та непрямі збитки від них становлять мільярди гривень щорічно. Значні прогалини в регулюванні економічних відносин, неефективність контролю за сферою державних закупівель, лобіювання інтересів конкретних виробників, низька ефективність ужитих державою антикорупційних заходів і відсутність комплексної нормативно-правової бази протидії економічній злочинності призводять до неефективності спорадичних антикриміногенних заходів у вказаній сфері. Окрім того, негативні тенденції економічної злочинності в України значно посилюються завдяки впливу низки економічних, соціальних і політичних детермінант, безпосередньо пов'язаних із наявністю збройного конфлікту на сході України. Убачається, що встановлені тенденції економічної злочинності мають бути враховані під час розробки комплексної стратегії протидії цьому виду злочинності як важливого інструменту забезпечення економічної безпеки держави та поліпшення добробуту її громадян.

Використані джерела:

1. Конституція України/ Відомості Верховної Ради України// , 1996, № 30, ст. 141- [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua /laws.
2. Кримінальний кодекс України // Відомості Верховної Ради України, 2001,- № 25-26, ст.131 [Електронний ресурс]. – [Електронний ресурс]. − Режим доступу: http://zakon.rada.gov.ua/laws.
3. Глущенко В. В. Економічна злочинність , прийоми приховування і методи ії виявлення. / В.В. Глущенко // Вісті Кримінологічної асоціації України .-2004.-Вип 1.- Х: В-цтво Харк. нац. ун-ту внутр. Справ.- с.173- 175

Гавриш Б.О. - курсант 1 курсу факультету підготовки фахівців для органів досудового розслідування;
Мирошниченко В.О. – науковий керівник, професор кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент

КРИПТОГРАФІЯ ТА СТЕГАНОГРАФІЯ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

На сьогоднішній день в нашому суспільстві постала велика проблема із захистом інформації, мережева безпека стала важливою частиною сучасної системи зв'язку.

Захист інформації (Data protection) — сукупність методів і засобів, що забезпечують конфіденційність, цілісність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

На сьогоднішній день існують декілька видів захисту інформації, при

чому кожен вид захисту інформації забезпечує окремі аспекти інформаційної безпеки:

• технічний — забезпечує обмеження доступу до носія повідомлення апаратно-технічними або програмними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарт-карти тощо), що забезпечує попередження витоку по технічним каналам та попередження блокування;

• інженерний — попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізацію);

• криптографічний — попереджує доступ за допомогою математичних перетворень, який забезпечує несанкціоновану модифікацію та розголошення інформації;

• організаційний — попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

На сьогоднішній день в інформаційній безпеці широке застосування отримали такі інструменти захисту інформації як криптографія та стеганографія. Стеганографія приховує сліди спілкування, тоді як криптографія використовує шифрування, щоб зробити повідомлення незрозумілим. Стеганографія не передбачає змін у структурі повідомлення. З іншого боку, криптографія змінює стандартну структуру секретного повідомлення при передачі по мережі.

Отже, стеганографія - це техніка приховування спілкування, приховуючи таємне повідомлення у фальшиве повідомлення. Термін стеганографія має грецький вплив, що означає «таємне письмо». Основна ідея стеганографії - запобігти підозрі щодо існування інформації. Раніше це було невидиме чорнило, відбитки олівців на рукописних символах, невеликі проколи шпильками - це методи, які використовувалися для приховування повідомлення. Найпростіша техніка приховування повідомлення - це створення повідомлення, в якому секретне повідомлення містить лише кілька значущих символів. Техніка стеганографії включає в себе носій обкладинки, секретне повідомлення, ключ шифрування та носій шифрування. Текст, аудіо, зображення та відео поводяться як носії обкладинки, які містять приховану інформацію, закладену в ньому. Носій шифрування генерується за допомогою носія обкладинки та вбудованого повідомлення. Ключ шифрування також використовується як додаткова таємна інформація, як пароль, що використовується одержувачем для отримання повідомлення. Як було сказано вище, текст, аудіо, зображення та відео використовуються в якості носіїв прикриття, тому стеганографія надходить у різних формах. Використовуючи текст, щоб приховати повідомлення, слово чи рядок можна змістити, можна використовувати пробіли, навіть кількість та положення голосних використовуються для приховування таємного повідомлення.

Перспективними на сьогодні є аудіо та відео стеганографія. Аудіо стеганографія дозволяє приховати таємне повідомлення в аудіофайлі за допомо-

гою його цифрового зображення. Це може бути досягнуто легко, оскільки типовий 16-бітний файл має 216 рівнів звуку, а різницю кількох рівнів неможливо виявити людським вухом. Зображення є найбільш вживаною формою стеганографії, причина цього в тому, що вона викликає найменшу підозру. Відеостеганографія дає більше можливостей маскування великого обсягу даних, оскільки це поєднання зображення та звуку. Тому методи відео- та ауді-остеганографії також можуть бути використані на відео.

Основним недоліком використання стеганографії є значна кількість накладних витрат, які вона створює для приховування невеликої кількості інформації. Крім того, не слід виявляти систему захисту, інакше вона марна.

Криптографія забезпечує кілька схем кодування для досягнення безпеки під час спілкування в загальнодоступній мережі. Слово криптографія походить від грецького слова, яке означає "таємне написання". Криптографію можна зрозуміти на прикладі, коли відправник посилає повідомлення, яке спочатку існує в простому тексті. Перед передачею повідомлення по мережі воно шифрується та перетворюється в шифротекст. Коли це повідомлення надійде до одержувача, воно знову розшифровується назад у простий текст.

На сьогоднішній день існує два типи криптографії: симетричний та асиметричний [1]. Симетрична криптографія використовує ключ для шифрування та розшифрування відповідно простого тексту та тексту шифру. Єдиною умовою тут є те, що він має один і той же ключ для шифрування та дешифрування, а також вимагає менше часу на виконання. Криптографія асиметричного ключа використовує два ключі, названі як приватний ключ і відкритий ключ. Відкритий ключ надається одержувачем відправника для шифрування повідомлення, тоді як приватний ключ застосовується самим одержувачем для розшифрування повідомлення. Ключі можна повторно використовувати з іншими об'єктами.

Таким чином, стеганографія - це наука, яка займається тим, як комунікацію можна замаскувати, тоді як криптографія - це наука про перетворення змісту комунікації на неясність. Це також передбачає різницю між порушенням системи захисту: стеганографія зазнає поразки, якщо виявлено наявність стеганографії, тоді як у криптографії зловмисник не повинен вміти прочитати секретне повідомлення, інакше система буде порушена. Захищеність стеганографії залежить від секретності системи кодування даних. Технічні характеристики сучасних обчислювальних систем є дуже потужними, що дозволяє при використанні таких інструментів захисту інформації як криптографія та стеганографія застосовувати складні математичні алгоритми.

Використані джерела:

1. Мухачев В.А., Хорошко В.А. Методы практической криптографии. – К.: ООО «Полиграф Консалтинг», 2005. – 215 с.