваційні інструменти, спрямовані на заохочення працівників до дій, спрямованих на зміцнення системи захисту інформації, підвищення рівня своєї інформаційної грамотності і, навпаки, мінімізувати ризики учинення дій, які уможливлюють витік конфіденційної інформації, сприяють порушенню цілісності баз даних, шкодять іміджу бізнесу тощо.

В умовах глобалізації бізнес-процесів інформаційна безпека стає невід'ємною складовою системи економічної безпеки сучасного підприємства. Тому без належного захисту інформаційного середовища компанії неможливо забезпечити її економічну безпеку.

Список використаних джерел

1. Маркіна І.А., Гарічев Ю.М. Інформаційна безпека підприємства та організаційні заходи її забезпечення. *Український журнал прикладної економіки.* 2019. Том 4. №4. С. 209-215.

2. Бехтер Л.А. Загрози інформаційної безпеки та захист інформації як складова економічної безпеки сільськогосподарських підприємств. *Агросвіт.* 2020. №12. С. 66-70.

3. Куроєдова Л. По секрету всьому світові: навіщо бізнесу інформаційна безпека. URL: https://mind.ua/openmind/20235412-po-sekretu-vsomu-svitovi-navishcho-biznesu-informacijna-bezpeka.

4. Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки. URL: https://ir.kneu.edu.ua/bitstream/handle/2010/36159/Ipspr_3-21_8.pdf?sequence=1.

Юрій КОРМИШКІН,
доктор економічних наук, доцент, професор кафедри публічного управління та адміністрування і міжнародної економіки,
Миколаївський національний аграрний університет,
Україна

ПІДХОДИ ДО ФОРМУВАННЯ ОЦІНКИ РОЗВИТКУ СОЦІАЛЬНО-ЕКОНОМІЧНОГО ПОТЕНЦІАЛУ ТЕРИТОРІАЛЬНИХ ГРОМАД

У ході досліджень нами систематизовано підходи на яких має базуватися алгоритм формування соціально-економічного потенціалу територіальних громад. Розглянемо їх зміст:

– **історичний** – дає можливість дослідити виникнення, формування і розвиток соціально-економічного потенціалу територіальної громади у хронологічній послідовності з метою визначення зв'язків між її елементами;

- **системний підхід** – передбачає дотримання певної послідовності в організації дослідження. Вона передбачає такі кроки:

- визначення територіальної громади;
- дослідження її інфраструктури;
- визначення сильних і слабих сторін територіальної громади;
- економічне обґрунтування;
- розробка стратегії соціально-економічного розвитку громади.

хілізм – це комплексне вивчення соціально-економічного потенціалу територіальної громади як єдиного цілого з позиції системного аналізу. Складовими системного аналізу є: формування задачі; виділення територіальної громади; формування моделі;

ентропійний – інструментом виявлення кризових явищ. Використання ентропійного підходу дає можливість побудувати більш коректну базу