УДК 004.056.53

Соколов В. Ю., Карацюба К. І. *(Держ. унів-т інформ.-комунікаційних технологій)*

ВИКОРИСТАННЯ ДЕРЕВ АТАК ДЛЯ АНАЛІЗУ ЗАХИЩЕНОСТІ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ СТАНДАРТУ IEEE 802.11

Соколов В. Ю., Карацюба К. І. Використання дерев атак для аналізу захищеності безпроводових технологій стандарту IEEE 802.11. Розглянуто дерево атак на безпроводову мережу. Описано головні атаки, які найбільше загрожують конфіденційності, цілісності, доступності та спостережності інформації, що передається через безпроводову мережу. Розглянуто ймовірність успішної реалізації таких поширених атак, як прослуховування, DDoS-атаки, підміни ARP-записів, фальсифікації пакетів, повна імперсоналізація (з боку як передавача, так и приймача), а також злом WEP-ключів. Виявлено різницю у принципах реакції на атаку для програмного забезпечення і адміністратора.

Ключові слова: ТОЧКА БЕЗПРОВОДОВОГО ДОСТУПУ, БЕЗПРОВОДОВА МЕРЕЖА, ЕЛЕКТРОМАГНІТНА ЗАВАДА, ДЖЕРЕЛО ЗАВАДИ, АТАКА НА БЕЗПРОВОДОВУ МЕРЕЖУ.

Соколов В. Ю., Карацюба К. И. Использование деревьев атак для анализа защищенности беспроводных технологий стандарта IEEE 802.11. Рассмотрено дерево атак на беспроводную сеть. Описаны главные атаки, которые более всего угрожают конфиденциальности, целостности, доступности и наблюдаемости передаваемой через беспроводную сеть информации. Рассмотрена вероятность успешной реализации таких распространенных атак, как прослушивание, DDoS-атаки, подмены ARP-записей, фальсификации пакетов, полная имперсонализация (со стороны как передатчика, так и приемника), а также взлом WEP-ключей. Обнаружено различие в принципах реакции на атаку для программного обеспечения и администратора.

Ключевые слова: ТОЧКА БЕСПРОВОДНОГО ДОСТУПА, БЕСПРОВОДНАЯ СЕТЬ, ЭЛЕКТРОМАГНИТНАЯ ПОМЕХА, ИСТОЧНИК ПОМЕХИ, АТАКА НА БЕСПРОВОДНУЮ СЕТЬ.

Sokolov V. Yu., Karatsyuba K. I. Usage of Trees to Attack Security Analysis of IEEE 802.11 Wireless Technology Standard. Considered a tree attacks on a wireless network. We describe the main attack, which most threaten the confidentiality, integrity, availability and sposterezhnosti information transmitted through the wireless network. We consider the likelihood of successful implementation of such common attacks as listening, DDoS-attacks, spoofing ARP-track rigging package, complete impersonalizatsiya (from both the transmitter and receiver so), and hacking WEP-keys. Revealed differences in response to attack the principles for software and administrator.

Key words: ACCESS POINT, WIRELESS NETWORK, ELECTROMAGNETIC INTERFERENCE, SOURCE OF INTERFERENCE, ATTACK ON WIRELESS NETWORK.

Постановка задачі. Кількість точок бездротового доступу в світі росте з кожним днем, обіцяючи в недалекому майбутньому широкосмуговий вхід в глобальну мережу з будь-яких точки світу. Разом з тим, з розширенням використання безпроводових технологій виникає проблема системного підходу до захисту всієї безпроводової інфраструктури, а не лише окремих точок безпроводового доступу (ТБД). Проблема ускладнюється легкістю доступу до середовища передавання даних. Зловмиснику достатньо бути в зоні покриття, а використання спрямованих антен розширює радіус небезпечної зони до декількох кілометрів. Для системного підходу потрібний універсальний інструментарій, який може легко розширюватися і змінювати свою структуру.

В [1] приведені основні методи побудови і роботи з деревами атак, які дозволяють застосовувати дерева не лише для проводових мереж, а також для безпроводових і змішаних. Автори [2] і [3] приводять детальний аналіз можливих атак. А в [4] дається спроба систематизації атак на безпроводові мережі, в [5] і [6] надаються перші рекомендації по захисту від несанкціонованого доступу. В [7] приведено статистику використання безпроводових технологій, за якою можна спостерігати динаміку розвитку сучасних безпроводових мереж.

Метою представленої праці є побудова дерева атак для безпроводових мереж, виявлення слабких місць і надання рекомендацій до підвищення захищеності ТБД.

