УДК 004.681.3

Л.П. Крючкова, О.П. Провозін

ПЕРЕХОПЛЕННЯ МОВЛЕННЄВОЇ ІНФОРМАЦІЇ МЕТОДАМИ ВИСОКОЧАСТОТНОГО "НАВ'ЯЗУВАННЯ"

Розглядаються процеси формування технічних каналів витоку мовленнєвої інформації методами високочастотного "нав'язування", фізична сутність процесу модуляції зондуючого високочастотного сигналу небезпечними сигналами та умови формування в колах основних та допоміжних технічних засобів і систем модульованих коливань. Сформульовано базові рекомендації, спрямовані на виключення можливостей перехоплення інформації каналами високочастотного "нав'язування".

Ключові слова: перехоплення інформації, високочастотне "нав'язування", зондуючі сигнали, модуляція.

Вступ

В умовах глобальної інформатизації суспільства реальна безпека держави багато в чому залежить від безпеки її інформаційних ресурсів і технологій. У загальній проблемі забезпечення безпеки інформації питання захисту конфіденційної інформації є одним із найважливіших. Це пояснюється, зокрема, тим, що частка конфіденційної інформації в загальному інформаційному потоці являє собою значну частину.

Захист національної конфіденційної інформації став одним із головних пріоритетів державної політики, у тому числі й у нашій країні. Віднесення інформації до категорії з обмеженим доступом та її засекречування є важливою складовою теорії і практики захисту інформації.

В даний час відомо багато способів перехоплення мовленнєвої акустичної інформації, обговорюваної в приміщенні. Усі їх можна розбити на декілька великих груп:

- ✓ впровадження на об'єкт технічних засобів перехоплення;
- ✓ пряме перехоплення акустичних сигналів за допомогою мікрофонів спрямованої дії;
- ✓ використання віброакустичного каналу перехоплення;
- ✓ використання акустоелектричного каналу;
- ✓ перехоплення побічних електромагнітних випромінювань і наведень;
- ✓ високочастотне "нав'язування".

Під високочастотним "нав'язуванням" розуміється спосіб несанкціонованого отримання інформації, при якому відбувається зондування радіосигналом приміщення і його струмопровідних комунікацій, в якому відбуваються переговори. В результаті взаємодії з технічними засобами або спеціально впровадженими пристроями відбувається модуляція зондуючих сигналів мовленнєвими. В колах технічних засобів, що знаходяться в зоні впливу високочастотних випромінювань, наводяться сигнали напруги до декількох вольт. Якщо в зазначених колах є елементи, параметри яких (індуктивність, ємність або опір) змінюються під дією низькочастотних сигналів, то в навколишньому просторі буде створюватися вторинне поле високочастотного випромінювання, модульоване низькочастотним сигналом.

Більшості фахівців у сфері захисту інформації відомо, що спосіб перехоплення акустичної інформації, який отримав назву "ВЧ-нав'язування", вперше був реалізований як "подарунок" радянських піонерів послу США в СРСР А. Гарріману в 1945 році. "Безцінний дар" був виконаний у вигляді гіпсового герба США, прийнятий з вдячністю розчуленим послом і розміщений на стіні його кабінету, де успішно провисів до 1952 р., поставляючи оперативну та стратегічну інформацію радянському керівництву [1].

З тих пір минуло багато років і спосіб, винайдений видатним ученим Л.С. Терменом, отримав подальший розвиток. Було розроблено методи його застосування в струмопровідному середовищі з використанням в якості пасивної закладки окремих електрорадіоелементів електронної техніки. В даний час такі методи перехоплення акустичної інформації є одними з найперспективніших беззаходових способів її здобування і мають тенденцію до подальшого розвитку.

