5. Lytvynenko K.O. Influence of crypto-currencies on the world financial system. URL: http://www.vestnik-econom.mgu.od.ua/journal/2017/27-1-2017/11.pdf

6. Дученко М.М. «Вплив крипто валюти на економіку країни». URL: http://economyandsociety.in.ua/journals/19_ukr/150.pdf

Фесенець В.С. – здобувач вищої освіти першого (бакалаврського) рівня, Херсонський державний аграрно-економічний університет

Лобода О.М. – к.т.н., Херсонський державний аграрно-економічний університет

СИСТЕМА ЗАХИСТУ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦТВА

У сучасних умовах інформаційні ресурси незамінні у розвитку науки, техніки, виробництва, послуг та інших складових промисловості. Виникає проблема класифікації інформаційних ресурсів, обмеження доступу до деяких із них та визначення економічної доцільності організації захисту інформації на підприємствах та в організаціях різних сфер економічної діяльності. Інформаційна безпека з погляду економічної безпеки – це стан захищеності діяльності організації та її інформаційного середовища від негативного впливу факторів, що дестабілізують, що забезпечує збереження основних властивостей інформації та досягнення соціально-економічної мети.

Інформаційна загроза виникає, коли величина та ймовірність можливої втрати інформації перевищують певний поріг, що вимагає вжиття низки заходів щодо її запобігання та захисту об’єкта безпеки. Загрози інформаційної безпеки – це події чи дії, які можуть призвести до спотворення, несанкціонованого використання чи навіть знищення інформаційних ресурсів системи управління та навіть програмно-апаратних засобів [1, с. 23]. Загроза збереженню цілісності та конфіденційності

інформаційних ресурсів з обмеженим доступом реалізується за рахунок ризику створення каналу несанкціонованого отримання цінної інформації та документів. Функціонування каналу несанкціонованого доступу інформації неминуче призводить до втрати інформації, зникнення носія інформації. Забезпечення інформаційної безпеки має починатися з виявлення проблем взаємовідносин, пов'язаних із використанням інформаційних систем. Спектр їх інтересів можна розділити на такі категорії: доступність, цілісність та конфіденційність [2, с.103].

Тобто у найзагальнішому вигляді інформаційну безпеку можна визначити як неможливість компрометації властивостей об'єкта безпеки, що визначаються інформацією та інформаційною інфраструктурою. До об'єктів забезпечення інформаційної безпеки в організації належать: інформаційні ресурси, що містять відомості, що становлять комерційну таємницю, та конфіденційну інформацію, що надається у вигляді інформаційних масивів та баз даних; інформаційні засоби та системи; комп'ютерне та організаційне обладнання; мережі та системи; загальне системне та прикладне програмне забезпечення; автоматизовані системи управління в організаціях; системи зв'язку та передачі даних; технічні засоби збирання; Реєстрація, передача, обробка та відображення інформації [3, с. 61]. До основних загроз в безпеці відносяться: розкриття конфіденційної інформації; несанкціоноване використання інформаційних ресурсів; нецільове використання ресурсів; несанкціонований обмін інформацією; злом системи; наклепницький.

До причин і умов, що створюють умови для втрати інформації, можуть бути віднесені: недостатнє знання працівниками організації правил захисту конфіденційної інформації та нерозуміння необхідності їх ретельного дотримання; використання несертифікованих технічних засобів для обробки конфіденційної інформації; слабкий контроль за дотриманням правил захисту інформації за допомогою правових, організаційних та технічних заходів тощо. Дані з точки зору системного підходу до захисту інформації встановлюються певні умови: забезпечення інформаційної безпеки може

бути разовим заходом; це безперервний процес, що полягає в обґрунтуванні та впровадженні найбільш раціональних методів, засобів та способів удосконалення та розвитку системи захисту, постійному контролі за її станом, виявленні її вузьких та слабких місць та протиправних дій; планування інформаційної безпеки здійснюється кожним відділом, який розробляє докладні плани забезпечення безпеки у своїй зоні відповідальності; для захисту інформації потрібні певні дані, які об’єктивно заслуговують на захист, втрата яких може завдати істотних збитків організації; методи та засоби захисту повинні надійно блокувати можливі шляхи несанкціонованого доступу; ефективність захисту інформації означає, що вартість її реалізації не повинна перевищувати можливі втрати від реалізації інформаційних загроз; чітко визначені повноваження та права користувачів на доступ до певних видів інформації; надання користувачеві мінімальних дозволів на виконання

Тому система захисту має мати певні види власного забезпечення: юридичне забезпечення, тобто нормативні документи, положення, інструкції; організаційне забезпечення, тобто здійснення захисту інформації окремими структурними підрозділами, тобто службою безпеки, службою безпеки, службою захисту інформації, технічними засобами; обладнання; інформаційна підтримка; програмне забезпечення; математичне програмне забезпечення; нормативно-методичне та ергономічне забезпечення. Тому зміст складових елементів, методів та засобів захисту інформаційних ресурсів у будь-якій системі безпеки має постійно змінюватися з метою запобігання їх розголошенню заінтересованою особою.

Використана література

1. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. Х.: ХНЕУ, 2018. 510 с.

2. Лобода О.М., Кириченко Н.В. Базові комунікаційні технології: навч. посіб. Херсон: Стар, 2018. 235 с.

3. Лобода О.М. Захист інформації в корпоративних мережах. Публічне управління та адміністрування у процесах економічних реформ: матеріали IV Всеукр. наук.-практ.конф., м. Херсон, 11 листопада 2020 р. ХДАЕУ, 2020. С. 61-63.

Чепура М.М. – здобувач вищої освіти першого (бакалаврського) рівня, Херсонський державний аграрно-економічний університет
Кириченко Н.В. – к.е.н., Херсонський державний аграрно-економічний університет

ОСОБЛИВОСТІ СОЦІАЛЬНО-ЕТИЧНОГО МАРКЕТИНГУ В УМОВАХ ВОЄННОГО ТА ПОВОЄННОГО ПЕРІОДІВ

Сучасний світ нерідко стикається з воєнними конфліктами та повоєнними періодами, які супроводжуються серйозними викликами та змінами у всіх сферах життя. Воєнні дії не тільки руйнують інфраструктуру та загрожують безпеці людей, але й залишають після себе негативні економічні, соціальні та екологічні наслідки. У таких непростих умовах підприємства стикаються зі складним завданням відновлення та розвитку, а також забезпечення стійкості та конкурентоспроможності.

Однак, підприємства мають можливість не тільки відновлюватись після конфлікту, але й позитивно вплинути на суспільство та сприяти його розвитку. В цьому контексті соціально-етичний маркетинг стає ключовим інструментом, що допомагає підприємствам впливати на громадськість, розбудовувати стосунки зі зацікавленими сторонами та вирішувати соціальні проблеми.

Розуміння та урахування особливостей соціально-етичного маркетингу в умовах воєнного та повоєнного періодів є важливим кроком для підприємств у напрямку сталого розвитку та позитивного впливу на суспільство.