Виклад основного матеріалу дослідження. Для систематизації можливих атак на безпроводові мережі і окремі ТБД використано методику побудови дерева атак. Такий підхід дозволяє отримати результати, за допомогою яких можливо побудувати автоматичну

систему виявлення атак і потенційних загроз, а також дає наочний інструментарії спеціалісту з інформаційної безпеки для аналізу і додавання нові видів атак в існуюче дерево.

Для побудови дерева атак потрібно систематизувати відомі атаки. Систематизація атак може бути за різними критеріями. Автори даної статті вибрали верхній рівень дерева атак за трьома групами: атаки на передавач, приймач та середовище. В свою чергу кожна група поділяється на підгрупи.

Атаки на передавач. Атаки на передавач можуть бути п'яти видів: *атака* «відмова в обслуговуванні» в адресу станції (DDoS-атака); повна *імперсоналізація* від імені легітимної станції; *приглушення* базової станції; *фальсифікація* IP-пакетів від імені легітимної станції; *атака* підміни ARP-записів.

Атака «відмова в обслуговуванні» в адресу станції полягає у створенні завади при доступі користувача до мережевих ресурсів. Стандартні методи ініціювання DDoS-атаки полягають в передаванні величезної кількості фіктивних пакетів, що заповнюють легальний трафік і призводять до зависання систем. DDoS-атака може проводитися як на фізичному, так і на канальному рівні. Напад на фізичний рівень у безпроводовій мережі набагато простіший, ніж на фізичний рівень в проводовій мережі, тому що фізичний рівень в безпроводовій мережі – це абстрактне місце навколо точки доступу. А факт проведення DDoS-атаки на фізичному рівні в безпроводової мережі довести досить важко. Зловмисник може створити пристрій, що заповнює весь спектр на частоті 2,4 ГГц завадами (наприклад, за допомогою магнетрона від НВЧ-печі) і нелегальним трафіком (наприклад, використовуючи декілька безпроводових інтерфейсів, які постійно обмінюються даними між собою). На канальному рівні стека OSI атака реалізується менш "грубими" способами (наприклад, імітація чужої MAC-адреси) [8]. Абсолютного захисту від подібних атак не існує, але деякі заходи дозволяють зменшити наслідки від проведення даного типу атак: налаштування міжмережевого екрану для відстеження підозрілих пакетів і активності, відстеження топології мережі і блокування "аномальних" даних за маскою тощо [9].

Повну імперсоналізацію від імені легітимної станції у безпроводовій мережі визначити складніше, ніж в проводовій. SSID (Service Set IDentifier) і MAC-адреси ТБД передаються в середовищі у відкритому вигляді, тому підробити їх досить легко, після чого можна зменшити пропускну здатності мережі, вставляти неправильні фрейми і атакувати алгоритми шифрування, влаштовувати атаки на структуру мережі (наприклад, ARP Poisoning для TKIP). Імперсоналізація користувача можлива не тільки у випадку MAC-аутентифікації або застосування статичних ключів, але і при використанні схеми на основі LEAP (Lightweight Extensible Authentication Protocol), EAP-TLS (EAP-Transport Layer Security) або PEAP (Protected Extensible Authentication Protocol) [10].

Приглушення базової станції або ТБД надає можливість підмінити її атакуючою станцією. Для тимчасового відключення ТБД часто використовують DDoS-атаку, після чого проводиться підміна на ТБД зловмисника. Абсолютного захисту від подібних атак не існує, але можна зменшити їх ймовірність вибором місця встановлення ТБД [11].

Фальсифікація IP-пакетів від імені легітимної станції (або IP-Spoofing) полягає у використанні IP-адреса з викраденої DNS-зони для генерації IP-пакетів, що імітують пакети від вузлів мережі (насправді ж, ці пакети можуть використовуватися для крадіжки інформації або злому ресурсів). Існує кілька варіацій атаки: підміна не всліпу (Non-Blind Spoofing) і підміна всліпу (Blind Spoofing), які відрізняються лише способом отримання доступу до заголовків пакетів [12; 13].

Атака підміни ARP-записів (Address Resolution Protocol) побудована на використанні недоліку швидкого з'єднання з легітимною станцією за одним записом IP-адрес без додаткової перевірки MAC-адреси. При підробці пакетів з IP-адресою (в яких буде стверджуватися, що IP належить до MAC-адреси іншого комп'ютера) всі дані, які передаються з використанням скороченого методу визначення комбінацій MAC/IP-адрес, будуть приходити на комп'ютер зловмисника. Таким чином, зловмисник може отримати

пакети, просто замінюючи в даному локальному кеші комбінації MAC/IP-адрес для будь-яких двох хостів, пов'язаних з фізичною мережею, в якій запущена ТБД [8].

