однаковий з «закритим». Якщо до тексту електронного документа були внесені зміни після його підписання КЕП, то система заблокує дану процедуру. Таким чином, підписати електронний документ може тільки власник «закритого» ключа, а перевірити наявність КЕП – будь-хто, у кого є «відкритий» ключ, відповідний «закритому» ключу відправника.

Отже, було систематизовано і виділено принципи функціонування, засоби захисту інформації у ході організації електронного документообігу. Впровадження СЕД забезпечує підприємство усім необхідним для своєчасного прийняття рішень, реагування на ситуації та оптимізація робочого процесу на підприємстві. СЕД можна називати захищеною, якщо в ній присутні такі системи захисту інформації: захист електронних документів, що містять конфіденційну інформацію, шляхом перевірки її КЕП на цілісність даних; керування доступом та автентифікація; контроль та протоколювання роботи співробітників з документами та ін..

Напрямком подальших досліджень є створення моделі всебічно захищеної системи електронного документообігу, що може бути використаною у діяльності реального підприємства для підвищення рівня інформаційної безпеки та ефективності його роботи.

Список використаних джерел

1. Кандзюба С. П. Електронний документообіг. Реінжиніринг адміністративних процесів в органах публічної влади / Кандзюба С. П., Матвійчук Р. М.. – Київ, 2017.
2. Матвієнко О. Основи організації електронного документообігу. Навчальний посібник / Матвієнко О., Цивін М. – Київ: Центр учбової літератури, 2008. – 112 с.
3. Кукарін О. Б. Електронний документообіг та захист інформації. Навчальний посібник / Кукарін О. Б. – Київ: НАДУ, 2015. – 84 с.
4. Закон України «Про електронні довірчі послуги». https://zakon.rada.gov.ua/laws/show/2155-19.

УДК 004.056.53

МЕТОДИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ ВІД КИБЕРАТАК

Вильотніков В. В., студ. гр. КБ-161
Науковий керівник**: Базилевич В. М.,** к.е.н., доцент
Національний університет «Чернігівська політехніка»

На сьогоднішній день, зважаючи на велику інформатизацію суспільства, потребу у мобільності користувачів мережі Internet все більшою і більшою популярністю користуються бездротові мережі. Сучасний розвиток бездротових мереж дозволяє встановлювати з'єднання такої ж якості, як і мережі з використанням фізичного середовища передачі даних, але із значно більшою кількістю користувачів. Але при цьому виникає необхідність захисту переданої інформації в таких типах мереж, тобто використання механізмів захисту і шифрування даних. Так як загрози інформаційним ресурсам, в деяких випадках, можуть бути великими і катастрофічними. Тому актуальним є дослідження методів підвищення ефективності захисту інформації в бездротових комп'ютерних мережах.

Для проведення досліджень необхідно провести аналіз можливих загроз, визначити результати їх впливу та здійснити системний аналіз методів захисту від них.

Базовим стандартом, який визначає набір протоколів для передачі даних в бездротових мережах є IEEE 802.11. Цей стандарт постійно доповнюється та оновлюється, таким чином його нові версії були опубліковані в 1999, 2007, 2012 роках, а також наступна очікується ще в 2016 році.

Існують основні та допоміжні методи захисту бездротових мереж.

Основними протоколами, які використовуються на даний час в бездротових мережах є: WEP Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access II), а

також стандарт IEEE 802.1X, який описує процес інкапсуляції даних EAP (Extensible Authentication Protocol).

Найпростішим способом захисту від криптографічних атак є використання WPA2. WPA / WPA2 значно підвищує безпеку бездротової мережі. Але додатковий захист відбувається за рахунок додаткової складності протоколу. На високому рівні, WPA атаки можна розділити на дві категорії: атаки аутентифікації та атаки шифрування.

Реалізація протоколу безпеки WPA2, безумовно, є кращим вирішенням проблем безпеки бездротової мережі. Поряд з тим доповненням до основних рекомендацій можуть бути такі: приховування паролів, використання MAC фільтрації для підключених пристроїв та побудова складних паролів.

Для управління мережевою структурою і типами пакетів, які передаються бездротовими мережами, були проаналізовані поняття і методи протоколів захисту за допомогою документації, представленої IEEE, основних протоколів, таких як: WEP, WPA, WPA2 і основних типів шифрування, які вони використовують.

