УДК 004.056.5
Д. Омелянюк
(Тернопільський національний технічний університет імені Івана Пулюя)

МІНІМІЗАЦІЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ПОБУДОВІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

UDC 004.056.5
D. Omelianiuk
(Ternopil Ivan Puluj National Technical University, Ukraine)

MINIMIZATION OF INFORMATION SECURITY RISKS UNDER INFORMATION SECURITY SYSTEM DEVELOPMENT

Проблема забезпечення захисту інформації є однією з найважливіших при побудові надійної інформаційної структури організації на базі автоматизованих систем. Одним із основних етапів забезпечення інформаційної безпеки є розробка політики безпеки інформації. До основних завдань політики безпеки належать:

- визначення даних, що потребують захисту;
- побудова моделі загроз та моделі порушника;
- оцінки ризиків та їх мінімізації.

Отже, на першому етапі необхідно визначити які інформаційні активи організації потребують захисту та їх цінність, яка в подальшому буде використовуватись для оцінки можливих збитків. Для побудови ефективної системи захисту інформації необхідно передбачити захист від зовнішніх порушників з високою кваліфікацією, що оснащені необхідними програмними та апаратними засобами для віддаленої реалізації загроз ІБ та метою яких є порушення конфіденційності, цілісності чи доступності інформації. З огляду на прийняте припущення щодо порушника, модель загроз можна розглядати в двох напрямках: розвідка та проникнення. Необхідно чітко розділяти поняття загроз та ризиків. Загроза – це потенційна небезпека, яка може використати вразливість інформаційної системи, що призведе до втрат інформації та збитків організації чи підприємства. Ризики інформаційної безпеки часто часто розглядають як комбінацію ймовірностей реалізації загроз інформації та оцінки потенційних втрат (в грошовому еквіваленті) при реалізації тієї чи іншої загрози. Існують різні методи оцінки ризиків та їх мінімізації. В найпростішому випадку їх можна оцінити як добуток ймовірностей загроз на величину потенційних втрат. Якщо збитки від порушення конфіденційності, цілісності чи доступності інформації власник здатний оцінити самостійно, то для оцінки ймовірностей реалізації загроз (атак) необхідно мати достатньо великий обсяг статистичних даних. Тому можна скористатись звітними даними розробників антивірусних чи інших систем захисту, доступними у відкритому доступі.

Складність побудови системи захисту організації чи підприємства полягає в розробці її архітектури з арсеналу доступних засобів. В реальному житті існує декілька обмежень при розробці таких систем, зокрема вартість системи захисту не повинна перевищувати вартість інформаційних ресурсів, що потребують захисту, та може бути обмежена виділеними коштами на її побудову. Тому задачу вибору адекватних механізмів захисту фактично можна сформулювати в термінах математичного програмування: мінімізувати цільову функцію оцінки ризиків для заданих обмежень. З іншого боку, цю ситуацію можна описати, як протистояння двох гравців (зловмисника та захисника) в термінах теорії ігор. Прийнявши припущення, що виграш зловмисника від отримання чи порушення властивостей інформації буде рівним збиткам власника інформації, побудуємо модель системи захисту інформації як гру з нульовою сумою. Платіжна (цільова) функція виражається через ризик інформаційної безпеки, який зловмисник намагається збільшити, а захисник зменшити. Фахівці з теорії ігор використовують умову рівноваги Неша для аналізу стратегічної взаємодії кількох гравців. Отже результатом розв'язання задачі буде розрахунок оптимальної стратегії дій для кожного гравця та значення цільової функції. Потрібно зазначити, що обчислене значення втрат буде середньо-статистичним при багаторазовому повторенні ігрової ситуації, що, фактично, відповідає дійсності при побудові системи захисту, адже передбачається, що зловмисник неодноразово робитиме спроби атак системи. В доповіді буде більш детально розглянуто побудову цільової функції та обмежень, а також приклад побудови системи захисту інформації з використанням апарату теорії ігор для мінімізації ризиків системи.