УДК 004.056.5

ВНУТРІШНІ АНТРОПОГЕННІ ДЖЕРЕЛА ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СТІЛЬНИКОВИХ СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ СТАНДАРТУ LTE З ІНТЕГРОВАНИМИ ФЕМТОСОТАМИ

Нікітенко К.О., ЛДУ БЖД
НК – Кухарська Н.П., к. ф.-м. н., доцент, ЛДУ БЖД

Джерелами загроз інформаційної безпеки (ІБ) можуть бути як суб'єкти (людина), так і об'єктивні прояви (природні і техногенні явища). Крім того, по відношенню до досліджуваного об'єкту джерела загроз можуть бути і внутрішніми, і зовнішніми. Розглянемо внутрішні антропогенні джерела загроз, властиві стільниковим системам мобільного зв'язку (ССМЗ) стандарту LTE з інтегрованими фемтосотами (ІФ).

Порушник – це суб'єкт, який здійснює деструктивний вплив на деякий об’єкт помилково, через незнання або усвідомлено і використовує для цього доступні можливості, методи і засоби.

При порушеннях, викликаних безвідповідальністю, користувач робить деструктивні дії, які не пов'язані зі злим умислом і в більшості випадків обумовлені його некомпетентністю або недбалістю. Порушення ІБ мережі може бути також спричинене корисливим інтересом користувача системи, коли він буде цілеспрямовано атакувати механізми системи захисту для порушення властивостей безпеки інформації, що циркулює в мережі. І для такого порушника використовують термін зловмисник.

Для досягнення поставленої мети зловмисник повинен докласти зусилля та використати відповідні ресурси. У відповідь адміністратор об’єкта, дослідивши причини порушень, зобов'язаний вплинути або на самі причини, або переконфігурувати систему захисту для протидії конкретному виду впливу.

Існує низка причин, через які ССМЗ стандарту LTE з ІФ стають об'єктами атак зловмисників:

- Фемтосоти для зловмисника більш уразливі, на відміну від класичних базових станцій через специфіку розміщення і функціональне призначення.
- Світові виробники абонентського обладнання поки що не здатні запропонувати простих і ефективних механізмів захисту від стороннього проникнення.
- При зломі фемтосот доступ виявляється анонімним на відміну від дротових мереж.
- Злом фемтосоти може дозволити зловмиснику отримати віддалений доступ до сервісів ядра мережі.

З огляду на вищевказані мотиви, до групи потенційних внутрішніх зловмисників віднесемо такі категорії персоналу:

- Адміністратори, співробітники служб ІБ, що володіють знаннями про структуру мережі та системи захисту, а також доступом у контрольовану зону (КЗ).
- Прикладні і системні програмісти, що володіють глибокими знаннями в сфері комп'ютерних технологій, знаннями структури мережі, мають доступ в КЗ, але володіють меншими привілеями і правами, ніж адміністратори мережі.
- Безпосередні користувачі і оператори стільникової мережі, технічний персонал з обслуговування будівель і обчислювальної техніки, допоміжний персонал і тимчасові працівники. Необов'язково володіють глибокими знаннями в сфері комп'ютерних технологій, але мають частковий або повний доступ в КЗ, а також потенційно можуть з'ясувати структуру мережі.