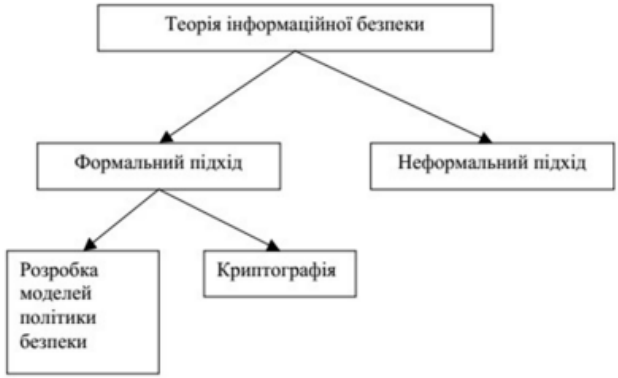
УДК 510.635:004.891(045)

А.В. Мельничук
Національна академія Служби безпеки України, Київ

ТЕОРІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодні інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, суспільство вже не може уявити свій день без гаджетів та Інтернету. Нині високотехнологічна злочинність набуває високих темпів. У зв'язку з цим виникає термінова потреба у створенні не тільки єдиного інформаційного простору, але й адекватного механізму організації інформаційної безпеки. Загалом об'єктами зазіхань можуть бути як технічні засоби (комп'ютери і периферія), так і програмне забезпечення та бази даних, для яких комп'ютер є середовищем. Небезпідставні побоювання викликають вразливості в програмному забезпеченні та в автоматизованих системах. Для зменшення цих ризиків необхідно вжити всіх необхідних заходів для поліпшення кібербезпеки. Аналіз інформаційних ризиків необхідний для визначення можливої шкоди (ризику) за існуючими видами цінної інформації, співвідношення ризику з витратами на забезпечення інформаційної безпеки, оцінки ефективності витрат на забезпечення інформаційної безпеки. Комплексна оцінка захищеності інформаційної системи, оцінка вартості інформації, оцінка ризику, розробка комплексної системи забезпечення інформаційної безпеки – основні завданнями аналізу. Тому метою аналізу інформаційних ризиків є розробка економічно ефективної і обґрунтованої системи забезпечення інформаційної безпеки. Критерії проведення аудиту інформаційної безпеки встановлюються на основі загальноприйнятих міжнародних стандартів (наприклад, міжнародний ISO 17799, німецький BSI і ін.), внутрішніх стандартів аудиторських компаній і вітчизняних відомчих стандартів. Важливий елемент організації інформаційної безпеки – поділ заходів захисту на групи. Основні групи заходів захисту інформації поділяють на активні засоби захисту (наприклад, розвідка, дезінформація, зашумлення), пасивні засоби захисту (наприклад, встановлення екранів несанкціонованому витоку інформації тощо) та комплексні засоби захисту (органічне поєднання названих груп). Визначення і перевірка стану безпеки є важливим шляхом реалізації заходів захисту інформації. Для

успішної розробки хорошої моделі безпеки необхідна наявність чітко визначеної політики безпеки. Визначення умов, яким повинно підкорятися поводження системи, створення критерію безпеки і проведення формального доведення відповідності системи цьому критерію при дотриманні встановлених правил – основна мета створення політики безпеки інформаційної системи. Зв'язок наведених напрямків теорії захисту інформації можна представити у вигляді схеми:



На даний час в Україні сформовано наукові школи з дослідження за різними сферами забезпечення кібербезпеки держави, насамперед, щодо планування і ведення кібероборони та кіберрозвідки, розслідування кіберзлочинів, відбиття кібератак та нейтралізації кіберзагроз; криптографічного та технічного захисту інформації; захисту в кіберпросторі державних інформаційних ресурсів; здійснення захисту та аудиту захищеності інформаційно-комунікаційних і технологічних систем об'єктів критичної інфраструктури держави на вразливість; відновлення сталості і надійності функціонування інформаційно-комунікаційних, технологічних систем після здійснення кібератак.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Захист систем електронних комунікацій: навч. посіб. / В. О. Хорошко, О. В. Криворучко, М. М. Браіловський та ін. Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.