науково-технічної конференції, 23–24 квітня 2020 року. Тернопіль : ТНТУ, 2020. С. 154.

3. Єзова С. А. Про нетикет, цифровий етикет і нову етику в навчальному процесі [Електронний ресурс]. *Культура: теорія та практика*. 2021. № 1 (40). URL: https://cyberleninka.ru/article/n/o-netikete-tsifrovom-etikete-i-novoy-etikev-uchebnom-protsesse.

УДК: 658.012.8

Хомюк Наталія,
д.е.к., доцент кафедри економіки, підприємництва та маркетингу,
Волинський національний університет імені Лесі Українки,
м. Луцьк, Україна

Никончук Людмила,
студентка четвертого курсу факультету економіки та управління,
Волинський національний університет імені Лесі Українки,
м. Луцьк, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ РОЗВИТКУ МЕРЕЖЕВОЇ ЕКОНОМІКИ

Інформаційна безпека є дуже важливою в умовах розвитку мережевої економіки. З розвитком технологій та зростанням кількості цифрових даних захист інформації стає все складнішим завданням. У такому середовищі збільшується ризик кібератак, крадіжки даних, витоків інформації, шахрайств та інших кіберзлочинностей.

Основні складові інформаційної безпеки в мережевій економіці включають захист від кібератак, захист від вірусів та інших шкідливих програм, захист від неправомірного доступу до інформації, збереження конфіденційності даних та захист від крадіжки інтелектуальної власності.

Основа мережевої економіки – це мережеві організації, саме вони і допомагають робітникам працювати та спілкуватись між собою та здійснювати свою діяльність. Саме тому, головним завданням є забезпечення захищеного здійснення співпраці робітників під час використання мереж.

Сьогодні всі підприємства використовують технології у введенні бізнесу, таким чином, з'явилась потреба нових посад та нових професій, а саме таких, як спеціаліст з кібербезпеки. Саме ці працівники забезпечують технологічну роботу підприємства, а також контролюють та здійснюють захист організації від витоку конференційної інформації.

У зв'язку з цим компанії та організації, які працюють у мережевій економіці, повинні розробляти та випускати ефективні заходи безпеки, які забезпечують захист їхньої інформації. Ці заходи повинні включати різноманітні технології, такі як захист від кібератак за допомогою фаєрволів та інших програмних засобів, шифрування даних, засоби автентифікації та контролю доступу.

Так як, загроз у мережевому світі є безліч, то можна їх поділити на зовнішні та внутрішні, кожна з цих груп додатково розподіляється на навмисні та випадкові, явні та приховані. Виявлення цих загроз допомагає при побудові систем захисту в середині підприємства. Саме тому, говорячи про інформаційну безпеку, ми маємо на увазі захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, в тому числі власникам і користувачам інформації і підтримуючої інфраструктури [1].

Важливо зазначити, що отримати успіх у забезпеченні інформаційної безпеки можна лише шляхом здійснення комплексного системного підходу. Сутність безпеки у використанні таких мереж – це безпосереднє забезпечення доступності, цілісності, конфіденційності та підтримці інформаційних ресурсів їх інфраструктури.

Якщо говорити про поняття інформаційної безпеки мереж, то важливо звернути увагу на те, що вона має певні необхідні критерії, а саме надійну роботу комп'ютера, захист матеріалів від несанкціонованого доступу, збереження даних цілими, а також таємницю робочого листування в середині колективу. Отже, до основних завдань систем інформаційної безпеки відносять виявлення та усунення загроз безпеки нанесенню економічного, фінансового, матеріального та морального збитку; створення механізмів реагування на загрози розвитку і функціонуванню підприємства та національній безпеці; прийняття заходів щодо забезпечення безпеки персоналу підприємства та інше.

