В. О. Шутенко
студент магістратури економіко-правового факультету Одеського національного університету імені І.І. Мечникова, спеціальність «Економіка»
Науковий керівник: ст. викладач кафедри економічної кібернетики та інформаційних технологій Одеського національного університету імені І.І. Мечникова О. С. Максимов

ЗАСТОСУВАННЯ КОНЦЕПЦІЇ GRC (GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE) В УПРАВЛІННІ ЗАХИСТОМ ЕКОНОМІЧНОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Інтенсивний розвиток засобів обчислювальної техніки відкрив великі можливості по автоматизації розумової праці і привів до виникнення принципово нових інформаційних технологій. Окрім істотних позитивних сторін, впровадження сучасних інформаційних технологій має також і негативний характер.

З кожним роком все більш поширюється знищення або розголошування певної частини конфеденційної інформації підприємств, також поширюються методи дезорганізації процесів її обробки і передачі в системах, які беруть участь в процесах автоматизованої інформаційної взаємодії.

Основними групами чинників, які сприяють поширенню комп'ютерних злочинів є: економічні, технічні і правові чинникі. До першої групи слід віднести впровадження ринкових стосунків, зміну форм власності, відмова від державного регулювання в економіці, розвиток нової сфери підприємницької діяльності – інформаційного бізнесу та ін.

До другої групи відносять зростання використовуваних персональних комп'ютерів, розвиток комп'ютерних систем і комунікацій, доступність широкого спектру програмних продуктів і тому подібне.

Самостійну групу утворюють правові питання. Це пояснюється головним чином не опрацьованістю багатьох юридичних аспектів про можливість функціонування інформації в якості специфічного

товару і ресурсу, авторського права на програмні продукти, а також отримане велике поширення «комп'ютерне піратство» [1].

Актуальність теми доповіді обумовлена тим, що в сучасному бізнесу необхідна ефективна система захисту економічної інформації.

Стеганографія – це наука, що вивчає методи організації передачі інформації, які приховують сам факт передачі повідомлень [1].

Стегосистема – це сукупність способів і методів, які використовуються для формування прихованого каналу передачі інформації. Може бути з відкритим і закритим ключем [1].

Слід відмітити, що у стегосистемі з секретним ключем використовується один ключ, який повинен бути визначений до початку обміну секретними повідомленнями або переданий по захищеному каналу. А у стегосистемі з відкритим ключем використовуються різні ключі, які відрізняються тим, що за допомогою обчислень неможливо вивести один ключ з іншого [2].

На сучасному етапі розвитку інформаційних технологій, а саме технологій захисту даних, останій час частіше стали використовувати контейнерну технологію. Контейнер – це об'єкт, в якому приховують секретну інформацію [1]. Існує декілька видів «контейнерів», найбільш відомими є [2]: порожній контейнер – контейнер без вбудованих повідомленнь; заповнений контейнер (стегоконтейнер) – контейнер, який містить вбудовану інформацію.

Системи GRC (Governance, Risk and Compliance) з кожним роком все більш застосовуються. Проте, описи невичерпних можливостей конфігурації і унікальності кожного впровадження цієї технології часто залишають суперечливе враження [4]. Системи класу GRC дають можливість компаніям реалізувати комплексний підхід до концепції GRC, дозволяючи вирішувати наступні завдання: чітко структурувати, автоматизувати і підвищувати ефективність бізнес-процесів; забезпечувати централізоване зберігання і доступ до інформації; формувати детальну і агреговану звітність; управляти правами доступу користувачів; автоматизувати розрахункові моделі; знижувати витрати на підтримку бізнес-процесів [3]. GRC–

системи, націлені на автоматизацію і підвищення ефективності відразу декількох бізнес-процесів або напрямів діяльності компанії, прийнято називати інтегрованими [3]. Впровадження інтегрованих GRC-систем – досить трудомісткий і тривалий процес, проте, більш ніж в 70% випадків результати, отримані від впровадження GRC-систем, повністю відповідають очікуванням бізнес-замовника, а в деяких випадках навіть перевищують їх [3].

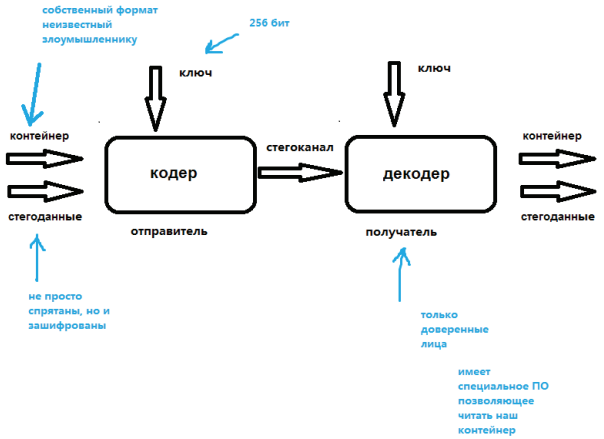

Рис.1. Модель розробленої стегосистеми

Джерело: розроблено автором

У своїй роботі ми створювали свій власний контейнер (і формат для нього, а саме – .mash) і спеціальне програмне забезпечення для відкриття цього формату, яке буде в доступі у довірених осіб. Довірених осіб ми додаватимо в систему за допомогою їх електронних сертифікатів і відкритих ключів.

Таким чином, працюючи в максимально агресивному середовищі, коли зловмисник знає якими методами ми шифруємо і де саме передаємо інформацію, ми зможемо по максимуму захистити передану інформацію за допомогою особистого контейнера і вже давно відомих методів шифрування даних.

Література:

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М: Солон-Пресс, 2011. – 272 с.
2. Ленков С. В. Методы и средства защиты информации / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К: Арий, 2008.
3. Фетисова Ю. К. Концепция «Governance, Risk, Compliance» (GRS): сущность, задачи, реализация // Молодой ученый. – 2018. – № 22. – С. 448-450.
4. Щеглов А. Ю. Захист комп'ютерної інформації від несанкціонованого доступу / А. Ю. Щеглов. – СПБ: Наука і техніка, 2014. – 384 с.