ВСТУП

Упровадження інформаційних технологій у всі сфери життєдіяльності сучасного суспільства, бурхливий розвиток глобальних інформаційних і телекомунікаційних систем, обумовлюють постійно зростаючу роль різноманітних інформаційних ресурсів і, як наслідок, визначають необхідність їхнього захисту як одного з чинників забезпечення безпеки особистості, суспільства, держави. Реалії сучасного інформаційного суспільства показують, що жодна сфера життя цивілізованої держави не може ефективно функціонувати без розвиненої інформаційної інфраструктури, широкого застосування апаратно-програмних засобів, мережевих технологій опрацювання та обміну інформацією. По мірі зростання цінності інформації, розвитку та ускладнення засобів її опрацювання та обміну безпека суспільства все більшою мірою залежить від безпеки використовуваних технічних засобів.

Відомим недоліком наявних інформаційних систем є принципова можливість доступу до інформації з боку осіб, для яких вона не призначена. Забезпечення адекватної та випереджальної протидії загрозам безпеки інформації – одна з найважливіших умов забезпечення політичної, економічної, оборонної та інших складових національної безпеки держави. На сьогодні методи захисту інформації мають величезне значення у кредитно-фінансовій сфері, бізнесі, під час зберігання конфіденційної інформації та її передавання незахищеними каналами зв'язку.

Важливою особливістю інформаційних ресурсів є те, що захист інформації необхідно забезпечувати на всіх етапах – від її виникнення до зберігання та передавання. Водночас протидіяти загрозам безпеки інформації необхідно комплексно, що вимагає від фахівця з інформаційної безпеки ґрунтовних теоретичних знань та практичних навиків з кожної зі сфер:

– криптографія – наука про захист інформації від прочитання її сторонніми особами. Захист досягають шляхом деякого перетворення вихідних даних, що робить їх складними для читання без знання спеціальної інформації (криптографічного ключа);

– безпека мережі – розглядає способи захисту (як апаратні, так і програмні) від несанкціонованого доступу до віддаленого вузла за допомогою мережевих технологій;

– захист від несанкціонованого копіювання – запобігає використанню неліцензованих копій програмного забезпечення та захищає права розробників;

– антивірусологія – наука про способи боротьби з комп'ютерними вірусами та іншими програмами, що самопоширюються, спрямована на забезпечення й підтримку цілісності даних, які зберігаються;

– системний захист – комплекс апаратних та програмних засобів, спрямованих на забезпечення цілісності та недоступності даних у разі відмови техніки, помилкових дій та інших причин стихійного характеру.

Сучасні системи захисту будуються за багаторівневою схемою, що дає змогу комплексно використовувати різноманітні засоби й методи захисту, підвищуючи загальну ефективність системи в разі зниження витрат за її організацію та обслуговування. Кожен рівень системи захисту може своєю чергою ділитися на низку підрівнів, що тісно взаємодіють між собою. До того ж окремий підрівень будується з врахуванням одного чи сукупності різних прийомів захисту, вкладених у захист від конкретної загрози.

Можна впевнено стверджувати, що створення ефективної системи захисту інформації сьогодні цілком реальне, а надійність захисту інформації насамперед визначатиметься повнотою вирішення цілого комплексу завдань, про які йтиметься в цьому навчальному посібнику.

Матеріал, викладений у навчальному посібнику, дасть змогу студентам оволодіти знаннями та вміннями, які створять теоретичне й практичне підґрунтя для отримання компетентностей щодо проведення аналізу загроз, які виникають під час зберігання, опрацювання та передавання інформації, побудови систем захисту, демонстрації здатності критично вивчати, аналізувати й оцінювати з різних точок зору: технології, методи та процедури для проєктних робіт, пов'язаних із розробленням профілю безпеки, надання порівняльної характеристики різних варіантів застосування механізмів і протоколів захисту інформації в інформаційних системах, забезпечення обґрунтованого підбору програмно-апаратних і програмних засобів для забезпечення необхідного рівня захисту інформації, проведення аналізу ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах.