УДК 004.056.5
М. Кузьо
(Тернопільський національний технічний університет імені Івана Пулюя)

ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ

UDC 004.056.5
M. Kuzyo
(Ternopil Ivan Puluj National Technical University, Ukraine)

ASSESSMENT OF INFORMATION SECURITY RISKS OF TERNOPIL NATIONAL TECHNICAL UNIVERSITY

Неконтрольований доступ до інформаційного ресурсу Вищого навчального закладу, стан інформаційної безпеки, низька захищеність від зовнішніх та внутрішніх загроз мають негативні наслідки – ризик порушення цілісності, доступності та конфіденційності інформації.

Визначення інформаційних ризиків – складне завдання.Усі методи оцінювання ризиків можна поділити на кількісні, якісні або мішані (комбінація кількісних і якісних методів).Кількісні методи використовують вимірні, об’єктивні дані для визначення числових значень вартості активів, імовірності втрат і пов’язаних із ними ризиків. Якісні методи використовують відносний показник ризику (низький, середній, високий) чи вартості активу на основі рейтингу або за шкалою від 1 до 10. Якісна модель оцінює дії та ймовірності виявлених ризиків у швидкий і економічно ефективний спосіб. Набори ризиків, сформовані й проаналізовані згідно з якісною оцінкою, можуть виступати основою для цілеспрямованої кількісної оцінки.

Внаслідок проведених досліджень доцільно запропонувати таку модель реалізації загроз інформаційої безпеки. Центральний маршрутизатор пов'язаний з локальними мережами корпусів Вищого навчального закладу за допомогою проводових ліній зв'язку. Через корпусні маршрутизатори здійснюється зв'язок з комутаторами кафедр та інших підрозділів вузу. Доступ в Інтернет здійснюється через центр інформаційних технологій. Деякі комп'ютери мережі можуть мати зовнішні IP-адреси, що робить їх доступними через Інтернет, минаючи ЦІТ. Інформаційна інфраструктура вузу може бути представлена у вигляді ієрархії наступних основних рівнів:фізичного (лінії зв'язку, апаратні засоби тощо); мережевого (мережеві апаратні засоби, маршрутизатори, комутатори тощо); мережевих додатків і сервісівопераційних систем (ОС); систем управління базами даних (СУБД); технологічних процесів і додатків; бізнес-процесів Вищого навчального закладу.

Як висновок хочу додади,що в ВНЗ повинні ретельно продумуватися заходи захисту інформації до яких можна віднести:правові (закони, статути, накази, постанови); організаційні (розробка і затвердження функціональних обов'язків посадових осіб служби ІБ; фізичний контроль доступу; розробка правил управління доступом до ресурсів системи; явний і прихований контроль за роботою персоналу; технічні (передбачається наявність методик визначення загроз та каналів витоку інформації і знання засобів добування (зняття) інформації); інженерно-технічні (забезпечують унеможливлення несанкціонованого доступу сторонніх осіб на об'єкти захисту); програмно-технічні (методи ідентифікації і аутентифікації користувачів; реєстрація дій користувачів; засоби захисту від НСД, міжмережеві екрани).

Список способів протидії повинен, у разі необхідності поповняться новими засобами захисту. Це необхідно для підтримки системи безпеки закладу в актуальному стані.