Атаки на приймач. Атаки на приймач поділяються на три підгрупи: *атака* «відмова в обслуговуванні» в адресу точки доступу; *повна* імперсоналізація від імені точки доступу; *приглушення* клієнтської станції.

Атака «відмова в обслуговуванні» в адресу точки доступу та повна імперсоналізація від імені точки доступу за принципом дії співпадають з описаними вище для передавача. Різниця полягає лише в напрямку атаки.

Приглушення клієнтської станції дає зловмиснику можливість заміняти клієнта нелегітимною станцією. Також глушіння може використовуватися для відмови в обслуговуванні клієнта або для підміни частини даних [11].

Атаки на середовище. Найбільшу групу атак на середовище можна поділити на дві підгрупи: заповнення ефіру та прослуховування.

Заповнення ефіру проводиться генеруванням навмисних електромагнітних завад (ЕМЗ), які погіршують якість функціонування інформаційної системи. ЕМЗ відрізняються за походженням, структурою і природою. Радіотехнічні, електротехнічні й електронні засоби, що створюють у процесі роботи ЕМЗ, називають джерелами завад (ДЗ).

Відносно класифікації ДЗ ЕМЗ можна розділити на стаціонарні, індустріальні, природні і контактні. Індустріальні ЕМЗ створюються електротехнічними, електронними або радіоелектронними пристроями (крім випромінювання передавача через високочастотний тракт). Як правило, індустріальна завада має імпульсний характер, характеристики якого залежать від типу конкретного пристрою. Контактні ЕМЗ створюються в результаті впливу електромагнітного поля радіопередавача на механічний контакт з перемінним опором, що перевипромінює електромагнітне поле.

За проявом в часі ЕМЗ бувають: *безупинні* (рівень не зменшується нижче визначеного граничного рівня довше 1 с); *нетривалі* (час дії менше 1 с); *короткочасні* (час дії менше 0,2 с); *регулярні* (з'являються і зникають через однакові проміжки часу); *нерегулярні*; *випадкові стаціонарні* (поточний процес має випадкову природу, відбувається без істотних змін математичного очікування перешкоди в часі); *випадкові нестаціонарні* (поточний процес має випадкову природу).

По відношенню до ДЗ ЕМЗ бувають: *вузькосмугові* (ширина спектра менше або дорівнює ширині смуги пропускання ДЗ); *широкосмугові* (ширина спектра більша ширини смуги пропускання ДЗ), зовнішні (джерело знаходиться поза ДЗ); *внутрішні* (джерело знаходиться всередині ДЗ); *міжсистемні* (джерело знаходиться в системі, що не відноситься до ДЗ); *внутрисистемні* (джерело знаходиться усередині аналізованої системи, але поза ДЗ); *мультиплікаційні* (дія на ДЗ змінює комплексну структуру корисного сигналу за рахунок накладення її на комплексну огинаючу деякого випадкового процесу); *симетричні* (дія на ДЗ виявляється між двома затискачами джерела індустріальних завад або між фазовими проводами мережі живлення ДЗ); *несиметричні* (дія на ДЗ виявляється між затискачем джерела індустріальних завад і землі) [3].

Більшість безпроводових карток підтримують можливість роботи в режимі моніторингу, що дозволяє зберігати кількість даних, що передаються, у безпроводовій мережі навіть без встановлення з нею логічного зв'язку. У конкретний момент часу картка має можливість прослуховувати тільки один з каналів, однак більшість мережевих безпроводових аналізаторів підтримують можливість поетапного перемикання між каналами (channel hoping) для збору пакетів на всіх можливих каналах. Після виявлення безпроводової мережі зловмисник може сконцентрувати увагу на потрібному каналі і збирати всі пакети окремої мережі. Як і у випадку з несанкціонованим підключенням, зловмисник має можливість аналізувати пакети, перебуваючи на значній відстані від ТБД. Існує багато різноманітних мережевих аналізаторів пакетів для WLAN, наприклад, програми AirMagnet Laptop,

Wildpackets Aeropeak, CommView (для ОС Windows) і Ethereal, Kismet (для ОС Linux), а також додаткові драйвери [4]. Прослуховування поділяється на активне і пасивне.

Атака "людина посередині" (Man-in-the-Middle Attack), як і DDoS-атака, виконуються у безпроводових мережах набагато простіше, ніж у проводових. Зазвичай атаки "людина посередині" мають два різновиди: підслуховування і маніпуляція. При прослуховуванні, зловмисник прослуховує набір передач між різними хостами, при цьому комп'ютер зловмисника не повинен бути однією зі сторін в з'єднанні. Атаки маніпуляції використовують можливість прослуховування і нелегального захоплення потоку даних з метою зміни його вмісту. Для запобігання атак прослуховування, необхідно проводити шифрування даних на різних рівнях, бажано використовуючи SSH, SSL або IPSEC [8].

