УДК 004.772

К.т.н, доцент Орлова М.М., магістрант Кокотова М.О.

**Національний технічний університет України
«Київський політехнічний інститут»**

МОДЕЛЬ ЗАГРОЗ ІНФОРМАЦІЇ ДЛЯ КОРПОРАТИВНИХ БЕЗПРОВОДОВИХ МЕРЕЖ

Abstract

Mariia M.Orlova, assoc. prof., PhD; Mariia Kokotova, student
The model of information threats for corporative wireless netwoks

There is the mathematical model of information threats in a wireless communication corporative computer systems under the influence of deliberate attacks in the conditions of information struggle presented at the article.

Вступ

Розвиток концепцій вторгнень у ресурси корпоративних мереж, засобів і методів їх реалізації обумовлений стрімким розвитком інформаційно-комунікаційних систем (ІКС). Однією з найбільш вразливих ланок ІКС є WLAN (Wireless Local Area Network). Засоби захисту, які на сьогодні використовуються в корпоративних WLAN, не здатні повною мірою забезпечити їх захищеність при вторгненні порушників. Відповідно до цього, найбільш актуальними напрямками роботи з безпроводовими мережами є оцінка їх захищеності та впровадження таких механізмів захисту.

Постановка завдання

Під інформаційною безпекою в системах безпроводового зв’язку будемо розуміти захищеність інформації, що передається в WLAN, та самої WLAN від навмисних або ненавмисних дій штучного та природного характеру, які можуть завдати неприйнятного збитку власникам і користувачам інформації у WLAN.

Завданням цієї роботи є аналіз можливих загроз пошкодження інформації у корпоративній WLAN та побудова на його основі математичної моделі загроз для оцінки захищеності інформації, що передається у WLAN, відповідно до результатів, отриманих в [2, 3].

Розглядаються тільки навмисні атаки на інформацію фізичного і канального рівнів WLAN відповідно до моделі OSI.

Основна частина

В сучасних WLAN основні механізми захисту інформації реалізуються на вищих рівнях моделі взаємодії відкритих систем [4]. Це пов'язано зі швидким розвитком комп'ютерних технологій, мереж, Internet-сервісів та ресурсів. Але найбільш вразливими з точки зору інформаційної безпеки є перші два рівні WLAN: фізичний та канальний. Ресурсами в WLAN, на які направлені атаки порушника, є інформація.

Проведений аналіз виявив наступні найбільш поширені загрози для корпоративних WLAN: перехоплення даних, відмова в обслуговуванні, використання несанкціонованих точок доступу, проникнення в мережу незареєстрованих користувачів, введення хибної інформації, порушення системи захисту, клонування точок доступу, безпроводовий фішинг (несанкціоноване отримання персональних даних користувачів Internet), придушення радіоінтерфейсу WLAN.

Для відображення послідовності реалізації атак порушником, взаємозв'язків між етапами реалізації атак у відповідності до семантичної моделі загроз інформації в WLAN, побудуємо граф $G = (S, J)$.

Вершинами графа є стани, кожний з яких відповідає спробі реалізації порушником певної атаки на інформацію WLAN. Позначимо через N множину ідентифікаторів загроз інформації. Початковий стан системи, при якому відсутні загрози інформації корпоративної WLAN, позначимо через s_0. Кожний стан s_i ($i \in N$) відповідає спробі реалізації i-ї атаки. У випадку її успішності здійснюється перехід до наступного стану системи s_j ($j=i+1$). При штатному реагуванні системи захисту інформації (СЗІ) здійснюється перехід до стану s_{n+1}, тобто порушник зазнає невдачі при спробі подолати СЗІ. Стан s_n є кінцевим і відповідає збиткам, які нанесені ресурсам мережі при досягненні порушником кінцевої мети.

Дуги графа відображають напрями переходів між станами. Кожна дуга характеризується значенням ймовірності успішного переходу між станами системи. Пунктиром позначені дуги, які відповідають імовірному переходу зі стану s_i в стан s_{n+1} за умови неуспішного подолання порушником i-ї системи захисту.

