УДК 004:681.5:697.7

ЗАХИСТ КОМП'ЮТЕРНИХ СИСТЕМ

PROTECTION OF COMPUTER SYSTEMS

Андрій Яцюк, Сергій Музичук, Світлана Яцюк

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *The main directions of information protection in computer systems have been researched, including technical, organizational, and legal aspects.*

Захист комп'ютерних систем та оброблюваної інформації в них є критично важливим аспектом інформаційної безпеки. Наведемо основні напрями захисту інформації.

1. Захист від несанкціонованого доступу. Сюди можна віднести аутентифікацію, авторизацію, шифрування, контроль доступу, журналювання та моніторинг.

2. Захист від витоку інформації через технічні канали, а саме, оптичні, акустичні, побічні електромагнітні випромінювання, наведені електромагнітні поля на провідниках і елементах системи.

Під час розробки комп'ютерної системи важливо дотримуватись захисту інформації на усіх етапах її життєвого циклу: планування та створення системи з урахуванням вимог безпеки, інсталяція системи та налаштування засобів захисту, підтримка системи в робочому стані, регулярне оновлення та моніторинг безпеки, безпечне знищення або зберігання даних при припиненні використання системи [2].

Для обробки інформації, яка підпадає під регулювання законодавства, необхідно отримати дозвіл від відповідного уповноваженого державного органу. Це досягається через проходження експертизи на відповідність системи встановленим нормам та критеріям безпеки, таким як НД ТЗІ 2.5-004-99 [3].

Кожен компонент обчислювальної системи може бути незалежно сертифікований на відповідність вимогам безпеки. Це включає апаратні засоби, програмні засоби та засоби захисту інформації. Наявність сертифікатів підтверджує потенційні можливості компонентів у забезпеченні захисту, але для повної інтеграції та реалізації всіх необхідних функцій захисту потрібне відповідне проектування та налаштування всієї системи [1].

Таким чином, забезпечення інформаційної безпеки в КС є складним процесом, що включає технічні, організаційні та юридичні аспекти. Це вимагає координації між різними компонентами системи, регулярного моніторингу та оновлення засобів захисту відповідно до нових загроз та вразливостей.

Бібліографія

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. Львів: «Новий Світ- 2000», 2020 . 678 с.
2. Когут Ю.І. Кібервійна та безпека об'єктів критичної інфраструктури [практичний посібник] / Ю.І. Когут; за редакцією доктора тех., наук, проф. А.С.Довгополого. Київ: Консалтингова компанія «СІДКОН»; ВД Дакор, 2021. 332 с.
3. Когут Ю.І. Корпоративна безпека: практичний посібник/Ю.І. Когут. Київ: Консалтингова компанія «СІДКОН», 2021. 460 с.