Під впливом акустичних коливань в приміщення, в якому міститься джерело мовного сигналу, виникають вібраційні коливання.

Проблема захисту конфіденційної мовної інформації вирішується у комплексі з використанням різних заходів, в тому числі й з використанням технічних засобів. Для захисту акустичної (мовної) інформації використовуються пасивні і активні методи, а також заходи з використанням певних засобів.

Деякі елементи допоміжних технічних засобів системи, у тому числі трансформатори, котушки індуктивності, електромагніти вторинного електрогодинника, дзвінків телефонних апаратів і т.п., мають властивість змінювати свої параметри (місткість, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу. Зміна параметрів призводить або до появи на цих елементах електрорушійної сили, або до модуляції струмів, що протікають по цих елементах відповідно до змін відповідного акустичного поля. Окрім вказаних елементів, можуть містити безпосередньо акустоелектричні перетворювачі. До таких належать: деякі типи датчиків охоронної і пожежної сигналізації, гучномовці ретрансляційної мережі, тобто, всі пристрої, які мають «мікрофонний ефект».

Нейтралізувати витік інформації можна двома поширеними способами: перший спосіб пасивний, полягає в установці спеціальних фільтрів на всі розетки в приміщенні. Дані фільтри будуть перешкоджати поширенню сигналів понад 50 Гц., тим самим блокувати роботу пристроїв, які працюють на високих частотах і перехопленню інформативних сигналів. Інший спосіб активний, полягає в постановці шумових перешкод на кожну фазу мережі в діапазоні частот, що використовуються апаратурою перехоплення. Прилади, що дозволяють реалізувати дану перешкоду, називаються мережними генераторами шуму, вони встановлюються на кожну фазу мережі, заведену в приміщення (включно освітлювальну).

Реалізація організаційних методів – це також важлива задача і в конкретних умовах досягається за допомогою різноманітних технічних засобів. Найбільший ефект досягається, коли сили й засоби, що забезпечують досягнення цілей і рішення завдань захисту акустичної інформації, утворюють комплексну систему. Крім того, ефективність обраних заходів щодо захисту інформації в значній мірі залежить від уміння і практичних навичок відповідних фахівців, й тому велика увага повинна приділятися практичним заняттям, на яких будуть розглядатися основні питання захисту акустичної інформації.

Одержано 17.04.2018

УДК 004.056.53

Ксенія Олександрівна КРАТАСЮК,
курсант групи Ф4-202 ХНУВС
Науковий керівник: викладач кафедри кібербезпеки
факультету № 4 ХНУВС кандидат технічних наук Світличний В. А.

ОСОБЛИВОСТІ КРИПТОВАЛЮТИ

Звичні для нас гроші випускаються в обіг центральними банками різних країн. На їх вартість впливають рішення урядів, економіка країн, міжнародна торгівля. Криптографічна валюта – це принципово новий інструмент взаєморозрахунків. Для генерації монет, або майнінгу, необхідно виробляти певний математичний алгоритм обчислень. Кожна криптоодиниця являє собою послідовність блоків, а кожен з блоків – складну математичну формулу. Для створення нової монети необхідно згенерувати нову ланцюжок блоків транзакцій. Таким чином криптовалюта – це цифрова (віртуальна) валюта, одиниця якої – монета, яка захищена від підробки, тобто криптовалюта по суті – це зашифрована інформація, скопіювати яку неможливо. Криптовалюта емітується безпосередньо в мережі і ніяк не пов'язана з будь-якою валютою або з державною валютною системою.

Це суттєва відмінність від звичайних грошей, які перш, ніж з'явитися на рахунку в електронному вигляді, повинні бути спочатку внесені на рахунок у грошовому еквіваленті. Наприклад, через банк або платіжний термінал. Тобто для звичайної валюти електронний вигляд – лише одна з форм представлення.

На даний момент у світі кількість видів криптовалют вже наближається до тисячі і ринок продовжує рости. Біткоін – це перша і найвідоміша з безлічі інших віртуальних електронних валют. Термін «біткоін» запозичений з англійської мови (bitcoin) і утворився шляхом злиття двох слів: bit (мінімальна одиниця комп'ютерної пам'яті) і coin (монета). Біткоін кваліфікують як віртуальну валюту, грошовий сурогат, електронну послугу, електронну інформацію, нематеріальну цінність, приватні гроші, віртуальний товар тощо.

Біткоін функціонує без будь-якого контролюючого органу або центрального банку; обробка транзакцій і емісія здійснюються колективно учасниками мережі, дозволяє проводити будь-які операції анонімно, без ідентифікації користувача. Біткоін має відкритий вихідний код; ніхто не володіє і не контролює біткоіни, але всі можуть стати учасниками мережі. Мережа біткоін заснована на так званому «блокчейні» (ланцюжку блоків) і являє собою публічний реєстр, який зберігає дані про всі транзакції системи. Усі транзакції захищені електронними підписами користувачів – учасників мережі, які видобувають біткоін і/або проводять з ними будь-які операції.

