АНАЛІЗ ІНФОРМАЦІЙНИХ ЗАГРОЗ У БЕЗПРОВОДОВИХ МЕРЕЖАХ ПІДПРИЄМСТВА

Куля Ю.Е.

Кафедра «Інфокомунікаційної інженерії»
ім. В.В. Поповського», ХНУРЕ, Україна

E-mail: yuliia.kulia@nure.ua

Abstract

Analysis of the current situation shows that the main reason for the indecision of the transition to wireless networks is the problem of information security, the level of which for both individual lines and for the system as a whole has not yet been determined. Wireless networks use air and space to transmit and receive information. Ensuring that the confidentiality and integrity of information is properly protected when it is transmitted between workstations and access points is a very important aspect of the security of the system as a whole. Due to the wide availability of wireless devices and their low cost, security breaches occur. The specifics of wireless networks provide that data can be intercepted and changed at any time.

Безпроводові мережі використовують повітря і простір для передачі та прийому інформації. Тобто сигнали є відкритими для будь-якої особи, що знаходиться в зоні дії. Забезпечення належного захисту конфіденційності та цілісності інформації при її передачі між робочими станціями і точками доступу є дуже важливим аспектом безпеки всієї системи в цілому. Велика популярність безпроводових пристроїв та їх доступна вартість призводять до того, що в периметрі мережної безпеки виникають проломи.

Специфіка безпроводових мереж (БМ) має на увазі, що дані можуть бути перехоплені та змінені у будь-який момент. Для одних технологій досить стандартного безпроводового адаптера, для інших потрібне спеціалізоване обладнання. Але в будь-якому випадку, ці загрози реалізуються достатньо просто, і для протистояння їм потрібні ефективні криптографічні механізми захисту даних. Спочатку визначимо основні терміни, які будуть використовуватися в подальшому: «вразливість», «загроза» та «атака». Під вразливістю системи захисту розуміється така її властивість, яка може бути використана зловмисником для здійснення несанкціонованого доступу (НСД) до інформації. При цьому будь-яка вразливість системи захисту несе в собі загрозу здійснення зловмисником НСД до інформації, за допомогою реалізації атаки (або атак, які в загальному випадку можуть принципово відрізнятися) на вразливість в системі захисту. Таким чином, саме уразливість системи захисту підприємства – це ознака системи, а наявність (відсутність) вразливостей є характеристикою захищеності системи [1]. Вочевидь, що в загальному випадку причиною вразливості може бути або некоректність реалізації механізму захисту, або недостатність набору механізмів для умов використання об'єкта інформатизації, що захищається. Взагалі кажучи, властивості коректності реалізації і повноти (достатності для умов використання) є основними властивостями будь-якої технічної системи, в тому числі, і властивостями системи захисту інформації. Аналіз існуючого стану показує, що основною причиною нерішучості переходу на безпроводові мережі є проблеми інформаційної безпеки, рівень якої як для окремих ліній, так і для системи в цілому, поки не визначений. Готуючись до забезпечення безпеки безпроводових мереж, перш за все, необхідно встановити, що може їм загрожувати [2].

Відразу слід зазначити, що безпроводові мережі відрізняються від проводових тільки на перших двох – фізичному і частково канальному рівнях семирівневої моделі взаємодії відкритих систем. Більш високі рівні реалізуються відповідно до тих самих принципів, що і в дротових мережах,
а реальна безпека мереж забезпечується саме на цих нижчих рівнях.

Прийнято вважати, що безпеці безпроводових мереж підприємства загрожують (рис. 1):

- порушення фізичної цілісності мережі;
- підслуховування трафіку;
- вторгнення в мережу.
-

Рис. 1. Інформаційне середовище підприємства

Загрозу мережній безпеці підприємства можуть представляти природні явища і технічні пристрої, проте тільки люди впроваджуються в мережу для навмисного отримання або знищення інформації і саме вони становлять найбільшу загрозу. При розгляді вразливостей мереж стандарту 802.11 можна виділити дві групи загроз: загрози на сигнальному рівні і загрози на інформаційному рівні.

Наявність вразливостей на сигнальному рівні робить проблематичним захист інформаційного рівня, на якому вони повинні бути попереджені [3]:

- цілеспрямоване спотворення переданих та отриманих даних;
- перехоплення управління системою зв'язку або інформаційною системою.

Висновки

На даний час ще не розроблена детальна модель загроз, які існують в області цифрових мереж безпроводового доступу, і методів боротьби з ними. Тому потрібно відзначити, що високий ступінь захищеності каналу на сигнальному рівні не є гарантією забезпечення настільки ж високої інформаційної захищеності всієї системи.

Література:

1. Буров Є.В. Комп'ютерні мережі. — Львів : БаК, 2003. — 584 с.
2. Климаш М.М., Пелішок В.О. Проектування ефективних систем безпровідного зв'язку. — Львів: «Львівська політехніка, 2010. — 224 с.
3. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.