УДК 654.1

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ ВІД ВИТОКУ ІНФОРМАЦІЇ

Пишка Дмитро Іванович, Торбєєва Марина Василівна
Державний ВНЗ «НГУ», www.nmu.org.ua, Dmytriy@email.ua

У доповіді виконаний аналітичний огляд методів та засобів захисту конфіденційної інформації від витоку через мобільні телефони та зроблені деякі рекомендації щодо їх застосування.

Ключові слова – захист GSM каналу, мобільні пристрої, канал витоку інформації.

Сучасні засоби мобільного зв'язку дають людині більше можливостей для обміну інформацією. Але разом з цим вони також можуть стати небезпечним інструментом для несанкціонованого отримання інформації сторонніми особами.

Перепрограмування мобільного телефону, підміна або подарунок модифікованого пристрою, впровадження вірусу у комунікатор дадуть можливість отримувати доступ к даним на мобільному телефоні, а також прослуховувати всі розмови, що ведуться поблизу нього.

З широким розповсюдженням мобільних пристроїв стає актуальним захист циркулюючої ними інформації. Для цього використовуються пасивні, активні та програмні методи захисту, такі як: екранування, індикація несанкціонованої активності мобільного пристрою, активне зашумлення, шифрування трафіку та маскування мовної інформації, а також методи ідентифікації та блокування несанкціонованого доступу до мобільного пристрою.

Принцип дії екранування реалізований за допомогою спеціального чохла, який блокує зв'язок телефону з базовою станцією. Для базової станції телефон знаходиться у статусі «поза зоною досяжності». Саме тому немає можливості визначити, що телефон вимкнуто навмисно.

Активні методи захисту на основі технології активного зашумлення та додаткової індикації застосовуються у «GSM-сейфі», «GSM-кейсі» та «GSM-Box».

GSM SAFE – це акустичний сейф, призначений для захисту від прослуховування через мобільні пристрої. Автоматичне спрацьовування GSM SAFE відбувається під час несанкціонованої віддаленої активації мобільного пристрою зв'язку. Він починає генерувати шуми в чутному діапазоні акустичних частот, що маскують мову. Це робить неможливим прослуховування і запис розмови, а на самому пристрої виникне слабкий шум приладу і мерехтіння світлодіода. Звичайні дзвінки будуть проходити у штатному режимі. Прихований дзвінок буде відразу детектуватися у трубці і сторонній особі буде чутний лише шумовий сигнал.

GSM CASE представляє собою акустичний кейс, що захищає від прослуховування через мобільний телефон шляхом його дистанційної активації. Принцип дії виробу – активація вбудованого генератора шуму детектором GSM-випромінювання. Як тільки телефон активується – вмикається генератор шуму, і телефон більше не може «підслуховувати». Легкий шум вказує на активацію телефону. Штатні дзвінки проходять у звичайному режимі, а при вийманні телефону з виробу генератор автоматично вимикається.

Індикатор активації мобільних засобів зв'язку GSM-Box усуває можливість несанкціонованого доступу до мобільних засобів зв'язку. Контрольовані протоколи: GSM900/1800, Wi-Fi, Bluetooth. GSM-BOX - це, в першу чергу, відображаючий пристрій, який дозволяє визначити несанкціоновану активність мобільного телефону, а також Bluetooth-обмін. У момент появи радіохвиль пристрій включить шумовий сигнал і засвітиться індикатор. Чутний шум при відсутності вхідного дзвінка або SMS свідчить про те, що відбувається якийсь обмін з базовою станцією. Якщо телефон розташувати мікрофоном у напрямку до динаміка GSM-Box, шум, що генерується пристроєм, глушить мікрофон, і прослуховування простору навколо телефону буде неможливим.