Головна відмінність бездротових мереж від проводових пов’язана з неконтрольованою областю між кінцевими точками мережі. Це дає змогу атакуючим, що перебувають близько від бездротових структур, робити багато нападів, які були неможливі у проводовій мережі.[1]

Проаналізуємо загрози з погляду звичайної бездротової мережі передачі даних, їхню актуальність для нас і стійкість до них нашої системи. Як і будь-яка інша бездротова мережа, мережа ZigBee піддана таким навмисним загрозам:

1. Підслуховування.
2. Відмова в обслуговуванні (Denial of Service - DOS).
3. Глушіння:
   - кінцевого (RFD) пристрою;
   - роутера (модуля FFD);
   - координатора.
4. Крадіжка фізичного пристрою.
5. Загрози криптозахисту:
   - пасивні мережеві атаки;
   - активні мережеві атаки.
6. Загрози автентифікації.

Крім того, перерахуємо загрози крім, тих, що є специфічними для бездротових мереж:

1) витік прошивань і відповідно витік ключів, які спочатку там були вбудовані;

2) несанкціоновані дії осіб, що мають доступ до терміналу захисту:
   - відключення датчиків або системи загалом;
   - знищення записів у журналі або файла журналу загалом.
   -

Для нашої системи характерні такі випадкові загрози:

1) вихід з ладу устаткування;
2) збій програми;
3) переривання живлення.

Стандартні методи захисту у мережах ZigBee [4, 5]:

- керування доступом за допомогою списків контролю доступу ACL;
- шифрування даних для захисту від несанкціонованого доступу;
- контроль цілісності кадру;
- оновлення симетричних ключів розсиланням.

У нашій системі [3] використовуватимемо усі ці методи захисту від можливих загроз, а також додаткові:

- синхронізацію за часом;
- організаційні заходи захисту;
- використання перевірених елементів відомих фірм із високими показниками

надійності продукції, що випускається;

- реєстрацію подій;
- обмеження, контроль і облік доступу;
- архівацію й резервування, використання для цього надійних засобів зберігання даних;
- тестування й перевірку програмного забезпечення на стійкість до збоїв;
- резервне живлення.

Отже, істотне збільшення використання бездротових мереж призвело до розробки механізмів безпеки, які спочатку були подолані зловмисниками, тому необхідне комплексне рішення для захисту мережі. Для цього доцільно впровадити технологію WPA2 в усіх типах бездротових мереж з використанням методології, яка включає в себе: створення пароля, створення плану забезпечення безпеки і захисту програмного забезпечення, що дозволяє більшу складність і безпеку бездротової мережі.[2]

Список використаних джерел

1. Матеріали V Міжнародної науково-технічної конференції молодих учених та студентів. Актуальні задачі сучасних технологій – Тернопіль 17-18 листопада 2016 [Електронний ресурс] – Режим доступу до ресурсу: http://elartu.tntu.edu.ua/bitstream/123456789/20131/2/ConfATMT_2016vII_Kovalenko_V_S-Methods_of_protecting_wireless_53.pdf

2. Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв [Електронний ресурс] – http://ena.lp.edu.ua/bitstream/ntb/21459/1/36-192-197.

УДК 004.056.5

АНАЛІЗ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕФОННИХ МЕРЕЖАХ

Васильєва С. П., студ. гр КБ-161
Науковий керівник: **Гур'єв В. І.,** к.т.н., доцент
Національний університет «Чернігівська політехніка»

На даний момент до складу телекомунікаційних систем входять телефонні мережі, основою яких є телефонні станції. Сучасні телефонні станції за архітектурою схожі на комп'ютери й сервери. Тому захисту мереж телефонного зв'язку необхідно приділити не менше уваги, ніж забезпечення безпеки комп'ютерних мереж.

Телефонні мережі являють собою сукупність кінцевих пристроїв (терміналів) телефонних станцій, ліній і каналів телефонної мережі, транзитних вузлів комутації.

Об'єкти телефонної мережі (АТС, телефонні апарати) можуть піддаватися таким атакам:

- несанкціонований доступ до програмних портів АТС;
- несанкціоноване використання послуг телефонних переговорів.

Несанкціонований доступ до програмних портів АТС. Джерелом загрози є зовнішній порушник і програмно-апаратна закладка. Засоби поширення – електромагнітні хвилі, радіоефір та наведення в провідниках, що виходять за межі контрольованої зони. Загроза реалізується через активацію закладок в програмному забезпеченні телефонних станцій за допомогою використання спеціалізованого цифрового термінала. Внаслідок такого несанкціонованого доступу може відбутися порушення конфіденційності або цілісності. Наприклад, замаскована передача даних з телефонної бази по службовому каналу, прослуховування переговорів абонентів або повне блокування роботи телефонної станції.

Несанкціоноване використання послуг телефонних переговорів. Джерело загрози – зовнішній порушник. Поширюється шляхом використання сервісної функції DISA, яка дозволяє забезпечити прямий доступ віддалених користувачів до їх внутрішніх сервісних послуг. Зловмисник здійснює з'єднання з номером УВАТС (установчої виробничої АТС)