Для відображення СЗІ та наочності процесу «атака-захист» в граф G включена множина псевдовершин Z, де кожна псевдовершина $z_i \in Z$ відображає засіб захисту від i-ї загрози, при реалізації атаки зі сторони порушника. Для захисту від i-ї загрози може використовуватись декілька засобів захисту z_i. Позначимо їх кількість через k та визначимо сукупність

засобів $z_{i_{,,}}$ які потенційно можуть бути використані для протидії реалізації порушником *i*-ї загрози (*i* = 1, 2, …, *k*), як множину *K*, при цьому *K* є підмножиною *Z*, тобто $K \subseteq Z$.

На *i*-у систему захисту може бути направлено декілька атак. Ймовірність подолання системи захисту в цьому випадку є сумою ймовірностей подолання кожної окремої системи захисту.

Для опису взаємних переходів порушника між етапами реалізації однієї атаки – досягнення успіху та реалізації іншої атаки, розпишемо відповідності J{s_i} для кожної з вершин $s_i \in S$ графа $G = (S, J)$:

$$J\{s_0\} = \{s_1, s_2, s_3\};$$

$$J\{s_1^{\langle 1\rangle}\} = \{s_9 \vee s_{10}\},\ J\{s_1^{\langle 2\rangle}\} = \{s_4, s_{10}\},\ J\{s_1^{\langle 3\rangle}\} = \{s_5, s_{10}\},\ J\{s_1^{\langle 4\rangle}\} = \{s_6^{\langle 1\rangle}, s_{10}\};$$

$$J\{s_2^{\langle 1\rangle}\} = \{s_6^{\langle 2\rangle}, s_{10}\},\ J\{s_2^{\langle 2\rangle}\} = \{s_9 \vee s_{10}\},\ J\{s_2^{\langle 3\rangle}\} = \{s_9 \vee s_{10}\};$$

$$J\{s_3^{\langle 1\rangle}\} = \{s_2^{\langle 3\rangle}, s_{10}\},\ J\{s_3^{\langle 2\rangle}\} = \{s_7, s_{10}\},\ J\{s_3^{\langle 3\rangle}\} = \{s_8, s_{10}\};$$

$$J\{s_4\} = J\{s_5\} = J\{s_6\} = J\{s_7\} = J\{s_8\} = \{s_9 \vee s_{10}\};$$

$$J\{s_9\} = J\{s_{10}\} = \phi.$$

Таким чином, представляючи кожну загрозу як стан s_i і відображаючи послідовність дій порушника як переходи між цими вершинами дугами графа *G*, отримаємо орієнтований граф, зображений на рис. 1.