Високочастотне "нав'язування" (зондування) є дуже ефективним способом перехоплення інформації, що циркулює в апаратурі основних технічних засобів і систем

(ОТЗС) або наводиться у допоміжних технічних засобах і системах (ДТЗС) за рахунок акустоелектричних перетворень, що утворюються при одночасному впливі на елементи технічних засобів конфіденційних мовленнєвих сигналів та зондуючого сигналу, якщо в останніх при їх розробці не було вжито радикальних заходів, що перешкоджають проникненню струмів високої частоти всередину цієї апаратури.

Метою публікації є розгляд фізичної сутності процесу модуляції зондуючого високочастотного сигналу небезпечними сигналами та умов формування модульованих коливань в колах основних та допоміжних технічних засобів і систем.

Опис каналу високочастотного "нав'язування"

Високочастотне "нав'язування" є активним способом перехоплення інформації, який може бути здійснений шляхом подання струмів високої частоти від відповідного генератора системи перехоплення інформації в нелінійні та (чи) параметричні кола ОТЗС та ДТЗС, в яких є присутнім з тих або інших причин небезпечний сигнал, і одночасного прийому (виявлення) промодульованих небезпечним сигналом струмів високої частоти за допомогою узгодженого за технічними характеристиками з генератором і іншими компонентами взаємодіючих систем оптимального приймаючого пристрою.

В основі методу високочастотного "нав'язування" лежить використання фізичного явища відбиття енергії високої частоти від неузгодженого навантаження.

Під навантаженням розуміється повний опір якого-небудь нелінійного або параметричного кола, величина якого змінюється під впливом небезпечного сигналу згідно із законом, властивим цьому сигналу. Таким чином, навантаження може розглядатися як модулятор високочастотного коливання небезпечним сигналом.

Подання на ОТЗС (у тому числі при одночасній дії акустичного поля мовленнєвих конфіденційних сигналів на ДТЗС) і знімання з них високочастотних коливань при застосуванні даного методу здійснюється за допомогою різноманітних ліній зв'язку, що відходять до ОТЗС і ДТЗС. Лініями зв'язку можуть виступати лінії передачі (у симетричному і несиметричному режимах), кола електроживлення, заземлення, управління, сигналізації – так звані струмопровідні комунікації – і т.п., а також лінії, утворені паразитними зв'язками між різними колами ОТЗС, ДТЗС, конструктивними елементами будівель, споруд, устаткування.

Ефективність методу високочастотного "нав'язування" в загальному вигляді визначається як результат взаємодії наступних технічних систем:

- ✓ системи перехоплення інформації;
- ✓ системи передачі, обробки і зберігання інформації;
- ✓ системи (лінії) зв'язку.

Апріорні результати взаємодії цих систем можуть бути оцінені проведенням системного аналізу функціонування складної технічної системи, що складається з трьох вказаних складових частин.

Структурну схему каналу високочастотного "нав'язування" представлено на рис.1.

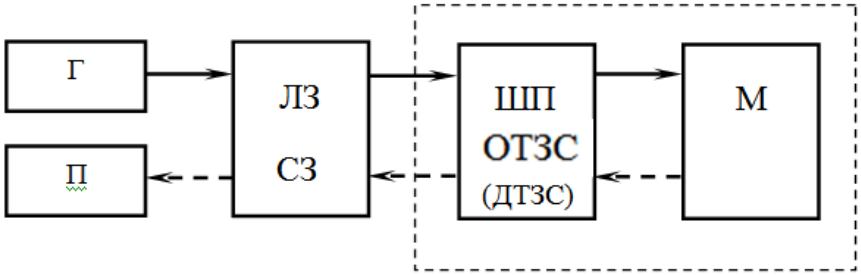

Рис. 1

У представленій схемі зондуючий високочастотний сигнал, що виробляється в генераторі (**Г**), поступає через лінію (систему) зв'язку (ЛЗ, СЗ) на елементи ОТЗС чи ДТЗС. В ОТЗС може циркулювати (у режимі виконання ним основній функції) або впливати на нього (у режимі очікування або використання як ДТЗС за умов, що описані вище) небезпечний сигнал (НС), що несе секретну інформацію. Усередині ОТЗС зондуючий високочастотний сигнал з виходу лінії зв'язку (ЛЗ) поступає по відповідних шляхах проникнення (ШП) на модулюючий елемент (М).

