УДК 004.42

ДО ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Мірошниченко М.Ю., к.т.н. **mykola.miroshnychenko@tsatu.edu.ua**

Таврійський державний агротехнологічний університет імені Дмитра Моторного

Актуальність та постановка проблеми. Сьогодні інформаційні ресурси набуваються важливого значення у розвитку економіки, суспільства, держави тощо. Водночас інформація стала стратегічним ресурсом підприємства, яка впливає на його функціонування та подальший розвиток. Поряд із виробничими та маркетинговими процесами, інформаційне середовище є невід'ємною складовою бізнес-середовища підприємства. Тому підтримка інформаційного середовища в актуальному та працездатному стані є важливим завданням, що повинно вирішуватися на підприємстві.

Зазвичай, обробка та зберігання інформації на підприємстві відбувається за допомогою інформаційних систем, що відрізняються функціональністю, вартістю, іншими характеристиками. Пошкодження або втрата інформації може негативно вплинути на окремі процеси, що відбуваються усередині підприємства. Особливо, якщо це стосуються несанкціонованого втручання до інформаційного середовища підприємства з боку зловмисників. Тому актуальним питанням є забезпечення належного захисту інформаційних систем та інформації, що в них зберігається та обробляється.

Основні матеріали дослідження. Сучасні інформаційні системи знайшли своє використання під час управління проєктами, бізнес-планування інвестиційних проєктів, прийнятті управлінських рішень. З'являються нові типи інформаційних систем, зокрема інтелектуальні інформаційні системи [5, с. 25], які використовуються елементи штучного інтелекту для прийняття ефективних рішень. Водночас з урахуванням постійного технологічного розвитку очікується поява більш складних, багатовимірних інформаційних систем [4, с. 62].

Залежність підприємств від різного роду систем, у тому числі інформаційних, призвели до підвищення вимог до інформаційної безпеки. Це пояснюється розвитком сучасних апаратно-програмних засобів обробки та передачі інформації, появою нових методів та засобів обробки інформації [2, с. 553], посилення впливу інформації на розвиток підприємства. Порушення режиму безпеки інформаційного середовища може відбуватися через зовнішні або внутрішні джерела, спеціально або ненавмисно, здійснюватися фахівцями або звичайними співробітниками, які мають низький рівень інформаційної культури. Дії зловмисників можуть призвести до крадіжки економічної, виробничої та персональної інформації, втрати даних, збоїв у роботі обладнання та програмного забезпечення [1, с. 250] тощо. У будь-якому випадку, незадовільний рівень інформаційної безпеки, зокрема системи захисту інформаційних систем підприємства, становить загрозу для функціонування підприємства [3, с. 157].

Захищена інформаційна система повинна мати механізми захисту від внутрішніх та зовнішніх загроз, відповідати загальноприйнятим стандартам, що стосуються захисту інформації, забезпечувати безпечну обробку та передачі інформації. Як наслідок, захист інформації на підприємстві, зокрема в інформаційних системах, не повинен зводитися до вибору окремих засобів або методів захисту. Іноді це може призвести до конфліктів мж різним програмним забезпеченням і, як наслідок,

зниження рівня безпеки та працездатності інформаційної системи [4, с. 64]. Процес захисту інформації повинен бути заснований на системному підході, принципах комплексності та адаптивності [2, с. 552], здійснюватися упродовж всього життєвого циклу програмного забезпечення.

В даному випадку потрібно комплексно підійти до вирішення проблеми та її уникнення в майбутньому. Слід забезпечити реалізацію низки юридичних, технологічних та організаційно-економічних заходів [3, 158], застосовувати апаратно-програмні засоби для ідентифікації користувачів в системі та розподілу між ними повноважень щодо використання сервісів та ресурсів [2, с. 554], використовувати програмні засоби для захисту від мережевих атак з боку зловмисників [6, с. 139]. Також доречно періодично проводити інформування співробітників підприємства щодо важливості інформаційної безпеки.

Слід зазначити, що проектування системи захисту інформаційних систем є складним та комплексним завданням, що передбачає врахування потенційних загроз, характерних для конкретного підприємства, вартості апаратно-програмного забезпечення високий рівень кваліфікації розробників та ін. На думку С. Толюпи та І. Пархоменко, система захисту інформації повинна бути реалізована на п’яти функціональних рівнях: фізичному технологічному, користувацькому, мережевому, управлінському. Використання багаторівневого захисту інформаційних систем дозволить спросити процес проектування системи захисту, формалізувати окремі завдання, розмежувати вимоги до конфіденційності та цілісності інформації [4, с. 65].

Висновок. Отже, інформаційні системи успішно застосовуються на підприємствах та забезпечують ефективну діяльність. В умовах розвитку інформаційного суспільства підвищуються вимогу до безпеки інформації, що циркулює всередині підприємства. Захист інформаційних систем повинен бути заснований на системному підході та передбачати комплексне застосування засобів та методів засобів.

Список використаних джерел

1.Делембовський М., Шабала Є., Терентьєв О. Аналіз методів та шляхів вирішення захисту інформації в інформаційно-телекомунікаційних системах. Грааль науки. 2021. №1. С. 249–254.

2.Рудий Т. В., Томаневич Л. М., Руда О. І. Засади захисту інформації в інформаційних системах підприємств. Актуальні проблеми економіки. 2014. №2. С. 551–557.

3.Северина С. В. Інформаційна безпека та методи захисту інформації. Вісник Запорізького національного університету. Економічні науки. 2016. №1. С. 155–161.

4.Толюпа С. В., Пархоменко І. І. Побудова комплексних систем захисту складних інформаційних систем на основі структурного підходу. Сучасний захист інформації. 2015. №4. С. 62–70.

5.Шаров С.В. Лубко Д.В., Осадчий В.В. Інтелектуальні інформаційні системи: навч. посіб. Мелітополь: Вид-во МДПУ ім. Б. Хмельницького, 2015. 144 с.

6.Шаров С. В., Лубко Д. В. Розробка та використання сніферу як засобу забезпечення безпеки ТСР з’єднань. Системи обробки інформації. 2017. № 5. С. 138–144.