Для розуміння функціонування криптовалют, перш за все потрібно ознайомитись з поняттям «Блокчейн» (Blockchain), Blockchain – це публічна база всіх транзакцій, які коли-небудь робились в межах певної системи. Це, так званий, ланцюжок блоків транзакцій, що побудований за певними правилами із сформованих блоків транзакцій. Вперше термін з'явився як назва розподіленої бази даних, реалізованої в саме у криптовалюті біткойн. По суті, блокчейн – це децентралізований реєстр інформації, копія якого є у всіх учасників системи, і кожна його зміна залишається в базі назавжди. Змінити щось заднім числом неможливо – для цього доведеться одночасно поміняти всі наступні записи у всіх учасників системи. Для такої операції не вистачить тих обчислювальних потужностей, які сьогодні є у людства. Учасники підключені до мережі та для переказу коштів використовують адреси, а не прізвища. Достовірність адреси перевіряється за допомогою публічних ключів шифрування. При цьому особи платника і одержувача залишаються в секреті.

Система ставить з ніг на голову традиційну банківську таємницю: всі операції проводяться відкрито, але пов'язати конкретну адресу з конкретною людиною не являється можливим.

Одержано 17.04.2018

УДК 004.056.53:351.74

Павло Ігорович ДРАГУНОВ,
курсант групи Ф4-102 ХНУВС
Науковий керівник: завідувач кафедри кібербезпеки
факультету № 4 ХНУВС кандидат технічних наук, доцент Гнусов Ю. В.

ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ З ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

З метою протидії злочинності, ефективного попередження, припинення та розкриття злочинів органи та підрозділи Національної поліції України здійснюють необхідні: слідчі (розшукові) дії; негласні слідчі (розшукові) дії; оперативно-розшукові дії. Під час підготовки та проведення зазначених дій працівники поліції використовують інформацію з обмеженим доступом в акустичному та електронному вигляді.

Така інформація може циркулювати в акустичному вигляді під час проведення нарад щодо планування певних негласних заходів. В електронному вигляді інформація циркулює, наприклад, під час підготовки необхідних документів, таких як плани, звіти, клопотання до суду.

Дана інформація може бути цікавою для представників організованих злочинних груп, та, навіть, представників іноземних розвідок. Вони можуть отримати доступ до цієї інформації шляхом фізичного доступу на об'єкт де циркулює ця інформація (в службовому кабінеті працівника поліції).

Також за допомогою сучасних приладів зловмисники можуть аналізувати бездротові мережі (Wi-Fi) та вилучати незаконним методом данні жертви. Сучасні засоби технічної розвідки дозволяються підключатися дистанційно до обчислювальних машин, створювати перешкоди у телекомунікаційних каналах між пристроями і супутниковою системою, бездротових мережах.

В разі отримання несанкціонованого доступу сторонніх осіб до інформації з обмеженим доступом, це може призвести до більш ефективної протидії злочинців щодо документування їх діяльності з боку працівників правоохоронних органів або неможливості затримання злочинців.

З метою не допущення витоку інформації з об'єктів інформаційної діяльності поліції необхідно вживати заходів з технічного захисту інформації, таких як періодичний пошук засобів негласного зйому інформації («закладних пристроїв») та використання технічних засобів захисту акустичної інформації та електронно-обчислювальних машин.

На сьогоднішній день на ринку представлено багато різних за призначенням та технічними можливостями технічних засобів пошуку та захисту інформації, як українського так і закордонного виробництва. При цьому періодично на ринку з'являються нові розробки та нові технічні засоби.

Під час вибору технічних засобів, що будуть використовуватися для забезпечення захисту інформації, слід звернути увагу на такі технічні засоби як:

1. Тепловізори – використовуються для виявлення пристроїв, що виділяють температурне поле. Зазвичай ці прилади приховуються зловмисником у стінах.

2. Багатофункціональні пошуковий прилади – зазвичай вони поєднують в собі широкосмуговий детектор електромагнітного поля, приймач інфрачервоного діапазону, різні додаткові зонди для перевірки провідних ліній і оцінки віброакустичного захисту приміщення.

3. Частотоміри – дозволяють виміряти частоту сигналу безконтактно, за допомогою антени. Така властивість дозволяє застосовувати їх як для замірів «відомих» сигналів, так і для пошуку «прихованих» сигналів від підслуховуючих пристроїв (жучків).

Таким чином, можна зробити висновок, що для забезпечення захисту інформації з обмеженим доступом від витоку з об'єктів інформаційної діяльності Національної поліції можуть використовуватися різноманітні технічні засоби, як пошукові та засоби захисту інформації.

Одержано 17.04.2018

УДК 004.159.9

Ярослав Віталійович ОСІПОВ,
курсант групи Ф4-202 ХНУВС
Науковий керівник: викладач кафедри кібербезпеки
факультету № 4 ХНУВС кандидат технічних наук Світличний В. А.

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК СПОСІБ ШАХРАЙСТВА

Соціальна інженерія – метод отримання необхідного доступу до інформації, заснований на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних і інших захищених систем.

Є декілька головних векторів нападу, які використовуються при проведенні атак за допомогою соціальної інженерії:

– Он-лайн;