Однією з найбільш відомих уразливостей в безпроводових мережах для WEP (Wired Equivalent Privacy) є схема аутентифікації: кодування кожного пакета за допомогою потокового шифру RC4, які декодуються на ТБД. Використання WEP є проблематичним в плані забезпечення захисту і заспокоює лише знання факту, що WEP ключі є статистичними. В 2004 р. з'явилися так звані KoreK-атаки, що дозволяють атакуючому отримати ключ після перехоплення набагато меншого обсягу даних, ніж в оригінальному варіанті [15]. Оскільки WEP не забезпечує адекватного рівня безпеки, для захисту безпроводових мереж досить широко використовуються засоби побудови віртуальних приватних мереж, а також шифрування за алгоритмами WPA і 802.1X [4].

"Стрибаюча" атака або затискальна (jamming attack) є спеціальним видом DoS-атаки в безпроводових мережах. Затискання відбувається, коли випадкові радіочастоти створюють завади у функціонуванні безпроводової мережі. У деяких випадках затискання відбувається через присутність інших пристроїв, наприклад, безпроводового телефону. Навмисне затискання відбувається, коли зловмисник спочатку аналізує спектр мережі, а потім передає потужний сигнал, щоб створити заваду. Затискання мережі являє собою короткочасну атаку, спрямовану на те, щоб вивести мережу з ладу на деякий час [14].

Схема на рис. 1 ілюструє дерево атак для безпроводової мережі.

Імовірнісні характеристики. Розглянемо атаки на безпроводову мережу. Несанкціоноване прослуховування мережі і внесення змін в її роботу можна змоделювати за допомогою мережі Петрі-Маркова (рис. 2), де: s_1 – готові до роботи ТБД і клієнт; s_2 – зловмисник, готовий для атаки; t_1 – передача даних між ТБД і клієнтом, перехоплення даних; s_3 – дані отримані і вибраний вид атаки; t_2 – проведення атаки; s_4 – успішна атака.

Елементи матриці, що визначають логічні функції реагування мережі від початку передавання даних до проведення атаки, мають вигляд:

$v_{s_1t_2}$	t_1	t_2
s_1	1	0
s_2	1	0
s_3	$s_1t_1 \cap s_2t_1$	1
s_4	0	1

Елементи матриці

Застосовуючи пуассонівське наближення [16], отримаємо середній час t_a переміщення по мережі Петрі-Маркова із початкової позиції до кінцевого переходу та ймовірність цього переміщення:

$$P_a(t) = 1 - e^{-\frac{t_a}{\tau}}, \qquad (1)$$

де t_a — середній час переміщення атаки по всій мережі.

Залежність ймовірності реалізації атаки від часу для безпроводової мережі показана на рис. 3.

За час атаки передані дані будуть втрачені або будуть визнані сумнівними. В табл. 1 показана мінімальна кількість даних, яка буде втрачена під час атаки, за умови, що передаються тільки службові дані.

Якщо передаються також пакети з даними, то кількість втрачених даних може відрізнятися на кілька десятків або десятків тисяч порядків.

Якщо в комерційній безпроводовій мережі присутня система моніторингу і системний адміністратор відслідковує стан мережі в реальному часі, то можна визначити відношення ймовірностей атаки P_a і захисту $P_з$:

