# ПРОГРАМНО-ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ОХОРОННОЇ СИСТЕМИ

*Бойко Каріна, Орест Полотай*
Національний університет «Львівська політехніка»

**Описано основні засоби і методи захисту інформації від несанкціонованого і таємного добування. Показано як можна захистити приміщення від зловмисників за допомогою охоронної системи. Описано криптографічний метод захисту інформації.**
**Ключові слова: захист інформації, охоронна система, крипто-захист.**

**The basic means and methods of protecting information from unauthorized and secret extraction is described. Shown how you can protect premises using the security system from intruders. The cryptographic method of information security is described.**
**Keywords: protection of information, security system, crypto-protection.**

Захист інформації в сучасних умовах стає все більш складною проблемою, що обумовлено рядом обставин, основні з яких: масове розповсюдження засобів електронної обчислювальної техніки; ускладнення шифрувальних технологій; необхідність захисту не тільки державної і військової таємниці, але і промислової, комерційної і фінансової таємниць; збільшення можливостей несанкціонованих дій над інформацією.

Крім того, в даний час набули широкого поширення засоби і методи несанкціонованого і таємного добування інформації. Вони все більше застосовуються не тільки в діяльності державних правоохоронних органів, але і в діяльності різного роду злочинних угруповань.

Недобросовісна конкуренція, активізація дій терористів примушують суспільство звертати увагу на проблеми забезпечення безпеки, одним з найважливіших аспектів якої є інформаційна безпека.

Основні надії фахівці пов'язують з впровадженням інтегральних підходів і технологій. Необхідною умовою реалізації інтегрального підходу є блокування всіх технічних каналів витоку і несанкціонованого доступу до інформації, тому для створення ефективних систем безпеки, в першу чергу, необхідно досліджувати можливі канали витоку і їх характеристики.

Необхідно пам'ятати, що природні канали витоку інформації утворюються спонтанно, через специфічні обставини, що склалися на об'єкті захисту.

Що стосується штучних каналів просочування інформації, то вони створюються навмисно із застосуванням активних методів і способів отримання інформації. Активні способи припускають навмисне створення технічного каналу витоку інформації з використанням спеціальних технічних засобів. До них можна віднести незаконне підключення до каналів, проводів і ліній зв'язку, високочастотне наведення і опромінення, установка в технічних засобах і приміщеннях мікрофонів і телефонних закладних пристроїв, а також несанкціонований доступ до інформації, що обробляється в автоматизованих системах (АС) і т.д.

Тому особливу роль і місце в діяльності із захисту інформації займають заходи зі створення комплексного захисту, що враховують загрози національної і міжнародної безпеки і стабільності, зокрема суспільству, особі, державі, демократичним цінностям і суспільним інститутам, суверенітету, економіці, фінансовим установам, розвитку держави.

Здавалося б, на перший погляд, нічого нового в цьому немає. Потрібні лише відомі зусилля відповідних органів, сил і засобів, а також їх відповідне забезпечення всім необхідним.

Разом з тим, проблемних питань із захисту інформації багато, їх вирішення залежить від об'єктивних і суб'єктивних чинників, у тому числі і дефіциту можливостей.

Таким чином, проблема захисту інформації і забезпечення конфіденційності набуває актуальності.

Захистити приміщення від зловмисників можна шляхом встановлення охоронної системи.

Охоронна система – автоматизований комплекс для охорони різних об'єктів майна (будівель, включаючи прилеглу до них територію, окремих приміщень, автомобілів, водного транспорту, сейфів та ін.) Термін є узагальнюючим для декількох типів систем. Основне призначення – попередити, по можливості запобігти або сприяти запобіганню ситуацій, в яких буде завдано шкоду людям або матеріальним і не матеріальним цінностям, пов'язаних насамперед з діями інших осіб.

Дієвим способом програмно-технічного захисту інформації, є крипто-захист, тобто системи, що дозволяють шифрувати та дешифрувати інформаційні потоки. Традиційна криптографія виходила з того, що для шифрування та дешифрування використовується один і той же секретний ключ, який мав мати відправник повідомлення і отримувач. Одним з поширених, сьогодні, методів шифрування є алгоритм RSA, в основі якого кожен учасник процесу має власний таємний ключ та відкритий ключ, що не є секретним з допомогою якого проводиться обмін повідомленнями. Електронний цифровий підпис (ЕЦП) – це аналог власного підпису посадової особи в електронному вигляді.

Криптографічні методи захисту інформації широко використовуються в автоматизованих банківських системах і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту. Використовуючи шифрування повідомлень в поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна добитися високого рівня захисту інформаційного обміну.

Отже, надійно захистити приміщення ми зможемо за допомогою охоронної системи. Крім того, захист інформації в сучасних умовах стає великою проблемою, яку важко вирішити. Ми вияснили, що криптографія є одним з найкращих засобів забезпечення конфіденційності і контролю цілісності інформації, також займає центральне місце серед програмно-технічних регулювальників безпеки.

**Список використаної літератури**

1. Засоби і методи захисту інформації [Електронний ресурс]. – Режим доступу: http://kiev-security.org.ua/

2. Охоронна система [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Охоронна_система

3. Крипто-захист [Електронний ресурс]. – Режим доступу: https://buklib.net/books/28625/