Отримавши в модулюючому елементі **М** модуляцію якого-небудь параметра високочастотного коливання (наприклад, амплітуди, фази) небезпечним сигналом НС (тут можна вважати, що небезпечний сигнал як би "нав'яже" якому-небудь параметру високочастотного сигналу свій закон зміни), зондуючий сигнал відбивається від неузгодженого навантаження, яке представляє модулятор **М** для цього зондуючого сигналу в діапазоні частот зондування, і поширюється у зворотному напрямі, як показано на рисунку пунктиром, до приймача **П**, який в результаті цього отримує інформацію про небезпечний сигнал.

Інформація зазвичай укладена в коефіцієнті модуляції (m – у разі амплітудної і β – у разі фазової модуляції) високочастотного зондуючого сигналу, відбитого від елементів ОТЗС чи ДТЗС.

Сигнали від ліній зв'язку до модуляторів усередині ОТЗС і у зворотному напрямі передаються через кола, утворені:

- ✓ паразитними електричними і магнітними зв'язками (зв'язок через паразитні індуктивності, ємності і їх комбінації);
- ✓ паразитними електромагнітними зв'язками (зв'язок по ефіру);
- ✓ паразитними зв'язками через загальні ланцюги (наприклад, кола заземлення, електроживлення).

Відбитий сигнал має місце в усіх випадках, за винятком одного – режиму повного узгодження.

Враховуючи, що в реальних ОТЗС режим повного узгодження практично неможливо забезпечити, особливо враховуючи широкодіапазонність методу високочастотного "нав'язування", можна вважати, що можливість отримання відбитого високочастотного сигналу по лініях зв'язку, що підключаються до ОТЗС і ДТЗС, є у будь-якому технічному пристрої.

Крім того, слід зазначити, що навіть при узгодженні лінії з навантаженням за наявності зміни величини цього навантаження під впливом небезпечного сигналу в приймачі системи перехоплення з'являється модульований сигнал.

Це повністю підтверджується практикою проведення спецдосліджень апаратури ОТЗС і ДТЗС.

Слід також відмітити, що в загальному випадку лініями зв'язку при високочастотному "нав'язуванні" можуть служити не лише реальні низькочастотні лінії, але і паразитні лінії, утворені будь-якими іншими провідниками (наприклад, заземлюючий провідник – заземлені металоконструкції будівель). В цьому випадку розглянуті вище явища ще більше посилюються.

Зондуючі сигнали високої частоти, використовувані при перехопленні інформації методом високочастотного "нав'язування", поступають по лініях зв'язку на ОТЗС та ДТЗС і проникають потім всередину цих пристроїв наступними шляхами:

- ✓ колами; утвореними паразитними електричними і магнітними зв'язками між елементами пристроїв;
- ✓ за допомогою електромагнітного випромінювання з одних ділянок дротів і кіл, і прийому цих випромінювань іншими дротами і колами (антенний ефект);
- ✓ безпосередньо колами прямого гальванічного зв'язку (наприклад, при підключенні генератора зондуючих коливань до систем заземлення, електроживлення).

Модуляція зондуючих високочастотних сигналів небезпечними сигналами.

Як було відмічено, при дії на кола і елементи ОТЗС зондуючими високочастотними коливаннями, останні в деяких випадках виявляються промодульованими циркулюючими в цих колах небезпечними (мовленнєвими, телеграфно-телекодовими і іншими порівняно низькочастотними) сигналами і можуть бути виділені при подальшій їх обробці в системі перехоплення інформації.

Таким чином, зондуючі високочастотні коливання стають носіями інформації небезпечного сигналу і створюють канал можливого витоку інформації.