$$P_a + P_з = 1. \qquad (2)$$

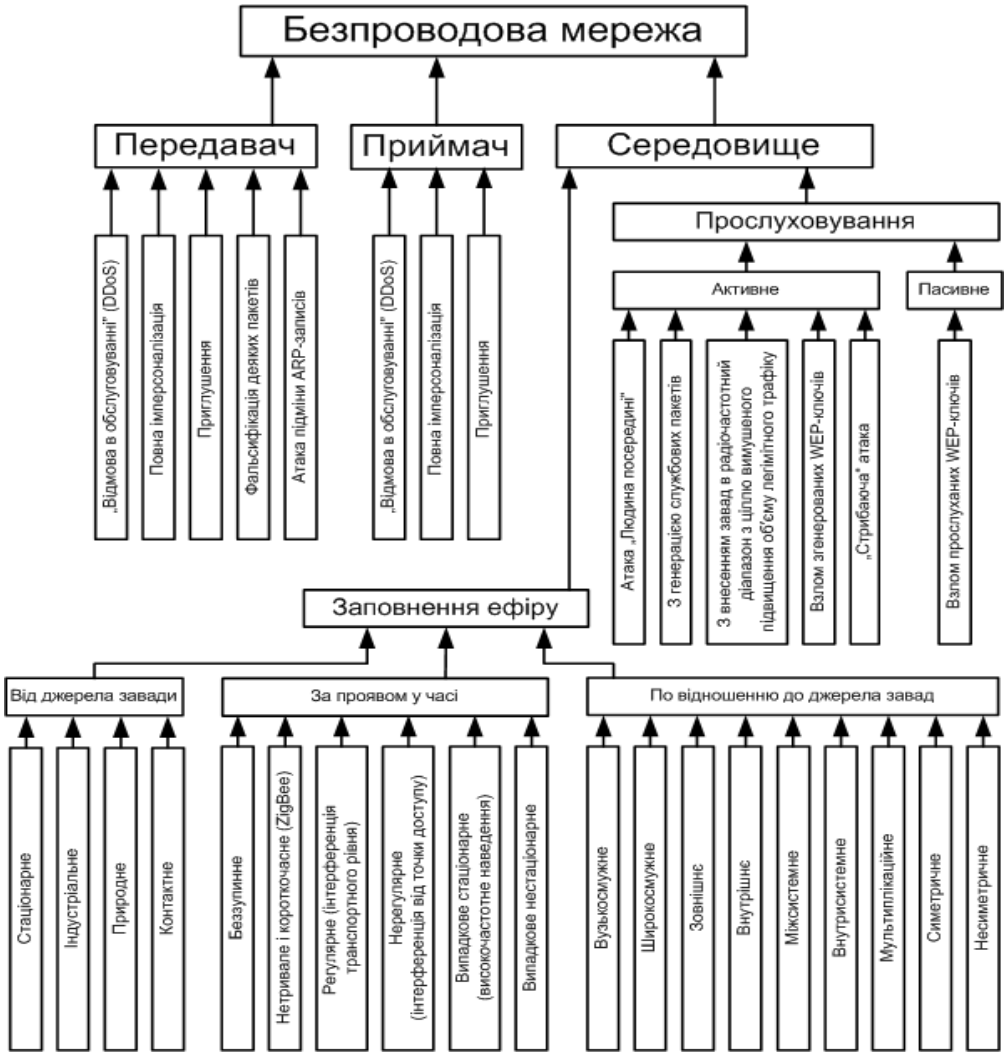

Рис. 1. Дерево атак на безпроводову мережу

Мінімальні втрати даних при різних атаках Табл. 1

Атака	Середній час переміщення, с	Кількість службових даних за час атаки*, кБ	
		802.11g	802.11n
DDoS-атака	11,15	1,5	3,1
Повна імперсоналізація	16,25	2,2	4,5
Сканування мережі і приглушення	48,80	6,6	13,6
Фальсифікація деяких пакетів	13,60	1,8	3,8
Підміна ARP-записів	15,50	2,1	4,3
Злом WEP-ключів	63,25	8,5	17,6

* Кількість службових даних отримана, виходячи з частоти передавання службових пакетів 10 Гц, довжини пакета (110 біт для 802.11g і 228 біт для 802.11n) і середнього часу атаки.

В [16] ймовірність визначається вартістю атаки і засобів захисту:

$$P_з = \frac{q_з \cdot C_з}{q_з \cdot C_з + q_a \cdot C_a}, \qquad (3)$$

де $C_з$ і C_a – вартість засобів захисту і атаки; $q_з$ і q_a – вагові коефіцієнти від часу реакції на атаку $t_{реак}$; t – середній час дій зловмисника у мережі:

