Отже, залежно від цілей, для яких використовується приховування даних, різними є і вимоги щодо рівня стійкості системи до модифікації контейнера. Як наслідок, для різних цілей оптимальними є різні методи стеганографії.

Список використаних джерел:

1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – К.: Солон-Пресс, 2002. – 265 с.

2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

3. Поліновський В.В. Інформаційна технологія для досліджень методів стеганографії і стегоаналізу / В.В. Поліновський // Міжвузівський збірник «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». – Луцьк, 2011. – № 5. – С. 236–242.

4. Таранчук А.А. Стеганографічний метод приховування даних в області частотних перетворень зображень / А.А. Таранчук, Л.Г. Гальпер // Вісник Хмельницького національного університету. – Хмельницький, 2009. – № 2: «Технічні науки». – С. 197–201.

5. Хорошко В.А. Методи й засоби захисту інформації / В.А. Хорошко, А. А. Чекатков. – К.: Юніор, 2003. – 504 с.

Лупаїна Д.А.

студент,

Навчально-науковий інститут інформаційної безпеки

Національної академії Служби безпеки України

РОЗРАХУНКОВА ВАРТІСТЬ ОБРАНИХ ЗАХОДІВ ЗАХИСТУ

Для визначення систем та засобів з яких складається комплекс ТЗІ необхідно зрозуміти, які збитки буде нести підприємство у разі несанкціонованого ознайомлення, модифікації, знищення, копіювання, поширення інформації.

Одним із принципів, які притаманні процедурі побудови системи захисту інформації є принцип економічної доцільності.

Економічна доцільність зазначає, що витрати на розробку і реалізацію системи захисту інформації не повинні перевищувати розміри потенційного збитку, який може наступити в результаті порушення безпеки інформації, що захищається [1, с. 8-10].

Основні економічні принципи:

– технологія захисту інформації повинна вибиратися таким чином, щоб при мінімальних витратах, забезпечувати максимальний захист;

– надійність захисту повинна визначатися з міркувань оптимізації відношення «функціональність системи без захисту» / «функціональність системи із захистом» [3].

Захист інформації, яка не становить державну таємницю забезпечується досягненням необхідного рівня захисту інформації з обмеженим доступом за

мінімальних чи допустимих затрат і допустимого чи заданого рівня обмежень видів інформаційної діяльності [2].

Під раціональністю КСЗІ захищеної ІТС можна розуміти показник, що характеризує оптимальність фінансових витрат на проек- тування, розроблення, упровадження, обслуговування й подальшу модернізацію КСЗІ, а також виведення її з експлуатації. І цей показник, який застосовується до різних варіантів реалізації КСЗІ, що мають експертну оцінку достатності рівня захисту, доцільно розглядати у двох площинах залежно від сфер застосування захищених ІТС.

Наприклад, у державному управлінні та інших сферах, діяльність яких направлена на досягнення цілей, що не у повну міру представлені в грошовій формі, показник раціональності може бути застосовано для оцінки:

– кошторису різних варіантів побудови КСЗІ, що забезпечують достатній рівень безпеки інформації в ІТС;

– показників ефективності роботи організації при експлуатації захищеної ІТС із різними технологічними варіантами побудови КСЗІ.

Перший і другий фактор у сукупності визначають економічне обґрунтування найбільш ефективного технологічного рішення КСЗІ із погляду адміністративної діяльності та забезпечення достатнього рівня захисту.

Що стосується суб'єктів економічної діяльності, то в цьому випадку показник раціональності КСЗІ захищеної ІТС може становити передусім оцінку економічної рентабельності послуг захищеної ІТС для запланованих сфер її застосування. Це означає співвідношення фінансових результатів використання системи із затратами на її розроблення, впровадження, обслуговування, модернізацію і можливе виведення з експлуатації.

Одним із загальноприйнятих універсальних показників вимірювання фінансового результату діяльності організації є її акціонерна вартість. Відповідно, економічна оцінка послуг захищеної ІТС потребує аналізу двох основних факторів:

– приросту капіталу компанії з урахуванням упровадження або використання послуг захищеної ІТС (включаючи вартість КСЗІ), що забезпечують достатній рівень безпеки інформації в ІТС;

– впливу захищеної ІТС (рівня безпеки інформації в ІТС) на грошову оцінку ризику економічної діяльності та акціонерну вартість компанії в цілому [4].

Пріоритетним напрямом у процесі формування та забезпечення інформаційної безпеки будь-якої компанії є збереження в таємниці важливої інформації, що дозволяє успішно існувати на ринку виробництва та збуту товарів і послуг [2].

Для досягнення збереження важливої відкритої інформації та інформації з обмеженим доступом потрібно будувати системи захисту інформації для підприємства. Щоб визначитись які заходи є необхідними для створення системи захисту інформації необхідно користуватися чинним законодавством України [1].

Вочевидь, процес оцінювання ефективності КСЗІ передбачає моделювання системи захисту, вибір і використання показни- ків, критеріїв і методик оцінювання ефективності КСЗІ.

Одним з етапів створення комплексу ТЗІ є його обґрунтування, а саме техніко-економічне обґрунтування.

Техніко-економічне обґрунтування комплексу ТЗІ – визначення оптимального обсягу технічних заходів у складі системи захисту інформації, необхідного для досягнення мети захисту. Для проведення досліджень слід виходити з того, що вартість витрат на створення системи захисту інформації на об'єкті не повинна перевищувати вартість інформації, що підлягає захисту. В іншому випадку захист інформації стає недоцільним [3].

Одним із принципів, які притаманні процедурі побудови системи захисту інформації є принцип економічної доцільності.

Економічна доцільність зазначає, що витрати на розробку і реалізацію системи захисту інформації не повинні перевищувати розміри потенційного збитку, який може наступити в результаті порушення безпеки інформації, що захищається.

Економічна складова комплексного підходу до захисту інформації безпосередньо впливає на масштаби впровадження систем кібернетичного захисту людини, суспільства, держави та рівень цього захисту відповідно. Наукові дослідження з питань оцінювання економічної ефективності комплексних систем захисту інформації базуються на економічній теорії, теорії управління, доробках учених із питань оцінювання ціннісних характеристик інформації, оцінювання та оброблення ризиків інформаційної безпеки тощо.

Список використаних джерел:

1. Ткачук Т. Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту [Електронний ресурс]: наукова стаття / Т. Ткачук. Режим доступу: http://www.pravoznavec. com.ua/

2. Миколенко В. В. Методика побудови моделей загроз автоматизованих систем [Електронний ресурс] / В. В. Миколенко. – Режим доступу: http://nc. nusta.com.ua

3. Маслова Н. А. Построение модели защиты информации с заданными характеристиками качества / Н. А. Маслова // Штучний інтелект. – Донецьк: ІШІ, 2007. − № 1. − С. 51–57.

4. Голиков Ю. А. Экономическая эффективность системы защиты информации: учеб.-метод. пособ. / Ю. А. Голиков, Л. Ю. Сульгина. – Новосибирск: СГГА, 2012. − 41 с.