Фізична сутність процесу модуляції. Зондуючі високочастотні коливання, що створюються системою перехоплення інформації, характеризуються в початковому стані певним числом постійних параметрів.

У простому випадку в якості зондуючого коливання супротивником може бути застосоване гармонічне (синусоїдальне) коливання. Аналітичне вираження таких коливань в загальному випадку має вигляд:

$$F(t) = A_0 \cos(\omega_0 t + \varphi_0) \tag{1.1}$$

де A_0 – амплітуда коливання,

$(\omega_0 t + \varphi_0)$ – фаза коливання.

При постійних значеннях параметрів A_0 и $(\omega_0 t + \varphi_0)$ коливання, що визначається вказаним співвідношенням, не несе ніякої смислової інформації про стан об'єкта спостереження. Якщо ж в такт з керуючим низькочастотним (НЧ) сигналом (небезпечним сигналом) змінюватимуться основні параметри цього коливання, то результуюче коливання може бути представлене у вигляді:

$$F(t) = A(t) \cdot \cos\Phi(t) \tag{1.2}$$

Тобто, зондуюче коливання в цьому випадку характеризуватиметься двома основними величинами, що змінюються в часі: амплітудою $A(t)$ і фазовим кутом $\Phi(t)$.

Процес, який полягає в тому, що той або інший параметр зондуючого коливання змінюється в часі згідно з оброблюваними в ОТЗС сигналами низької частоти (небезпечними сигналами), є процесом небажаної (паразитної) модуляції.

Відоме [2] представлення АМ коливання

$$u(t) = U_H \cos\omega_0 t + \frac{m}{2} U_H \cos(\omega_0 + \Omega)t + \frac{m}{2} U_H \cos(\omega_0 - \Omega)t \tag{1.3}$$

показує, що модульоване коливання, на підтвердження вищесказаного, є складним коливанням. Перший член суми являє собою зондуюче високочастотне коливання, яке не несе, як було відмічено вище, ніякої інформації про небезпечний сигнал, тоді як два інші члени є інформативними і формують огинаючу та представляють собою нові частотні складові гармонічного характеру, величини амплітуд яких визначаються як $m \cdot U_H / 2$. Оскільки уся перехоплювана інформація знаходиться саме в цих додаткових членах, то, отже, для зменшення або виключення витоку інформації, необхідно зменшити або виключити величини m і U_H.

Отже, сутність явища ВЧ-"нав'язування" полягає в отриманні модульованих високочастотних коливань (коли модулюючим сигналом є перехоплюваний небезпечний сигнал) при дії зондуючого немодульованого коливання високої частоти на вузли технічних засобів (ОТЗС і ДТЗС). Додаткові частотні складові, що з'явилися при цьому, формують високочастотний інформаційний сигнал, мають частоти (ω_0+Ω) та (ω_0–Ω), зрушені відносно зондуючого високочастотного коливання ω_0 на величину модулюючих частот і, отже, за умови $\omega_0 >> \Omega$, є також високочастотними.

Основні принципи здійснення модуляції і умови формування в колах ОТЗС і ДТЗС модульованих коливань. Враховуючи викладене, можна зробити висновок, що дане явище супроводжується процесом лінійного переносу спектра низькочастотного сигналу

(мовленнєвого, телекодового, тощо) в область радіочастотного діапазону. Лінійність характеру вказаного процесу полягає в тому, що при його здійсненні вид і співвідношення між компонентами спектра первинного інформаційного сигналу залишаються незмінними.

Крім того, виходячи з (1.3) це явище можна розглядати як результат перемноження двох початкових коливальних процесів, що взаємодіють між собою в електричних колах ОТЗС. Процес такого перемноження двох коливань може бути здійснений двома способами.