$$q_з = q_a \frac{\tau}{t_{реак}}.$$

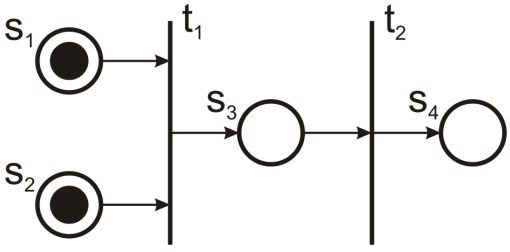

Рис. 2. Атака на безпроводову мережу

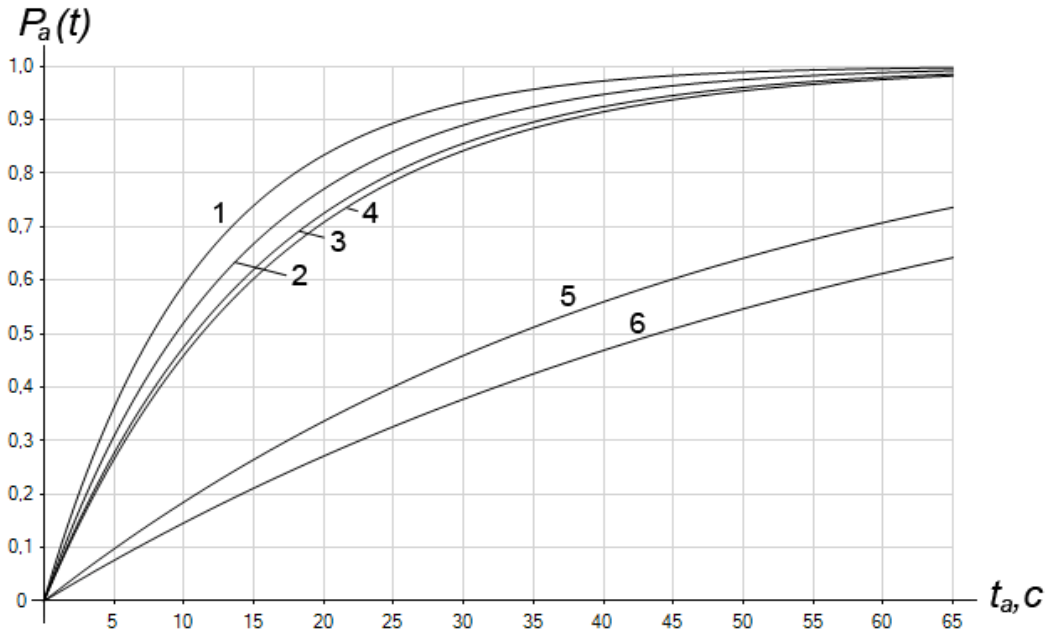

Рис. 3. Залежність ймовірності реалізації атаки від часу:
1 – DDoS-атака, 2 – фальсифікація деяких пакетів, 3 – підміна ARP-записів,
4 – повна імперсоналізація, 5 – сканування мережі і приглушення, 6 – злом WEP-ключів

За відношенням часу реакції до часу атаки побудовані криві (рис. 4). Виходячи з (2) і (3), при близькій вартості засобів захисту і атаки маємо:

$$P_з = \frac{\tau \cdot C_з}{\tau \cdot C_з + t_{реак} \cdot C_a} = \frac{\tau}{\tau + t_{реак}}\Bigg|_{C_з \approx C_a}. \qquad (4)$$

З (1), (2) і (4) маємо: $$t_{реак} < \tau(e^{\frac{t_a}{\tau}} - 1). \qquad (5)$$

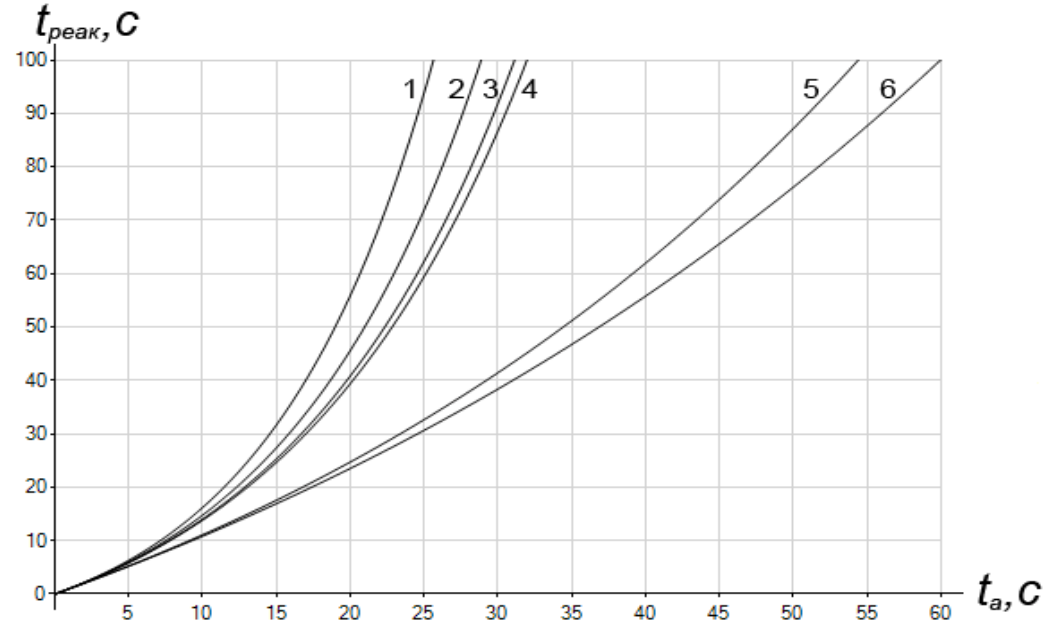

Рис. 4. Залежність ймовірності реалізації атаки від часу:
1 – DDoS-атака, 2 – фальсифікація деяких пакетів, 3 – підміна ARP-записів,
4 – повна імперсоналізація, 5 – сканування мережі і приглушення, 6 – злом WEP-ключів

З кривих видно, що при автоматичному виявлені атаки відношення має майже лінійну характеристику (час реакції не перевищує 5 с). Після розкладення (5) в ряд Тейлора $t_{реак} \le \sum_{0}^{\infty} \frac{t_a^{i+1}}{i!\tau^i}$ і виборі першого члену ряду $t_{реак} \le t_a$ отримуємо лінійне співвідношення.