Як зазначалось вище, інформаційні мережі піддаються великій кількості загроз, які класифікують за обумовленістю факторів на природні та людські фактори. Наприклад, до природних факторів слід відносити такі, що носять об'єктивний і абсолютний характер, поширюється на всіх, тому до них можна віднести стихійні лиха [2]. Такі джерела загроз абсолютно не піддаються прогнозуванню, а отже, заходи захисту від них повинні застосовуватися завжди. В свою чергу, до людських факторів слід відносити випадкові дії та навмисні дії, що здійснюються людиною до потоків інформаційних мереж. Таким чином, говорячи про випадкові фактори, ми маємо на увазі помилки обробки, передачі, обміну інформації, а говорячи про навмисні загрози – помилки, що призводять до шкідливих наслідків користувачам автоматизованих інформаційних систем. Навмисні загрози – це ті загрози, які можна спрогнозувати, тому працівники відділів інформаційної безпеки підприємств завжди працюють на результат та прагнуть розробити таку систему здійснення робочих процесів, щоб мінімізувати пасивні та активні загрози цього виду перешкод.

Захищена мережа може допомогти уникнути цих проблем та захистити важливу інформацію від несанкціонованого доступу. Для досягнення цього можна використовувати різноманітні заходи безпеки, такі як аутентифікація, авторизація та шифрування даних. Також можна використовувати системи виявлення та захисту від кібератак, які перевірені вчасно виявити та зупинити атаки [3; 4].

Однак захист інформаційних мереж є складним процесом, який потребує постійного оновлення та удосконалення. Кіберзлочинці постійно шукають нові способи атаки, тому необхідно завжди бути в курсі останніх трендів та технологій в області кібербезпеки.

Отже, сьогодні питання захисту інформаційних мереж є досить актуальним. Захищенні інформаційні мережі на підприємстві запорука ефективної діяльності, що безпосередньо впливає на економіку країни. З кожним днем з'являються нові проблеми в інформаційному світі на що також впливає і науково технічний прогрес, саме тому здійснення захисту мереж є складним процесом, але необхідним.

Список використаних джерел:

1 Бурячок В. Л., Аносов А. О., Семко В. В., Соколов В. Ю., Складанний П. М. *Технології забезпечення безпеки мережевої інфраструктури*. К.: КУБГ, 2019. 218 с.

2 Рибальченко Л. В., Гребенюк А. М. *Основи управління інформаційною безпекою:* навч. посібник. Дніпро: Дніпроп. держ. Ун т внутріш. справ, 2020. 144 с.

3 Pavlikha N., Khomiuk N. Economic security of development of rural territories in Ukraine. *International Journal of New Economics and Social Sciences*. 2018. № 1(7). p. 119-130.

4 Павліха Н. В., Войчук М. В. Концептуальні засади безпеки сталого просторового розвитку: теоретико-методологічний аспект. *Міжнародна економічна безпека України: теорія, методологія, практика* : колективна монографія / за наук. ред. Кравчука П. Я. Луцьк : ІВВ Луцького НТУ, 2020. С. 161–183.

УДК: 331.108.2"364"

Науменко Наталія,
к.е.н., доцент,
доцент кафедри міжнародних економічних відносин
та управління проєктами,
Волинський національний університет імені Лесі Українки,
м. Луцьк, Україна

Савко Богдан,
студент третього курсу Українсько-польської програми
«Крок до Євроінтеграції»
Вищої школи суспільно-господарчої,
м. Пшеворськ, Польща

УДОСКОНАЛЕННЯ ІНДИВІДУАЛЬНИХ ПАРАМЕТРІВ ЕФЕКТИВНОГО КЕРІВНИЦТВА ОРГАНІЗАЦІЄЮ В УМОВАХ ВІЙНИ

Російсько-українська війна посилила потребу у відборі і підготовці вмотивованого персоналу. Великі соціальні зрушення, що відбуваються нині в нашій держав призвели і до фізичного пересування кваліфікованих кадрів. Часто це відбувається не з волі