Перший спосіб заснований на використанні елементів, що мають нелінійну провідність. З теорії електричних і радіотехнічних кіл відомо, що якщо на деякий нелінійний елемент з вольтамперною характеристикою, що апроксимується виразом:

$$i = i_0 + \alpha u + \beta u^2 + \gamma u^3,$$

діятимуть дві напруги u_c і $u_г$, то вихідний струм цього елементу міститиме множину комбінаційних складових з частотами

$$\omega_к = \left(\pm r\omega_г \pm q\Omega_c\right),$$

де r і q – цілі позитивні числа (включаючи і шум), а амплітуди і фази їх залежатимуть відповідно від амплітуд і фаз прикладених напруг u_c і $u_г$. Таким чином, елементи з нелінійною провідністю дозволяють реалізувати процес перемноження двох початкових напруг і при цьому, разом з різними комбінаціями їх вищих гармонічних складових, отримати частоти, рівні сумі і різниці частот інформаційної небезпечної і допоміжної (зондуючої) напруг.

Другий спосіб перемноження базується на використанні лінійних кіл зі змінними параметрами (параметричних кіл). Так, якщо деякий чотириполюсник, лінійний по відношенню до зондуючої напруги, матиме періодично змінюваний коефіцієнт передачі

$$K(t) = K_0(1 + \cos\Omega t)$$

то при поданні на його вхід напруги коливань на виході чотириполюсника отримаємо

$$u_{вих.} = K(t) \cdot u_г$$

і тоді

$$u_{вих.} = K_0(1 + \cos\Omega t) \cdot u_{mг} \cos(\omega_г t + \varphi\omega),$$

тобто, в результаті перемножувальної дії даної системи можна виділити напруги, за своїм вираженням аналогічні (1.3).

Таким чином, тільки в результаті нелінійного або параметричного перемноження двох напруг, на відповідному селективному навантаженні можна виділити сигнал, що має вигляд

$$u = u_m(t)\cos[\omega t + \varphi\omega(t)],$$

який відповідає шуканому, зміни амплітуди u_m або фази φ якого повністю визначаються законами зміни амплітуд і фаз вхідних напруг небезпечних сигналів.

В результаті численних досліджень було показано [3], що в колах ОТЗС і ДТЗС, які містять нелінійні елементи і мікрофони, модульовані коливання виникають внаслідок зміни їх опору при спільній дії небезпечного – інформативного сигналу акустоелектричних перетворень, у тому числі – високочастотного зондуючого сигналу. У загальному випадку модулюючі елементи кіл ОТЗС – випадкові модулятори – можна розділити на дві групи:

- ✓ нелінійні і лінійні активні опори (мікрофони, діоди, транзистори, електронні лампи та ін.);
- ✓ нелінійні і лінійні реактивні опори (індуктивності трансформаторів, дроселів, обмоток реле, дзвінкових котушок, ємність конденсаторних мікрофонів та ін.).

Елементи 1-ої групи є, в основному, причиною появи АМ коливань в резистивних колах. Елементи 2-ої групи – ФМ коливань або коливань складнішої форми (наприклад, АМ і ФМ).

Виникнення ненавмисної модуляції в ОТЗС може мати місце лише за цілком певних умов. Для оцінки цих умов передусім з'ясуємо механізм дії високочастотних коливань на кола з навантаженнями, провідність яких змінюється за законом зміни низькочастотного сигналу Ω. Для прикладу розглянемо процес при зміні параметра хоча б одного з елементів кола (наприклад, резистивного опору у вугільному мікрофоні під впливом акустичного поля).

Для випадку, коли $Z=R$ і $Z_M=R_1$, коло складається з джерела напруги частоти ω $e = U_m \cos\omega t$ і двох послідовно включених опорів, постійного – R і змінного – R_1: $R_1=R+ R_0$.

Під впливом звукових коливань мембрана коливається і, натискаючи на вугільний порошок, що знаходиться в мікрофоні, змінює його провідність.

