Перелік посилань

1. Борисов М. А. Основы программно-аппаратной защиты информации. / М. А. Борисов, И. В. Заводцев, И. В. Чижов. – М.: УРСС: Либроком, 2013. – 370 с.

2. Гольдштейн Б.С. IP-телефония. / Б.С.Гольдштейн, А.В.Пинчук, А.Л.Суховицкий. - М.: Радио и связь, 2015-336 с.

3. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

4. Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинінін, С. В. Толюпа. - Київ : Логос, 2018. - 227 с.

5. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.

6. Шинкарук О.М. Основи функціонування багатоканальних систем передачі інформації: навч. посіб./ О.М. Шинкарук, Ю.М. Бойко, І.І. Чесановський. – Хмельницький : ХНУ, 2011. – 245с.

7. Кодування джерел інформації та каналів зв'язку: навчальний посібник / [Беркман Л.Н., Бондарчук А.П., Гайдур Г.І., Чумак Н.С.]. – Київ: НННТІ ДУТ, 2018. – 91 с.

Інформаційна модель захисту інформації.

Даценко В.С., Тітова В.Ю., Шевчук І.М.
Хмельницький національний університет

Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян та організацій», правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та цілі, а також інші умови і дії, що порушують безпеку [1]. При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до заподіяння шкоди.

Практика показала, що для аналізу такого значного набору джерел, об'єктів і дій доцільно використовувати методи моделювання. При цьому слід враховувати, що модель не копіює оригінал, а є простішою. При цьому, модель повинна бути досить загальною, щоб описувати реальні дії з урахуванням їх складності [2].

Можна запропонувати компоненти моделі захисту інформації на першому (інформаційному) рівні декомпозиції. На нашу думку, такими компонентами інформаційної моделі можуть бути:

- об'єкти загроз;
- загрози;
- джерела загроз;
- цілі загроз з боку зловмисників;
- джерела інформації;
- способи неправомірного оволодіння інформацією (способи доступу);
- напрямки захисту інформації;
- способи захисту інформації;
- засоби захисту інформації.

