УДК 004.77
Чорноморець В.В. – ст. гр. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

ОСНОВНІ ВЛАСТИВОСТІ ІНФОРМАЦІЇ ТА ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІТС

Науковий керівник: асистент Маєвський О.В.

Інформаційні ресурси окремих організацій і фізичних осіб є певною цінністю, мають відповідне матеріальне вираження і вимагають захисту від різних за своєю суттю дій, які можуть привести до зниження цінності інформаційних ресурсів. Дії, які призводять до реалізації потенційних небезпек, що ведуть до зниження цінності інформаційних ресурсів, називаються несприятливими. Потенційно можлива несприятлива дія називається загрозою.

Захищеність інформації пов'язана із захистом активів від погроз, де погрози класифіковані на основі потенціалу зловживання активами, що захищаються. До уваги слід брати усі різновиди погроз, але у сфері забезпечення захищеності інформації в ІТС найбільша увага приділяється тим з них, які пов'язані з діями людини, зловмисними або іншими.

За збереження інформаційних активів відповідають їх власники, для яких ці активи мають цінність. Власники активів аналізують можливі погрози, щоб вирішити, які з них дійсно властиві середовищу їх ІТС. В результаті аналізу визначаються ризики.

Аналіз може допомогти при виборі контрзаходів для протистояння погрозам і зменшення ризиків до прийнятного рівня.

Заходи забезпечення захищеності роблять для зменшення уразливостей і захисту від можливих погроз. Але і після реалізації цих заходів можуть зберігатися залишкові уразливості. Такі уразливості можуть використовуватися порушниками, представляючи рівень залишкового ризику для активів. Власники повинні прагнути мінімізувати цей ризик, задаючи додаткові обмеження.

Діяльність, спрямована на забезпечення захищеності (безпеки) інформації, що обробляється в ІТС, називається захистом інформації. Захист інформації, що обробляється в ІТС, полягає в створенні і підтримці в працездатному стані системи як технічних, так і нетехнічних заходів, що дозволяють запобігти або утруднити можливість реалізації погроз, а також понизити потенційний збиток у разі їх реалізації. Іншими словами, захист інформації спрямований на забезпечення захищеності оброблюваної інформації і ІТС в цілому, тобто такого стану, в якому зберігаються задані властивості інформації і ІТС, які її оброблюють. Система вказаних заходів, що забезпечує захист інформації в ІТС, називається системою захисту інформації (СЗІ).

Зазвичай в процесі побудови СЗІ в ІТС виділяють наступні етапи:

1. Аналіз ІТС як об'єкту захисту і визначення інформаційних ресурсів, що захищаються. Розробка політики безпеки інформації, що обробляється в ІТС.
2. Аналіз потенційних погроз інформації в ІТС.
3. Аналіз і оцінка ризиків, пов'язаних з реалізацією погроз інформації в ІТС.
4. Вибір контрзаходів (заходів протидії) і реалізація набору заходів щодо забезпечення захисту інформації в ІТС.
5. Оцінка ефективності СЗІ в ІТС.
6. Супровід СЗІ в ІТС (підтримка СЗІ в працездатному стані протягом усього життєвого циклу ІТС).