Припустимо, що мікрофон строго лінійний, тобто що провідність суть лінійна функція звукового тиску. Тоді для провідності змінного елементу маємо

$$g = g_0 + kP.$$

Нехай зміна звукового тиску

$$P = P_m \cos\Omega t\,.$$

Тоді для провідності змінної частини кола можна записати

$$g(t) = g_0 + kP_m \cos\Omega t = g_0 + g_1 \cos\Omega t\,.$$

Позначивши

$m = \dfrac{g_1}{g_0}$ (коефіцієнт модуляції для провідності),

маємо $g(t) = g_0(1 + m\cos\Omega t).$

Якщо для електрорушійної сили e, створюваної зовнішнім високочастотним генератором у розглядуваному колі, справедливий вираз

$$e = E_m \cos\omega_0 t\,,$$

де ω_0 – частота високочастотного генератора, то струм в колі буде рівним добутку електрорушійної сили e на провідність кола:

$$i_{вых.} = eg = E_m g_0(1 + m\cos\Omega t)\cos\omega_0 t\,.$$

Отримуємо звичайний вираз амплітудно-модульованого коливання, тому що добуток $E_m g_0(1 + m\cos\Omega t)$ можна розглядати як амплітуду коливань $E_m(1 + m\cos\Omega t)$ частоти ω_0, що змінюється з частотою Ω при постійній величині провідності кола, тобто має місце лінійна параметрична амплітудна модуляція.

Амплітудна модуляція може бути здійснена також за наявності коливальних контурів і нелінійних елементів в колах.

Оцінка основних параметрів методу високочастотного "нав'язування".

В якості основних параметрів для оцінки методу високочастотного "нав'язування" з точки зору реальних можливостей перехоплення інформації можна прийняти наступні:

1. діапазон частот вживаних сигналів зондування;
2. рівень і форма зондуючих сигналів;
3. максимальна відстань, на якій можливе застосування даного методу;
4. способи підключення апаратури зондування до елементів ОТЗС і ДТЗС;
5. можливості методів виділення, обробки і реєстрації отримуваних з елементів ОТЗС і ДТЗС промодульованих високочастотних коливань;
6. імовірність перехоплення секретних відомостей методами високочастотного "нав'язування" (зондування).

На підставі вище викладеного у перспективі проглядається можливість використання деяких норм на вторинні параметри апаратури ОТЗС і ДТЗС: встановлення на початкових етапах розробки цієї апаратури вимог на ефективність екранування конструкції і ступінь фільтрації високочастотних зондуючих сигналів в усіх підключених до апаратури дротах, колах і лініях зв'язку для діапазону частот від 10кГц до 30МГц і більше, та реалізація цих вимог у процесі розробки, а отже, як наслідок, створення технічних засобів захисту від витоку інформації при застосуванні зазначеного методу.

Виконання при розробці апаратури ОТЗС і ДТЗС вимог по екрануванню, фільтрації і розв'язкам в широкому діапазоні частот (від 10кГц до 30МГц і більше) і ряду інших, спрямованих на виключення можливостей перехоплення інформації по каналу витоку, що утворюється при застосуванні методу високочастотного "нав'язування", суттєво зменшить імовірність витоку інформації по переважній більшості інших, відомих нині каналів витоку інформації.

Доцільно розробити спеціальні тимчасові вимоги і рекомендації для розробників апаратури ОТЗС і ДТЗС, забезпечити їх обов'язкове виконання при створенні апаратури ОТЗС і ДТЗС, для яких апріорі пред'являються вимоги забезпечення захищеності інформації від витоку каналами ВЧ-"нав'язування".

Як бути при перевірці на застосування методу ВЧ-"нав'язування" у випадку визначення каналу витоку конфіденційної мовленнєвої інформації з незахищених ДТЗС, які найчастіше використовуються в сучасних умовах на об’єктах інформаційної діяльності? Найпростіший метод захисту – заборона їх використання та заміна на такі, що не мають зазначеного каналу витоку. Наступні заходи полягають в застосуванні пасивних та активних засобів технічного захисту, що не є питанням цієї статті.