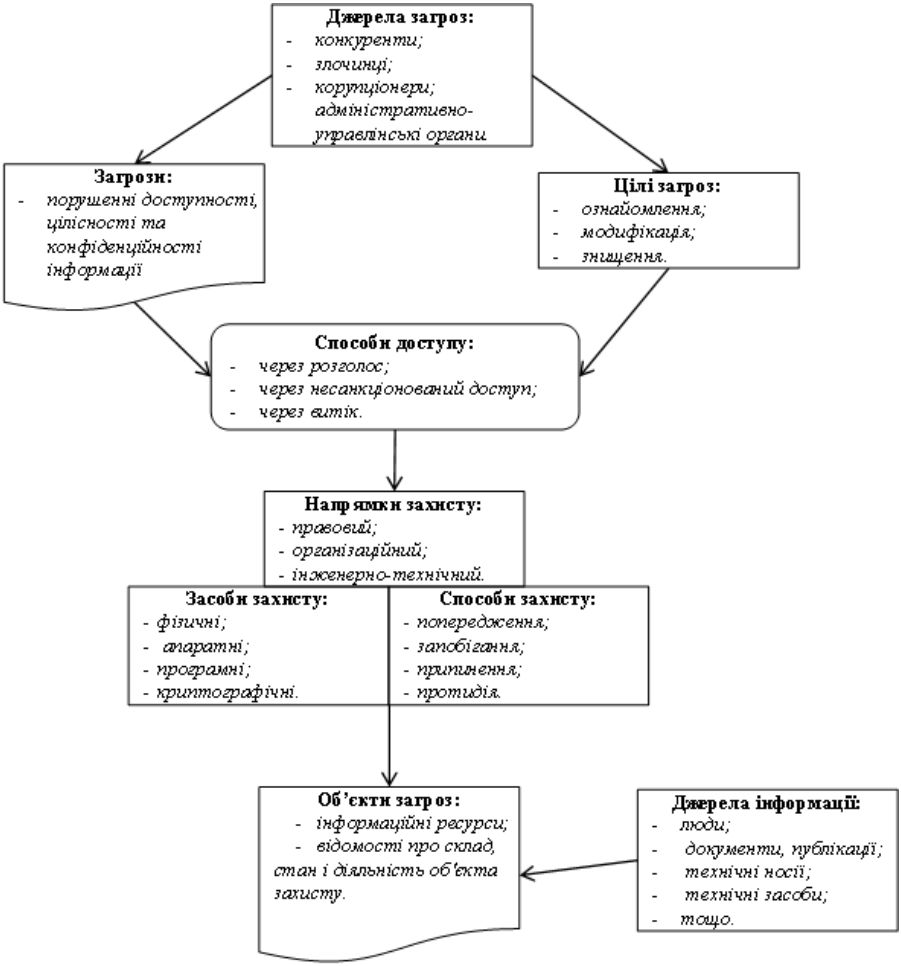

Рисунок 1 – Інформаційна модель захисту інформації

Об'єктами загроз інформаційної безпеки виступають відомості про склад, стан і діяльність об'єкта захисту (персоналу, матеріальних і фінансових цінностей, інформаційних ресурсів), тощо.

Загрози інформації виражаються в порушенні її доступності, цілісності і конфіденційності.

Джерелами загроз виступають конкуренти, злочинці, корупціонери, адміністративно-управлінські органи, тощо.

Джерела загроз переслідують при цьому наступні цілі: ознайомлення з відомостями, їх модифікація в корисливих цілях і знищення для нанесення прямих матеріальних збитків.

Неправомірне заволодіння відомостями можливо за рахунок їх розголошення джерелами інформації, за рахунок витоку через технічні засоби і за рахунок несанкціонованого доступу до відомостей. Джерелами інформації є люди, документи, публікації, технічні носії інформації, технічні засоби забезпечення виробничої та трудової діяльності, продукція і відходи виробництва.

Основними напрямками захисту інформації є правовий, організаційний та інженерно-технічний захист інформації, як показники комплексного підходу до забезпечення інформаційної безпеки.

Засобами захисту інформації є фізичні засоби, апаратні засоби, програмні засоби та криптографічні методи. Останні можуть бути реалізовані як апаратно, програмно, так і змішано-програмно-апаратними засобами. В якості засобів захисту виступають всілякі заходи, шляхи, способи і дії, що забезпечують попередження протиправних дій, їх запобігання, припинення та протидія несанкціонованому доступу.

В узагальненому вигляді розглянуті компоненти у вигляді інформаційної моделі безпеки інформації наведені на наступній схемі (рис. 1).

Співставлення об'єкта (фірма, організація) і суб'єкта (конкурент, зловмисник) в інформаційному процесі з протилежними інтересами можна розглядати з позиції активності, яка призводить до оволодіння інформацією. У цьому випадку можливі такі ситуації:

- власник (джерело) не приймає ніяких заходів до збереження інформації, що дозволяє зловмисникові легко отримати цікаві для нього відомості;
- джерело інформації суворо дотримується заходів інформаційної безпеки, тоді зловмисникові доводиться докладати значних зусиль до здійснення доступу до потрібних йому відомостей, використовуючи для цього всю сукупність способів несанкціонованого проникнення;
- проміжна ситуація - це витік інформації по технічним каналам, при якій джерело ще не знає про це (інакше він прийняв би заходи захисту), а

зловмисник легко, без особливих зусиль може їх використовувати в своїх інтересах.

Отже, на основі вищевикладеного можна зробити наступні висновки:

1. Інформація - це ресурс. Втрата інформації приносить моральні чи матеріальні збитки.

2. Умови, що сприяють неправомірному оволодінню інформацією, зводяться до її розголошенню, витоку і несанкціонованого доступу до її джерел.

3. У сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки системою захисту інформації, яка буде протидіяти загрозам через блокування неправомірних способів доступу та охоплювати усю множину існуючих способів за засобів захисту інформації

Перелік посилань

1. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту/ О. В. Черевко. // Ефективна економіка. – 2014. – №5. – Режим доступу: http://nbuv.gov.ua/UJRN/efek_2014_5_103

2. Інформаційна безпека. Навчальний посібник. Ч.1/С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

3. Основні поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 1999. – 30 с.

Метод приховування великого об'єму даних в файлах формату JPEG

Дацюк Р.М., Муляр І.В.
Хмельницький національний університет

Актуальність вивчення стеганографії постійно зростає, оскільки з поширенням персональних комп'ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу значної кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена розробці нових та вдосконаленню існуючих методів приховування даних. Кількість останніх постійно зростає з часом, але в сучасній науковій літературі [1] відсутня чітка класифікація таких методів, що ускладнює пошук і не дозволяє повною мірою оцінити рівень існуючих досягнень для їх подальшого ефективного використання.

Аналізуючи процес розвитку комп'ютерної стеганографії, можна сказати, що в найближчі роки інтерес до розробки її методів буде дедалі