2. Капля А. В. «Кібербезпека як важливий аспект сьогодення».
3. URL:https://www.5.ua/suspilstvo/kiberbezpeka-derzhavy-chomu-tse-vazhlyvo-ta-stosuietsia-navit-prostykh-hromadian-siuzhet-220414.html
4. Лісовська Ю.П. КІБЕРБЕЗПЕКА: РИЗИКИ ТА ЗАХОДИ. 272с.

УДК 004.056

Зінченко Б.В., студент 4 курсу спеціальності 122 «Комп'ютерні науки»
Січко Т. В., к.т.н., доцент, доцент кафедри інформаційних технологій

ЦИФРОВІ РИЗИКИ ПІДПРИЄМСТВА ЕЛЕКТРОННОЇ ТОРГІВЛІ

Донецький Національний університет імені Василя Стуса, м. Вінниця

Під поняттям електронної комерції розуміють будь-який вид ділової активності суб'єктів господарювання, що провадиться з використанням сучасних інформаційних технологій, систем та комунікаційних засобів з метою отримання прибутку та задоволення потреб споживачів.

Електронна комерція як система включає в себе: суб'єкти електронного бізнесу (виробники, продавці, посередники, покупці, споживачі), процеси (реалізація продукції та послуг, маркетинг, розрахункові операції тощо) та мережі (як внутрішньофірмові, так і глобальні).

Оскільки для вітчизняного ринку електронна комерція є досить новим явищем, як для виробника, так і для споживача важливо оцінити з одного боку ті вигоди, які принесе участь у електронному бізнесі, а з іншого – потенційні проблеми, що можуть постати на шляху їх взаємодії. Вважаємо, що є необхідним систематизація як переваг, так і проблем впровадження електронної комерції в розрізі її суб'єктів, оскільки один й той самий пункт для виробника може бути перевагою, а для споживача – проблемою чи навпаки

Брак часу у споживачів змушує все більше придбань робити через Інтернет, а це, в свою чергу, зумовлює ще більший розвиток електронної торгівлі завдяки появі нових її різновидів.

Особливих темпів розвитку і впровадження електронна торгівля отримала у зв'язку з пандемією COVID-19, яка потрясла економічні ринки та вплинула на повсякденне життя багатьох людей і компаній по всьому світу. Для великої кількості людей, що перебувають на самоізоляції, покупки онлайн стали фактом життя. Через вірус люди замовляють товари в Інтернеті, які вони зазвичай купують в магазині [1-2].

Ведення торгівлі в глобальній мережі Інтернет несе як свої переваги, так і недоліки – ризики для бізнесу.

Цифровий ризик – це ймовірність отримання прямих чи побічних збитків суб'єктом економічної діяльності внаслідок його функціонування у кіберпросторі.

Джерела виникнення операційних кібер-ризиків систематизували Й. Кебула та Л. Янг, виділивши чотири класи: дії людей; збій системи; помилки у внутрішніх процесах; зовнішні події.

За видами кібератаки на підприємство електронної торгівлі можна розподілити наступним чином:

1. Нецільові атаки – фішинг;
2. Цільові атаки – фінансове шахрайство, викрадення баз даних, DDoS-атаки, вимагання;
3. Внутрішні атаки – викрадення, знищення інформації, сприяння цільовим атакам.

У наслідок реалізації цифрових ризиків підприємство електронної торгівлі може уповільнити або зупинити бізнес-процеси, втратити конкурентну перевагу, втратити репутацію та отримати судові позови при крадіжці особистих даних.

За даними глобального огляду кількарічної давності, проведеного у 129 країнах об'єднанням ISACA, незалежною некомерційною міжнародною асоціацією, яка об'єднує спеціалістів з інформаційної безпеки, тільки 38% респондентів вважають, що вони підготовлені до кібернападів, 83% відносять кібернапади до однієї з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки [3].

Побоювання респондентів не були безпідставними і світ вразили масштабні кібератаки. Так у 2017 році по всьому світі було інфіковано більше 500 000 комп'ютерів вірусом шифрувальником WannaCry.

Для України 2017 рік також не був простим. Проти України відбулася масштабна хакерська атака, що проходила у декілька етапів. Розпочалась атака з компрометації системи оновлення програми для подання звітності до контролюючих органів та обміну документами між контрагентами в електронному вигляді M.E.Doc. Наступний етап відбувся з використанням різновиду вірусу Petya та спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Зараженню піддалися інформаційні системи Міністерства інфраструктури, Кабінету Міністрів, сайти Львівської міської ради, Київської міської державної адміністрації, кіберполіції та Служби спецзв'язку України [4].

Ці події показали всім необхідність дотримання кібербезпеки у будь-яких установах незалежно від їхнього розміру, оскільки жертвами атак були як малі приватні підприємства, так і державні установи. Проте, якщо підприємства й прийняли усі міри з дотримання кібербезпеки та ізоляції певних частин своєї локальної мережі від глобальної мережі Інтернет після 2017 року, то пандемія COVID-19 принесла нові кіберризики пов'язані з необхідністю надання можливості співробітникам працювати віддалено. Якщо раніше це було

поодиноке явище, то під час пандемії воно прийняло масовий характер. Чому вірогідно були раді зловмисники. Більшість підприємств були вимушені відкрити доступ до своїх локальних мереж ззовні для роботи користувачів з дому. Це потенційно збільшує вірогідність зламу мережі підприємства через домашній пристрій користувача внаслідок не дотримання ним цифрової гігієни.

Висновки. Усе вищенаведене говорить про те, що злочинці ніколи не зупиняють свою діяльність, навіть під час пандемії. Тому відповідальним за кібербезпеку ні в якому разі не можна втрачати пильності і треба працювати над покращенням безпеки при роботі з дому, а користувачам обов'язково необхідно дотримуватися правил кібергігієни

Список використаної літератури

1. COVID-19: вплив на електронну комерцію. Юридична газета online. [Електронний ресурс] – Режим доступу : https://yur-gazeta.com/publications/practice/medichne-pravo-farmacevtika/covid19-vpliv-naelektronnu-komerciyu.html
2. Прямухіна О.-М. Д., Січко Т.В. Розвиток інтелектуальних технологій в умовах пандемій. Комп'ютерні технології обробки даних: матеріали всеукр. наук.-практ. конф., м. Вінниця, 2021. С. 47-49.
3. Стандарти ISO/IEC захистять від кіберзагроз. ДП «Укрметртестстандарт». [Електронний ресурс] – Режим доступу : http://csm.kiev.ua/index.php?option=com_content&view=article&id=3631%3A-isoiec---&catid=122%3A2015-09-15-07-01-23&lang=uk
4. Хакерська атака на Україну: подробиці. РБК-УКРАЇНА. [Електронний ресурс] – Режим доступу : https://www.rbc.ua/ ukr/news/hakerskaya-ataka-ukrainu-podrobnosti-1498566985.html

УДК 004.8

Комар Ю.О., студент 4 курсу спеціальності 122 «Комп'ютерні науки»
Потапова Н. А., к.е.н, доцент, доцент кафедри інформаційних технологій

ТЕСТУВАННЯ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ

Донецький Національний університет імені Василя Стуса, м. Вінниця

Занурюючись у діяльність оцифровування українських правил та переведення систем забезпечення життєдіяльності, ми стикаємось з новими проблемами безпеки інформаційних технологій.

Слід зазначити, що на сьогодні інформаційні технології є невід'ємною частиною майже всіх сфер сучасного суспільства. За всіма оцінками експертів, до теперішнього часу склалася ситуація, коли можливості і стійкість