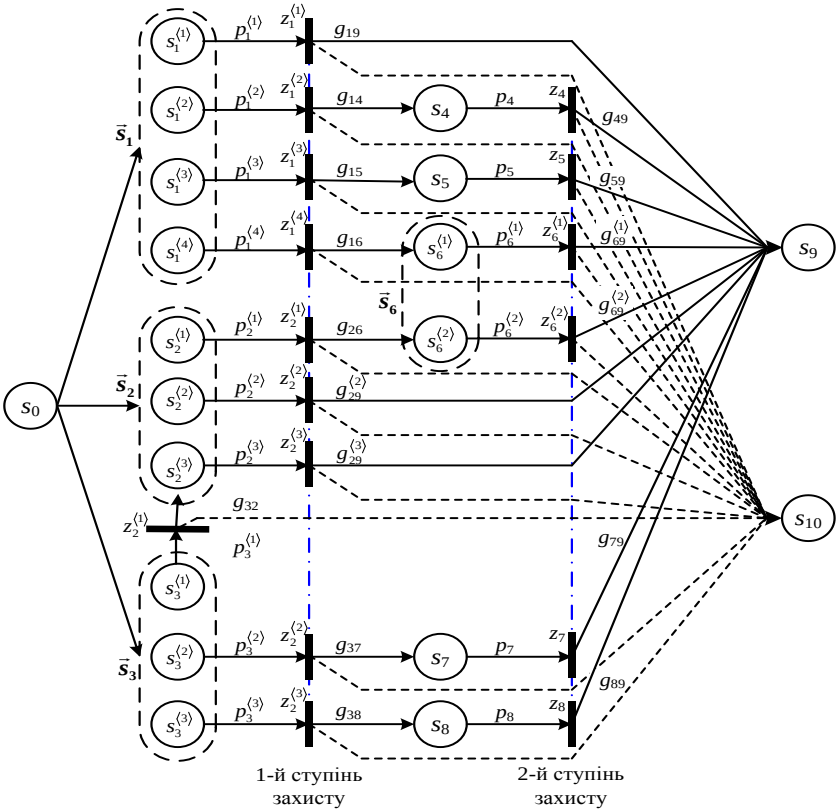

Рис. 1. Граф моделі загроз інформації в мережі при дії навмисних атак порушника

Вершини графа G відображають ймовірності: s_1 – перехоплення даних; s_2 – використання несанкціонованих точок доступу; s_3 – проникнення в мережу незареєстрованих користувачів; s_4 – введення хибної інформації; s_5 – блокування радіоінтерфейсу WLAN; s_6 – клонування точок доступу; s_7 – безпроводовий фішинг; s_8 – порушення системи захисту; s_9 –нанесення збитку ресурсам; s_{10} – невдача порушника по нанесенню збитків ресурсам.

Приведений граф моделі загроз відображає багатоступеневу систему захисту. Щоб досягти успіху – стану s_n – в нанесенні інформаційним ресурсам збитку, порушнику необхідно подолати всі ступені захисту.

Визначимо основні ймовірнісні характеристики, що описують модель. Ймовірність знаходження системи в j-му стані при спробі реалізації порушником цілі визначається наступним чином:

$$P_j = p_i p_{ij},$$

де P_j – ймовірність досягнення j-го стану, j – наступний стан порушника, $j \in N$; p_i – ймовірність того, що порушник досягнув i-го стану, p_{ij} – ймовірність переходу з i-го в j-й стан.

Відповідно до цього, ймовірність переходу із стану s_i в s_j визначається як:

$$p_{ij} = \rho_i g_{ij}^k,$$

де ρ_i – ймовірність реалізації порушником i-ої (поточної) атаки для переходу в j-й (наступний) стан; g_{ij}^k – ймовірність подолання i-го захисту при спробі досягнення порушником мети; k – кількість засобів захисту для i-ї загрози, $k \in K$.

Успіх подолання одного із засобів захисту визначається ймовірністю g_{ij}^k. Вона, в свою чергу, залежить від того, як ефективно функціонує система захисту, чи дійсно перекриває вразливості WLAN, і від того, на скільки технічно оснащеним і кваліфікованим є порушник. Така залежність визначається наступною формулою:

$$g_{ij}^k = \left(1 - e^{-q\omega}\right) \prod_{k \in K} \left(1 - r_{ik} \beta_{ik}\right),$$

де r_{ik} – ймовірність успішного функціонування i-го засобу захисту щодо протидії реалізації порушником атаки для завдання збитків; $q(0\ldots1)$ – коефіцієнт технічної оснащеності порушника; $\omega(0\ldots1)$ – рівень кваліфікації порушника при реалізації атаки; $\beta_{ik} = \{0, 1\}$, $\beta_{ik} = 1$, якщо i-й засіб захисту використовується для усунення i-ї загрози, $\beta_{ik}=0$ – в іншому випадку.