Для забезпечення конфіденційності телефонних розмов, що здійснюються незахищеним GSM каналом, використовуються системи безпеки на основі шифрування даних. В країнах СНД для цього використовується друга версія алгоритму A5/2. Алгоритм заснований на регістрах зсуву з лінійної зворотним зв'язком певної довжини (19, 22, 23 біта). Початкові заповнення регістрів визначаються секретним і відкритим ключами. Відкритий ключ відомий і різний для кожного нового сеансу. При зв'язку двох абонентів шифрування здійснюється двічі, між абонентом і базовою станцією, станцією та абонентом. Але цього буває недостатньо.

Принцип дії більшості пристроїв для захисту передачі даних і голосу засновано на додатковому шифруванні даних. Одним з таких засобів є скремблери. Перевагою скремблерів є висока надійність захисту від будь-якого засобу прослуховування стільникових телефонів, у тому числі і від спеціального обладнання, встановленого у оператора. Недоліком є необхідність усім абонентам мати сумісні пристрої для приватної бесіди.

Криптофони - це звичайні смартфони з додатковим програмним забезпеченням. Першими такі пристрої розробила німецька компанія Cryptophone, звідки і їх назва. Принцип дії криптофонів, як і скремблерів, полягає у наступному: сигнали з мікрофону оцифровуються, кодуються і відправляються в мережу стільникового зв'язку в зашифрованому вигляді. Вся різниця між криптофонами і скремблерами полягає у способі

реалізації цієї методики. Головною перевагою криптофона є використання двох алгоритмів шифрування AES і Twofish з ключами довжиною 256 біт, розподіленими за системою Діффі-Хелмана (з власним ключем завдовжки 4096 біт). Також існують криптографічні картки SECUSMART, які встановлюються у телефон і перетворюють його у повноцінний криптофон.

Маскувальники мови працюють за абсолютно іншим принципом, ніж скремблери і криптофони. Ці пристрої призначені для стаціонарних телефонів, саме до яких вони і підключаються. Маскувальники дозволяють захищати всі розмови, в яких приймають участь будь-які інші, у тому числі і стільникові, абоненти. Після включення захисту маскувальник генерує та подає в лінію зв'язку шум, який розповсюджується по всьому каналу. Таким чином, зловмисник, що намагається прослуховувати розмову, отримає тільки безладний набір звуків. Пристрій накладає на сигнали спеціальний фільтр, який компенсує шум, виключаючи з нього розмову абонента. Недолік маскувальника в тому, що він може встановлювати тільки односторонній захист.

Комбінація застосування цих пристроїв дає змогу достатньо ефективно захиститись від більшості випадків прослуховування. Інтелектуальні детектори радіоперешкод контролюють режими передачі даних і виявляють несанкціоновані підключення. При цьому мобільні телефони залишаються у включеному стані, на зв'язку. На відміну від чохла-блокиратора, який блокує усі сигнали.

Для захисту переговорів, що ведуться мобільними телефонами в GSM-каналі, найбільше підходять скремблери. Вони підключаються до вже існуючого апарату і прості у використанні. Криптофони, як і скремблери, шифрують сигнали, але мають більш стійкі алгоритми, виконані як цілісні пристрої та ще й можуть використовуватись як багатофункціональний комунікатор. Тому і вартість криптофонів значно більша. Для дзвінків на стаціонарний телефон із стільникового в закритому режимі краще використовувати маскувальник мови. А для захисту від вірусних атак та несанкціонованого доступу на мобільний пристрій можливо застосування програмних методів захисту.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Вся правда о прослушивании мобильных телефонов: Спецвыпуск: Хакер, номер #059, стр. 059-052-1 (Електрон. ресурс) / Спосіб доступу: URL: http://www.xakep.ru/magazine/xs/059/052/1.asp

2. Документация на средства защиты: «Диджитал лабс» (електронний реурс) / Способ доступа URL http://www.digiscan-labs.com/ru/Products/TSCM-devices/GSM-SAFE-3.html

3.Коммерческие речевые шифраторы: журнал «НЕСТОР» (електронний реурс)/ Способ доступа URL http://www.nestor.minsk.by/sr/2006/03/sr60312.html