При виявленні атаки адміністратором час реакції становить близько хвилини, тому у наближеному випадку можна брати перші чотири члени ряду (похибка наближення не перевищує 5%, як показано на рис. 5), отримуємо ступеневу функцію

$$t_{реак} \le \frac{1}{24\tau^3} t_a^4 + \frac{1}{6\tau^2} t_a^3 + \frac{1}{2\tau} t_a^2 + t_a .$$

При побудові системи забезпечення безпеки важливо визначити модель загроз, тобто вирішити, чому власне захист буде протистояти. Політика безпеки щодо бездротових мереж може бути представлена як у вигляді окремого документа, так і в складі інших нормативних документів або програмних засобів.

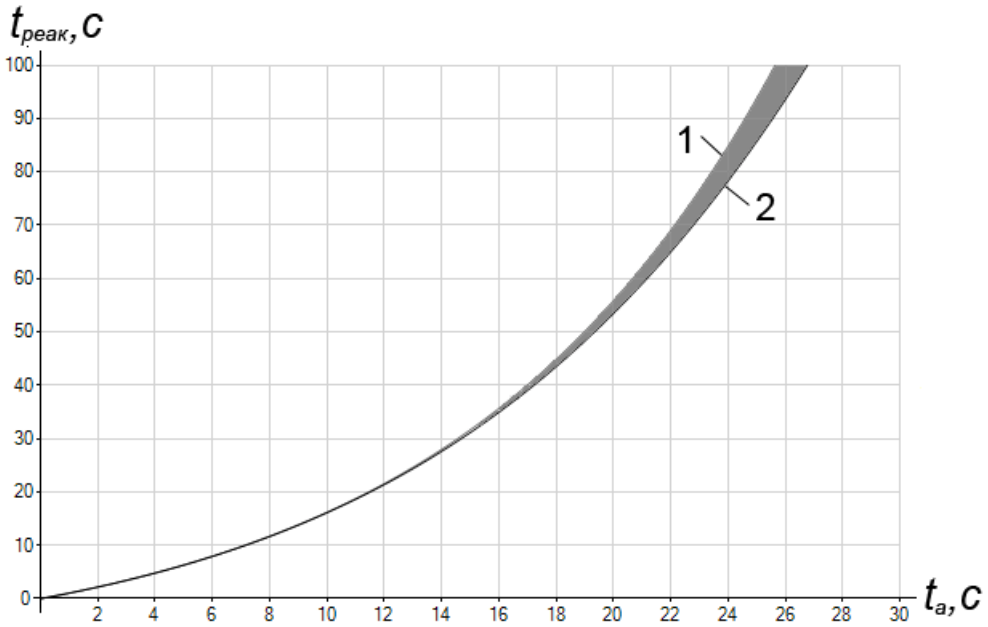

Рис. 5. Залежність ймовірності реалізації атаки від часу:
1 – показникова крива, 2 – наближена ступенева крива

При побудові системи забезпечення безпеки важливо визначити модель загроз, тобто вирішити, чому власне захист буде протистояти. Політика безпеки щодо бездротових мереж може бути представлена як у вигляді окремого документа, так і в складі інших нормативних документів або програмних засобів. Так у [2] існує п’ять критеріїв захищеності системи: конфіденційності, цілісності, доступності, спостережності та гарантій. Безпроводову мережу стандарту 802.11 можна віднести до четвертого рівня гарантії Г-4, за яким кожний з компонентів повинен мати мінімум повноважень, зберігати результати моніторингу і гарантувати безпечний запуск мережі.

Висновки. Поширеність безпроводових технологій у наш час ставить під загрозу захист інформації в корпоративних мережах, навіть коли користувач працює за стаціонарною робочою станцією, але в мережу входить один або декілька безпроводових сегментів. Традиційні засоби захисту безсилі проти принципово нових класів безпроводових загроз. При цьому ситуація ускладнюється тим, що необхідно захищати також віддалених користувачів.