Момент часу, при якому порушник ще не здійснив жодної атаки – початковий момент, і на графі G представлений як стан s_0. Початковий момент часу характеризується такими значеннями:

$$P_0 = 1;\ P_n = 0;\ P_{n+1} = 0;\ \beta_{ik} = 0, \forall i, k.$$

Сума ймовірностей переходу в стани s_n і s_{n+1} є ймовірністю повної групи подій, і дорівнює одиниці: $p_n + p_{n+1} = 1$. Тоді ймовірність захисту *k*-ю СЗІ від *i*-ої загрози (перехід в стан «невдача противника»):

$$p_{i,n+1} = 1 - g_{ij}\,.$$

Ефективність функціонування СЗІ WLAN може бути визначена за допомогою наступних параметрів.

1. Середнє значення інформаційних втрат в WLAN від реалізації порушником атак:

$$C^{\text{p}} = \sum_{\substack{j \in N, \\ j \neq 0}} P_j c_j \,,$$

$$c_i = c_{i1} + c_{i2} + c_{i3} + c_{i4} + c_{i5}\,,$$

де c_{i1}, c_{i2}, c_{i3} – обсяг втрат WLAN від порушення конфіденційності інформації, цілісності, доступності; c_{i4} – обсяг втрат від невиконання завдань; c_{i5} – ціна відновлення WLAN при реалізації порушником *i*-ї атаки.

2. Ймовірність реалізації порушником всіх цілей:

$$P^{\text{p}} = \sum_{j=1}^{n} P_j p_{jn}\,.$$

3. Ймовірність успішної протидії СЗІ діям порушника:

$$P^{\text{з}} = 1 - \sum_{i=1}^{n} P_j p_{jn}\,.$$

Перший показник дає можливість оцінити ризик нанесення збитку системі. Параметри обсягу втрат визначають збиток, що отримує власник інформації при реалізації інформаційних атак. Другий і третій показники оцінюють порушника і захищеність системи відповідно. Для відображення повної картини функціонування системи захисту WLAN необхідно розглядати перший та третій показники ефективності системи захисту.

Висновки

Представлена модель загроз пошкодження інформації корпоративної WLAN об’єднує всі типи атак, які може реалізувати порушник для впливу на канальний та фізичний рівні WLAN. Кожній загрозі відповідає певний механізм захисту, що відображає множина псевдовершин побудованого графа. Це дозволяє більш наочно відобразити процес «атака-захист». Відповідно враховуються показники можливості реалізації атак порушником і подолання системи захисту.

Розроблена модель дозволяє виділити та оцінити атаки порушників, що створюють відповідні загрози та оцінити захищеність WLAN. ЇЇ

використання доцільно на етапі проектування і побудови систем захисту інформації для корпоративних WLAN.

За допомогою розрахованих на основі моделі показників вдалося проаналізувати захищеність різних топологій безпроводових мереж, виявити їх слабкі місця, встановити додаткові механізми захисту в гілках, які є менш захищеними та уникнути надлишковості, яка може бути створена системою захисту там, де ризики і втрати є прийнятними. Це дозволяє знизити вартість системи захисту корпоративної WLAN, зберегти її продуктивність та скоротити час на побудову.

Модель загроз є універсальною і може бути використана як для опису конкретної технології WLAN, так і для опису ІКС, що включає радіоінтерфейс.

Література

1. *Данільян О.Г., Дзьобань О.П., Панов М.І.* Національна безпека України. Сутність, структура та напрямки реалізації // Фоліо, 2002. – 150 с.
2. *Кокотов О.В., Шевченко А.С.* Загрози інформаційній безпеці систем безпроводового зв'язку в умовах інформаційної боротьби відповідно до критеріїв захищеності інформації // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2010. – № 1. – С. 35 – 40.
3. *Кокотов О.В., Шевченко А.С.* Модель загроз інформації в системах безпроводового зв'язку в умовах ведення інформаційної війни // V науково-практичний семінар Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення – К.: ВІТІ НТУУ„КПІ". – 2009. – С. 140.
4. *Максименко В.Н., Афанасьев В.В., Волков Н.В.* Защита информации в сетях сотовой подвижной связи // Горячая линия – Телеком, 2007. – 360 с.