Як визначити, що на об’єкті інформаційної діяльності є небезпека витоку мовленнєвої інформації з ОТЗС та ДТЗС і їх струмопровідних комунікацій при застосуванні методу ВЧ-"нав'язування"? На практиці об’єкти інформаційної діяльності, де циркулює мовленнєва інформація, підлягають перевірці спеціальними пристроями контролю, найбільш відомим з яких є ще радянський пристрій "Ожерелье-2", а з сучасних – російські пристрої типу "Арфа", "Облако" та інші, проте особливості роботи з ними є предметом окремої статті.

Список використаної літератури

1. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – СПб.: ООО "Издательство Полигон", 2000. – 896 с.

2. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. Том 1. Несанкционированное получение информации. – К.: Арий, 2008. – 464 с.

3. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. Том 2. Информационная безопасность. – К.: Арий, 2008. – 344 с.

Надійшла 27.07.2017 р. Рецензент: д.т.н., проф. Карпінський М.П.

УДК 004.62+004.77

А.О. Аносов, А.В. Платоненко

ГЕНЕРУВАННЯ УНІКАЛЬНОГО ПАРОЛЮ ЗІ ЗМІННИМ ПРАВИЛОМ УСКЛАДНЕННЯ

Розглянуто метод підвищення захисту бездротових мереж від перехоплення інформації та впливу на неї, шляхом створення надійного паролю зі змінним правилом ускладнення. Даний метод дає змогу його використання для програмних та апаратних засобів захисту, а також можливість застосовувати його для підвищення захисту облікових записів користувачів та інших систем захисту, де необхідне використання надійного паролю.

Ключові слова: інформаційна безпека, загрози інформаційної безпеки, бездротові мережі, захист мереж від несанкціонованого доступу, захист мобільних пристроїв.

Вступ

Ненадійні паролі зазвичай стають причиною хакерських атак [1]. Після того як зловмисник підключиться до мережі, він отримує доступ до підключених пристроїв. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі підключені пристрої також піддаються ризику хакерської атаки, яка вже може здійснюватися віддалено [2].

Більшість атак направлена на підбір паролю, стійкість якого залежить від можливої швидкості підбору. Для сучасного комп'ютера, при стандартних режимах роботи, з використанням центральних процесорів (CPU), швидкість підбору може становити 6000-7000 паролів за секунду, в залежності від моделі та режиму роботи.

Існує можливість збільшити ці значення в тисячі разів, завдяки використанню графічних процесорів у відео-картах (GPU). На прикладі однієї із відео-карт, що використовується для перебору хешів паролів, швидкість підбору може становити до 15 млрд. за секунду, а з використанням GPU-ферм (наприклад 12 відео-карт, об'єднаних для спільної роботи) може досягати 200 млрд. за секунду. Спеціалізовані ферми можуть досягати значення в 350 млрд. переборів за секунду, та не обмежуються цим значенням.

Таким чином кількість часу необхідного на перебір може значно зменшитись, саме тому постає необхідність в ускладненні паролю, для зменшення ймовірності його злому.

Основна частина

Завдання пошуку надійного паролю для захисту інформації в бездротових мережах потребує перевірки на стійкість до підбору. Множина паролів складається з комбінацій символів, які можуть складати пароль, ймовірність підбору якого може здаватись досить малою (при використанні CPU), але враховуючи використання спеціального обладнання (об'єднаних GPU), час на підбір може значно зменшитись, а відповідно, ймовірність підбору паролю буде більшою, ніж могло здаватись.

Враховуючи статистику [2] та проведені розрахунки [3], можна вважати, що використання методу генерування унікального паролю зі змінним правилом ускладнення дасть змогу підвищити рівень захищеності бездротової мережі, шляхом зменшення ймовірності підбору пароля.

Складовими частинами, що покладені в основу методу є використання інтегрованого підходу до аналізу та генерації паролів:

- за показниками довжини,
- набору символів з різних множин,
- на можливу/часткову наявність у різних за типами словниках паролів.