ПЕРЕДМОВА

Навчальний посібник “Інформаційна безпека” спрямований на ознайомлення студентів із основними поняттями та визначеннями в галузі інформаційної безпеки. У ньому описано математичні основи криптології. Розглянуто відомі та сучасні методи криптографії, стеганографії, криптоаналізу. Висвітлено питання ідентифікації, автентифікації та санкціонованого доступу. Значну увагу в навчальному посібнику звернено на практичний захист інформації, розглянуто питання безпеки інформаційних систем, висвітлено особливості захисту програмного забезпечення в інформаційних системах. Розглянуто питання інформаційної безпеки підприємств та організацій. Особливу увагу приділено проектуванню, побудові та функціонуванню систем інформаційної безпеки.

Цей навчальний посібник відповідає навчальному плану підготовки бакалаврів і магістрів за спеціальностями 172 “Телекомунікації та радіотехніка”, 125 “Кібербезпека” та 163 “Біомедична інженерія”. Основою посібника є науково-методичні матеріали, напрацьовані його авторами під час викладання відповідних дисциплін у галузі інформаційної безпеки, що передбачені навчальними планами для підготовки студентів за згаданими вище спеціальностями.

Навчальний посібник “Інформаційна безпека” буде корисний усім охочим отримати або поглибити свої знання в галузі інформаційної безпеки та захисту інформації. Посібник складається з восьми розділів, що охоплюють:

– основні поняття та визначення в галузі інформаційної безпеки;

– математичні основи криптології;

– криптологію;

– стеганографію;

– ідентифікацію, автентифікацію, санкціонований доступ;

– безпеку інформаційних систем;

– захист програмного забезпечення в інформаційних системах;

– інформаційну безпеку підприємств та організацій, системи інформаційної безпеки.

Навчальний посібник підготували співробітники кафедри теоретичної радіотехніки та радіовимірювання Національного університету “Львівська політехніка” професори Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, співробітники кафедри безпеки інформаційних технологій Національного університету “Львівська політехніка” доценти С. С. Войтусік, І. М. Журавель, асистент О. А. Нємкова, співробітники кафедри захисту інформації Національного університету “Львівська політехніка” доценти А. Я. Горпенюк, Б. М. Березюк, В. І. Отенко, І. Я. Тишик та співробітник кафедри електронних засобів

інформаційно-комунікаційних технологій Національного університету "Львівська політехніка" доцент Є. І. Яковенко.

Авторами та співавторами окремих розділів підручника є:

загальне редагування та передмова – Ю. Я. Бобало;

загальне редагування – І. В. Горбатий;

розділ 1 – І. В. Горбатий, М. Д. Кіселичник;

розділ 2 – С. С. Войтусік;

розділ 3 – А. Я. Горпенюк, О. А. Нємкова, С. С. Войтусік;

розділ 4 – І. М. Журавель, О. А. Нємкова;

розділ 5 – С. С. Войтусік;

розділ 6 – І. В. Горбатий, А. П. Бондарєв, Б. М. Березюк, Є. І. Яковенко;

розділ 7 – В. І. Отенко, Є. І. Яковенко;

розділ 8 – І. В. Горбатий, І. Я. Тишик.

За слушні зауваження та поради, що сприяли поліпшенню змісту цього посібника, автори висловлюють подяку рецензентам: завідувачу кафедри захисту інформації Національного університету "Львівська політехніка", доктору технічних наук, професору Валерію Богдановичу Дудикевичу; професору кафедри безпеки інформаційних технологій Навчально-наукового інституту інформаційно-діагностичних систем Національного авіаційного університету, доктору технічних наук, професору Володимиру Олексійовичу Хорошку; завідувачу кафедри комп'ютерних та інформаційно-вимірювальних технологій Одеської державної академії технічного регулювання та якості, доктору технічних наук, доценту Надії Феліксовні Казаковій; заступнику головного конструктора Акціонерного товариства "Інститут інформаційних технологій", доктору технічних наук, професору Олександру Володимировичу Потію.

За сприяння в організації роботи над цим посібником автори вдячні завідувачеві кафедри безпеки інформаційних технологій Національного університету "Львівська політехніка", доктору технічних наук, професору Володимиру Миколайовичу Максимовичу.

Автори вдячні Андрію Едуардовичу Лагуну, кандидату технічних наук, доценту, доценту кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності за надані матеріали з математичних основ криптології.

Відповідальний редактор –
доктор технічних наук, професор Ю. Я. Бобало