МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

С.Е. Остапов, С.П. Євсеєв, О.Г. Король

КІБЕРБЕЗПЕКА :
СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ

Навчальний посібник

«Новий Світ-2000»
Львів
2020

УДК 004.056.5(076.5)

Рекомендовано до видання рішенням вченої ради Харківського національного економічного університету

Рецензенти:

Дудикевич В.Б. докт. техн. наук, професор, зав. кафедри захисту інформації Національного університету "Львівська політехніка";

Поморова О.В. докт. техн. наук, професор, зав. кафедри системного програмування Хмельницького національного університету;

Виклюк Я.І. докт. техн. наук, проректор з наукової роботи та міжна-родних зв'язків ПВНЗ "Буковинський університет".

Автори: доктор фізико-математичних наук, професор С.Е. Остапов (вступ, розділи 1 – 3, 8, 9); доктор технічних наук, старший науковий співробітовик С.П. Євсеєв (розділи 4, 5, 7, 10); кандидат технічних наук О.Г. Король (розділи 6, 11 – 13).

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.

У пропонованому виданні викладені основи сучасного захисту інформації в комп'ютерних системах, не пов'язаних з державною таємницею. Посібник складається з теоретичного матеріалу та лабораторного практикуму. У теоретичній частині висвітлено основні поняття й подані визначення, які стосуються захисту інформації, формування політики безпеки. Розглянуто критерії оцінки захищеності комп'ютерних систем, основи криптографічного захисту інформації, захист інформації від несанкціонованого доступу в сучасних операційних системах, описано комплексні системи захисту в корпоративних інформаційних системах.

Для студентів, які навчаються за галуззю 12 – «Інформаційні технології» всіх форм навчання, інших спеціальностей, де вивчається цикл дисциплін захисту інформації, а також для самостійного опанування його основами.

ISBN 978-617-7519-44-6

ЗМІСТ

ВСТУП

Захист інформації перетворюється сьогодні на одну з найактуальніших задач унаслідок надзвичайно широкого розповсюдження як власне різноманітних систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передається величезний обсяг інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення з нею сторонніх осіб. Проблема набула особливої гостроти після прийняття урядом України закону про захист персональних даних, який зобов'язує зберігати та передавати персональні дані працівників лише в захищеному вигляді.

Не менш важливим завданням вважається широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, уведення електронних паспортів та медичних карт, студентських квитків та залікових книжок. Зрештою, дедалі більше державних установ і приватних підприємств переходять на електронний документообіг, який до того ж вимагає юридичної чинності підписів фізичних або юридичних осіб. Розповсюдження таких технологій також, безперечно, вимагає добре поставленого захисту інформації.

Усі ці та багато інших задач покликані розв'язувати різноманітні технології захисту інформації.

Навчальний посібник, що пропонується читачеві, містить систематичний опис основ захисту інформації. Він складається зі вступу, тринадцяти розділів і лабораторного практикуму.

Перший розділ присвячено основним поняттям та визначенням курсу захисту інформації. Тут висвітлено властивості інформації, розглянуто захист інформації як галузь людської діяльності та його основні завдання, подано класифікацію основних загроз для інформації та їх джерел.

У другому розділі вивчаються основні поняття політики інформаційної безпеки, аналізуються моделі загроз і модель порушника, подано методику оцінки ризиків підприємства.

Розділи з третього по дев'ятий містять основи криптографічного захисту інформації, де розглядається симетрична й асиметрична криптографія, хешувальні алгоритми та електронний цифровий підпис,

елементи криптоаналізу, основні напрямки розвитку сучасної криптографії.

У наступних розділах описані механізми та протоколи керування криптографічними ключами, методи та пристрої забезпечення безпеки, а також моделі захисту й використання механізмів контролю доступу.

Вивчення навчальних дисциплін циклу захисту інформації дозволить студентам, що навчаються за галуззю знань 12 - "Інформаційні технології" усіх форм навчання, оволодіти знаннями та вміннями, які створять теоретичне та практичне підґрунтя для отримання компетенцій із проведення аналізу загроз, що виникають при зберіганні, обробці та передаванні інформації; побудові систем захисту з використанням методів традиційної криптографії; демонструвати здатність критично вивчати, аналізувати й оцінювати з різних точок зору: технології, методи та процедури для проектних робіт, пов'язаних з розробкою профілю безпеки, давати порівняльну характеристику різних варіантів застосування механізмів та протоколів захисту інформації в комп'ютерних системах, забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації, проводити аналіз ефективності технічних рішень щодо забезпечення захисту інформації в інформаційних системах.

Навчальний посібник узагальнює окремі методичні розробки з навчальних дисциплін "Захист інформації в інформаційних системах", "Технології захисту інформації", "Безпека програм та даних" і містить систематизований навчальний матеріал у галузі інформаційної безпеки для вивчення теоретичного матеріалу та набуття практичних навичок як самостійно, так і під керівництвом викладача.

Книга призначена для студентів, які навчаються у вищих навчальних закладах за спеціальностями: 121 –"Інженерія програмного забезпечення" , 123 – "Комп'ютерна інженерія" та 122 – "Комп'ютерні науки", а також може бути корисною для усіх інших спеціальностей та освітньо-професійних програм, в межах яких викладаються дисципліни, пов'язані з інформаційною безпекою. Звичайно, корисною ця книга буде й особам, що займаються освітою самостійно.

Розділ 1. Огляд безпеки системи

1.1. Основні поняття

Вже давно інформація стала загальнолюдським надбанням, однак досі не існує загальнонаукового визначення цього поняття. З точки зору різних галузей науки, це поняття набуває різних специфічних ознак. Вікіпедія, наприклад, дає таке тлумачення інформації [1-2]: **інформація** – це відомості про щось незалежно від форми їх подання. Сучасна наука розглядає два типи інформації: об'єктивна – властивості матеріальних об'єктів та явищ, які передаються іншим об'єктам і відображаються в їхній структурі; та суб'єктивна, яка відображає зміст об'єктивної інформації, сформована свідомістю людини за допомогою слів, образів і відчуттів та зафіксована на будь-якому матеріальному носієві. У побутовому розумінні інформація – це відомості про оточуючий світ і процеси, що в ньому відбуваються, які сприймаються людиною або спеціальним пристроєм.

До захисту інформації найближчими, на наш погляд, такі визначення інформації.

За Клодом Шенноном: *інформація* – це відомості, за допомогою яких усувається невизначеність, що існувала у споживача до їх отримання [45].

За В.М. Глушковим,: *інформація* – міра неоднорідності розподілу матерії та енергії у просторі та часі, міра змін, якими супроводжуються всі процеси, що протікають у світі [4].

Згідно з визначенням, яке надає ЮНЕСКО, *інформація* – універсальна субстанція, що пронизує всі сфери людської діяльності, служить провідником знань та думок, інструментом спілкування, взаєморозуміння та співробітовицтва, утвердження стереотипів мислення та поведінки.

Відповідно Закону України «Про інформацію», *інформація* – документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі [5].