УДК 004.056

Денисюк В.В., студент 2 курсу спеціальності 125 «Кібербезпека»
Зелінська О.В., к.т.н., доцент, доцент кафедри інформаційних технологій

ВАЖЛИВІСТЬ КІБЕРБЕЗПЕКИ В СУЧАСНОМУ СВІТІ

Донецький національний університет імені Василя Стуса, м.Вінниця

Поява та розвиток новітніх технологій мають дуже гарний вплив на суспільство. Вони полегшили людям життя, але разом із тим також прийшов великий ризик, оскільки з'явилася велика загроза різних кібератак [1]. Проте через небачене досі поширення інформаційних комп'ютерних технологій світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу.

Кібербезпека – це захист усіх електронних даних та інформації, що зберігається на електронних носіях. Кібернетична безпека захищає електронні системи на комп'ютерах, мобільних телефонах, серверах і мережах від зловмисних атак [2]. Незалежно від того, хто ви і яка ваша мета, захист особистих даних від несанкціонованого входу дуже важливий.

Можна навести ряд причин, чому все таки важлива інформаційна безпека у кіберпросторі.

Перша причина – це те, що існують різні типи кібератак. В даний час ніхто на планеті немає сто відсоткового захисту від кіберзлочинців. Ці атаки включають зловмисне програмне забезпечення, фішинг, атаки " людина посередині" та атаки "проїжджаючий поряд". Це справді страшно, адже у будь-яку хвилину ти можеш стати об'єктом злочину. Але на сьогоднішній день, основою метою великих кіберзлочинів є крадіжка криптовалюти [3]. Саме для цього зловмисники можуть використати ваш комп'ютер для крадіжки таких ресурсів, як біткойн та інші цифрові валюти. Якщо вони зможуть отримати доступ до вашого комп'ютера, вони можуть легко викрасти ваші особисті дані.

Друга причина - це швидке зростання числа кіберзлочинців. Швидкий розвиток технологій, з метою створення кращих гаджетів та хмарних сховищ, призвів до збільшення кількості підключених пристроїв. Згідно з статистичними даними, у 2021 році в усьому світі зафіксовано приблизно 21,1 мільярда мережевих пристроїв [1]. З розвитком темної мережі це створило сприятливий ґрунт для кіберзлочинної діяльності.

Третя причина, що технічні користувачі вразливі. Фактично, майже всі на планеті зараз більше покладаються на інформаційно-комунікаційні технології, а це є ознакою того, що кримінальні можливості для кіберзлочинців стрімко розвиваються [4]. Такі фактори, як розширення хмарного сховища та зростання

соціальних мереж, зробили багатьох людей вразливими до кібератак. Це робить кібербезпеку важливішою, ніж будь-коли.

Четвертою причиною є те, що хмарні сховища потребують безпеки та захисту. Сьогодні усі зберігають важливу інформацію таку як: банківські реквізити та паролі на електроних носіях [1]. А це в свою чергу збільшує ризик того, що ваша інформація буде вкрадена. Також кількість соціальних мереж та людей, що ними користуються з кожним днем зростає і це призводить до збільшення кількості шахраїв, які постійно хочуть викрасти ваші дані або кошти.

П’ята причина - це заощадження коштів. Згідно з останніми проведеними дослідженнями, середня вартість кіберзлочинів для середньостатистичної організації в минулому році склала близько 13 мільйонів доларів. Дослідження також виявило різке збільшення випадків витоку різної інформації, включаючи фінансову інформацію, медичні записи, комерційну таємницю, персональні дані та інтелектуальну власність [2]. Ви швидше заплатите трохи за кібербезпеку і заощадите на захисті своєї організації, ніж втратите цілий статок через промислове шпигунство.

Шоста – забезпечення довірою. В основному кібератаки часто роблять онлайн-платформи, такі як веб-сайти. Це може призвести до поганої репутації, адже після такого буде менше відвідувачів, і таку помилку буде важко виправити. Отже, кібербезпека важлива для захисту вашої платформи від таких ризиків. Це також може допомогти захистити клієнтів від потенційних хакерів.

Сьомою причиною є віруси, які можуть завдати шкоди і вам, і вашому бізнесу [1]. Комп'ютерні віруси можуть поширюватися зі швидкістю світла, ви не встигнете зрозуміти навіть що сталося. Це може призвести до серйозних проблем для вас і вашого бізнесу, якщо їх не контролювати. Комп'ютерні віруси здатні пошкодити ваші файли і системи. Тому дуже важливо серйозно ставитися до кібербезпеки, оскільки вона може захистити ваші комп'ютерні системи від вірусів.

Восьма причина – це темна сторона інтернету або «DarkNet». Розвиток новініх технологій не залишили й темну сторону інтернету. Темний інтернет або темна сторона інтернету - це секретна мережа інтернет-сайтів, доступ до якого можливий лише через спеціалізовані веб-браузери [3]. В основному цю мережу використовуєть для приховування інтернет – активності, збереження анонімності та конфіденційності користувачів.

Отже, кібербезпека дуже важлива для людей 21 століття. Оскільки вона захищає вас або вашу компанію від потенційних кіберзагроз. Заходи щодо протидії кіберзлочинності вживаються, але їх не достатньо, тому необхідно розробляти нові методи боротьби, що будуть давати більш явні результати, а також вдосконалити системи захисту, які виступатимуть як методи загальної превенції. Нашій державі необхідно посилити безпеку в інтернет-просторі, оскільки в сьогоднішніх реаліях цей напрям є пріоритетним у внутрішній і зовнішній політиці.

Список літературних джерел.

1. URL: https://hakin9.org/8-reasons-cyber-security-is-important/

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.