Безпроводові мережі можна умовно розділити на домашні (Small Office/Home Office, SOHO), загальнодоступні і корпоративні. У кожному з цих випадків потрібно будувати окреме дерево атак, оскільки моделі загроз розрізняються для кожного з типів мереж. Разом з

використанням дерев атак для своєчасного виявлення нападу можна використовувати ТБД-приманки (AP Honeypots), спеціальне скануюче обладнання, а також SSL і SSH.

Для кращої безпеки потрібно дотримуватися основних правил при організації і налаштуванні безпроводової мережі: *віртуальні канали*, *802.1X, RADIUS-сервера, мережеві екрани*; *планове оновлення* програмного забезпечення і мікропрограм мережевого апаратного забезпечення; *по можливості не використовувати* в безпроводової мережі DHCP-сервери і стандартні засоби для зберігання даних.

З розглянутих атак на передавач видно, що при автоматичному виявлені атак за допомогою програмного забезпечення швидкість протидії повинна бути порівняна з швидкістю атаки. При оперативному виявлені атаки на пізніх стадіях у адміністратора є приблизно в півтора рази більше часу на протидію. Однак незважаючи на всі можливі засоби краще не відправляти секретні дані через безпроводові мережі.

Література

1. Степашкин М. В. Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак: дис. канд. тех. наук : 05.13.11, 05.13.19 / М. В. Степашкин. – М.: РГБ, 2007. – 196 с.

2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 2.5-004-99. – [Чинний від 1999-04-28]. – К.: Департ. спец. телеком. систем та захисту інформації, 1999.– №22. – 53 с. (СБУ).

3. Основи інформаційної безпеки / [Андрєєв В. І., Хорошко В. О., Чередниченко М. Є., Шелест В. С.] ; за ред. В. О. Хорошка. – [2-е вид.]. – К.: Вид. ДУІКТ, 2009. – 292 с.

4. Гордейчик С. Безопасность беспроводных LAN / Сергей Гордейчик // Беспроводные технологии. – 2004. – №2. – С. 51-52. – Режим доступу до журн.: http://www.wireless-e.ru/assets/files/pdf/2006_2_51.pdf

5. Филиппов М. Г. Вопросы обеспечения безопасности корпоративных беспроводных сетей стандарта 802.11. Специфика России / М. Г. Филиппов // Сети. – 2003. – №7. – Режим доступу до журн. : http://www.osp.ru/nets/2003/07/148575/

6. Деева Д. А. Методы обеспечение безопасности сетей стандарта 802.11 / Д. А. Деева // Матер. Всероссийской научно-практ. конф. с международным участием. Том 1. [«Актуальные проблемы современной науки и образования: Естественные науки»], (Уфа, февраль 2010) / Башкирский гос. ун-т. – С. 161-164. – Режим доступу : http://sibsu.ru/files/Natural_science.pdf

7. Соколов В. Ю. Підвищення захищеності Wi-Fi мереж: пошук триває / В. Ю. Соколов. // Наук.-виробн. журнал адміністрації зв'язку та радіочастот України «Зв'язок». – 2011. – №1 (93). – С. 53-57.

8. http://www.securitylab.ru/analytics/216360.php

9. http://www.digilex.ru/

10. Бандурян А. Анализ угроз для беспроводных сетей / Арсен Бандурян // Компьютерное обозрение. – 2010. – №12 (723). – С. 21-25. – Режим доступу до журн. : http://itcpublishing.com/salespdf/download/free/49

11. Червяков А. С. Угрозы и риски безопасности сетей стандарта Wi-Fi / А. С. Червяков // Матер. XVII Междунар. научно-методической конф-и. Том 2. [«Высокие интеллектуальные технологии и инновации в образовании и науке»], (С-Пб. гос. политех. ун-т., 11–12 февраля 2010 г.) – 2010. – С. 131-132. – Режим доступу: http://window.edu.ru/window_catalog/files/r70192/proceeding_v2.pdf

12. http://econference.ru/blog/corp_lnet_problems/

13. http://www.symantec.com/connect/articles/ip-spoofing-introduction

14. http://www.windowsecurity.com/articles/Wireless_Attacks_Primer.html

15. Петренко С. А. Безопасная беспроводная корпоративная сеть / С. А. Петренко, А. В. Беляев. // Wireless Ukraine. – 2009. – №2-3 (3). – С. 20-24. – Режим доступу до журн. : http://www.wireless.ua/templates/new_template/images/wu2.pdf

16. Радько Н. М., Скобелев И. О Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – Вид. РадиоСофт, 2010. – 232 с.

17. Иващук И. Ю. Модель и метод построения семейства профилей защиты для беспроводной сети: дис. канд. тех. наук : 05.13.19. – С-Пб., 2007. – 133 с.