ПЕРЕДМОВА

Питання безпеки – важлива частина концепції впровадження нових інформаційних технологій у всі сфери життя суспільства. Широкомасштабне використання обчислювальної техніки та глобалізація мереж спричиняють якісно нові можливості несанкціонованого доступу до ресурсів і даних інформаційної системи, тобто високу вразливість. Отже, забезпечення цілісності, достовірності та доступності інформації – важливі складові успіху діяльності будь-якої організації. Про важливість інформаційної безпеки в сучасному світі, світі постіндустріального інформаційного суспільства, свідчать, наприклад, лише такі інциденти безпеки світового масштабу, які трапились за останні півроку, як операція Carbanak, під час якої кіберзлочинці вкрали мільярд доларів зі 100 фінансових організацій по усьому світу; різноманітні версії шифрувальників-здирників, таких як Onion, здатні обходити механізми захисту багатьох антивірусних продуктів; фішингові атаки тощо.

Сучасна комп'ютерна безпека виконує надзвичайно широкий спектр завдань – від захисту спеціальних державних мереж до забезпечення закритої електронної пошти на домашньому комп'ютері. Вибір серед багатьох сучасних методів і засобів захисту таких, що найбільше відповідають конкретним умовам діяльності та гарантують достатній рівень безпеки, є достатньо складним завданням. Тому для спеціалістів різноманітного профілю в сучасних умовах є особливо актуальною підготовка в галузі захисту інформації. Саме для набуття відповідних знань та навичок майбутніми фахівцями з розроблення та тестування програм і призначений посібник "Безпека програм та даних". Сьогодні в концепції інформаційних технологій акцент зміститься на поняття інформації. До того ж сама інформація перетворюється на об'єкт, на захист якого спрямовані основні зусилля та ресурси багатомільйонної армії математиків, програмістів, фахівців з електроніки та інженерів. Методи захисту інформації динамічно розвиваються, ускладнюються та поступово оформлюються в окрему галузь інформаційно-комунікаційних технологій.

У теперешній час розвитку Інтернету, соціальних мереж, хмарних обчислень, кібернетичних війн тощо навіть найпростіші програмні

продукти мають інтеграцію з соціальними мережами, містять конфіденційну чи персональну інформацію, не кажучи вже про широку інтеграцію платіжних сервісів у значній кількості програм. Тому розуміння основних принципів інформаційної безпеки є надзвичайно важливим навіть для звичайних користувачів програмних засобів. Важливість розуміння цих принципів стократно зростає для розробників програмного забезпечення, які повинні не тільки розуміти основні сервіси та механізми захисту, але й грамотно й ефективно реалізовувати їх у програмних продуктах, ураховуючи характеристики алгоритмів, апаратного забезпечення та загальні нефункційні вимоги якості кінцевого програмного продукту. (Варто лише згадати вимкнення обов'язковості шифрування даних в Android Lollipop для старших версій апаратного забезпечення через проблеми продуктивності.) Навіть робота в галузі створення спеціалізованих програмних продуктів не звільняє програміста від відповідальності за захист і інформації, і програмного оточення – згадаймо, наприклад, дуже відомий свого часу вірус Stuxnet, який можна використати для несанкціонованого збору даних та диверсій у системах управління промисловими об'єктами, зокрема атомні станції. Тому дисципліна "Безпека програм та даних", вивченню якої сприятиме цей посібник, логічно завершує фаховий цикл підготовки бакалаврів з напряму "Програмна інженерія", що повинна надати необхідні знання та навички зі створення безпечних та ефективних програмних продуктів.

Структура цього посібника побудована так, щоб спочатку ознайомити читача з основними поняттями захисту інформації, видами порушень інформаційної безпеки та вивчити основні механізми безпеки: алгоритми традиційного шифрування та шифрування з відкритим ключем, хешування, аутентифікації інформації та цифрового підпису. Ці теоретичні відомості доповнюються практичними аспектами створення захищених програмних продуктів (розділи 16 та 17). Автори сподіваються, що посібник буде корисним читачам і для ефективного використання готових програмних засобів та захисту своїх персональних чи банківських даних, і для створення ефективних та захищених програмних засобів на задоволення вимог своїх клієнтів.