

КОМПЛЕКСНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ

Метою інформаційної безпеки є забезпечення безперебійної роботи організації та зведення до мінімуму збитків від подій, які становлять загрозу безпеці, за допомогою запобігання їм та зведення наслідків до мінімуму.

Нині питання побудови системи захисту є дуже актуальними та постійно ускладнюються. Це зумовлено стрімким розвитком сучасного ринку інформаційних та комп'ютерних технологій, засобів електронного обміну інформацією, засобів захисту інформації, а також засобів несанкціонованого отримання інформації. У зв'язку з цим з'явилися та постійно вдосконалюються різноманітні технічні, програмні, організаційні та інші способи вирішення питань пов'язаних з побудовою комплексних систем санкціонованого доступу та питань, пов'язаних узагалі із захистом інформації загалом, незважаючи на її належність (державної, військової, комерційної, фінансової тощо).

Одним з найефективніших підходів до розв'язання задачі комплексної безпеки об'єктів різної форми власності є використання комплексних систем санкціонованого доступу.

Грамотна побудова та правильна експлуатація комплексних систем санкціонованого доступу на об'єкті дає змогу закрити несанкціонований доступ на його територію, в будівлю, окремі поверхи та приміщення. Водночас функціонування системи не спричиняє додаткових незручностей та перешкод для проходу персоналу та відвідувачів у дозволені їм для проходу зони.

Система контролю та керування доступом на об'єкті у наш час не усуває необхідності контролю з боку людини, але значно підвищує ефективність роботи служби безпеки. Це особливо важливо за умов наявності численних зон ризику на об'єкті з різним рівнем доступу. Комплексні системи санкціонованого доступу позбавляють охоронців від рутинної роботи із ідентифікації користувачів та надає їм додатковий час на виконання основних функцій: охорони об'єкта та захисту працівників та відвідувачів від злочинних посягань.

Оптимальне співвідношення людських та технічних ресурсів у такій системі вибирають відповідно до поставлених задач і мети та виявленого рівня можливих загроз. Зацікавленість в системах санкціонованого доступу останнім часом стрімко зростає у зв'язку з автоматизацією процесу ідентифікації та можливістю виконання системою багатьох додаткових функцій.

Розв'язання задач побудови комплексної системи санкціонованого доступу ґрунтується на двох складових: теоретичній (науковій) та практичній (отриманій на основі певного досвіду). Оптимальним є варіант, коли на основі певного теоретичного обґрунтування різноманітних варіантів розв'язання поставленої задачі будуть вироблені практичні рекомендації, які згодом будуть використані. Хоча на практиці досить часто все відбувається не завжди в такій послідовності. Є багато випадків, коли практичні рекомендації та способи вирішення часто випереджають теоретичні. Якщо технічні рішення, які використовуються в деякій

послідовності побудови комплексної системи захисту, не пов'язані єдиним системним проектом, не варто очікувати позитивного результату від реалізації окремих елементів системи. Отже, вирішуючи питання захисту інформації, неможливо обійтися без науково обгрунтованого комплексного підходу для розв'язання поставлених задач захисту, який би враховував різноманітні загрози, зокрема суспільству, установам, особистості тощо.

Науковий керівник – к.т.н., доц., Т.Л.Щербак