УДК 511:003.26.09

ОЦЕНКА ВЫЧИСЛИТЕЛЬНЫХ ЗАТРАТ ρ-МЕТОДА ПОЛЛАРДА В ЗАВИСИМОСТИ ОТ ВЫБОРА ОТОБРАЖЕНИЯ И НАЧАЛЬНОГО ПРИБЛИЖЕНИЯ ДЛЯ МАЛЫХ ФАКТОРИЗУЕМЫХ ЧИСЕЛ

Степан Винничук, Евгений Максименко, Виталий Мисько

Для ряда задач защиты информации криптостойкость используемых алгоритмов связана с решением вычислительной задачи разложения на множители (факторизации) многоразрядных чисел. Алгоритмы современных методов факторизации могут использовать, как составляющую часть, известные алгоритмы. Поэтому исследование свойств известных методов и разработка способов ускорения их работы представляется актуальной задачей. Для ρ-метода Полларда факторизации известны общие оценки для числа итераций, но не представлены результаты исследований по влиянию на него начального приближения. Для оценки такого влияния предложено определять среднее число итераций для ρ-метода Полларда на примере $2*10^7$ вариантов чисел, не превышающих 2^{31}, вида $N=p\cdot q$, где p и q простые. При определении средних значений числа итераций рассчитывалось суммарное число итераций по всем исследуемым вариантам чисел N и делилось на количество этих вариантов. Для обеспечения разложения чисел на множители каждый раз, когда итерационный процесс зацикливался, константа c в полиноме увеличивалась на единицу. Проведены исследования по оценке среднего значения числа итераций в зависимости от выбора константы c в полиноме, реализующем итерационный процесс вида $x_{k+1} = (x_k^2 - c) \bmod N$, а также от выбора начального приближения. Определено, что для исследуемых вариантов чисел среднее значение количества итераций ниже известных оценок, а за счет выбора начального приближения оно может быть уменьшено более чем на треть.

Ключевые слова: *факторизация, ρ-метод Полларда, начальное приближение, отображение в кольце вычетов, вычислительная сложность.*

Вступление. При решении задач защиты информации достаточно широкое распространение получил асимметричный криптоалгоритм RSA. Его криптографическая стойкость основывается на трудоемкости вычислительной задачи разложения на множители многоразрядных чисел вида N=p·q, где p и q простые. Алгоритм RSA является наиболее распространенным в зарубежных криптосистемах и является стандартом де-факто для многих криптографических приложений [1]. Многочисленными исследованиями по методам криптографического анализа RSA алгоритма [2-5] показано, что известные примеры компрометации RSA алгоритма относятся только к определенным его практическим реализациям и в общем случае не являются эффективней задачи факторизации.

В настоящее время разработано ряд методов факторизации и основные из них представлены в работе [6]. Алгоритмы современных методов факторизации могут использовать, как составляющую часть, другие известные алгоритмы. Поэтому исследование свойств известных методов и разработка способов ускорения их работы представляется **актуальной** задачей.

Настоящая статья посвящена **исследованию свойств** одного из известных методов факторизации – ρ-метода Полларда. В работе рассмотрены вопросы **сходимости итерационного процесса,** проанализирована **эффективность метода в зависимости от выбора константы в полиноме**, реализующем итерационный процесс вида $x_{k+1} = (x_k^2 - c) \bmod N$, а также от выбора **начального приближения**.

Постановка задачи. Алгоритм ρ-метода факторизации Полларда. ρ-метод Полларда был впервые описан в работе [8]. Известны варианты усовершенствования метода (алгоритмы Флойда и Брента), связанные с уменьшением числа хранимых данных, а также со способом выбора пары итерационных значений x_j и x_k, для которых определяется НОД($(x_j - x_k, N)$). С его помощью было разложено на множители число Ферма $F8=2^{256}+1$ [9].

ρ-метод Полларда изложен во многих книгах и статьях. Поэтому здесь приводится его конспективное описание, в основном соответствующее приведенному в работе [10].

На входе задано натуральное число N, которое следует разложить на множители.

1 шаг. В кольце Z/(N) выбрать отображение f (обычно f(x) – многочлен степени большей или равной 2).

2 шаг. Случайно выбрать $x_0 \in Z/(N)$ и вычислять члены рекуррентной последовательности x_1, x_2, x_3, … по правилу

$$x_{k+1}=f(x_k)(\bmod N). \quad (1)$$

3 шаг. Для некоторых номеров j, k проверять условие

$$1<НОД(x_j - x_k, N)<N, \quad (2)$$

до тех пор, пока не будет найден делитель числа N, или пока не закончится время, отведенное для работы алгоритма, либо не будет определено, что НОД($x_j - x_k$, N)=0.

Конец алгоритма.

Выбор номеров j, k на третьем шаге алгоритма может быть реализован одним из следующих способов [7, 9, 10]:

1. Для каждого j перебирают все k, k<j.
2. Рассматривают пары k и 2k, т. е. проверяют условие 1<НОД($x_{2k} - x_k$, N)<N (вариант Флойда).
3. При выбранном k значение j заключено в пределах k<j<=2k (вариант Брента), где каждое новое значение k удваивается, например, k=2, k=4, k=8, k=16 и т.д).

При проведении численных экспериментов использовался третий способ.

Вычислительная сложность ρ-метода Полларда оценивается величиной порядка не выше $O(N^{1/4})$, где N – разлагаемое на множители многоразрядное число или $O(p^{1/2})$, где p – меньший из делителей N [7]. При этом существуют две причины, по которым такой алгоритм может оказаться не таким эффективным:

1. Эвристический анализ времени его работы нестрогий и цикл значений по модулю p может оказаться намного длиннее чем $\sqrt{p}$ (в этом случае алгоритм работает правильно, но намного медленнее).
2. Среди делителей числа N может оказаться тривиальный вариант, равный N.

В первом случае согласно результатам исследований, приведенных в [10], утверждается, что среднее значение количества итераций m(p), необходимое алгоритму для нахождения множителя p, примерно равно $2\sqrt{p}$ и не превышает $12\sqrt{p}$ для $p<10^6$. Но возможны редкие случаи, когда результат не удается найти (вторая причина). Тогда предлагается поменять функцию f(x), где в случае $f(x)=x^2+c$ установить другое значение c, не совпадающее с 0, 1 и –2 [10]. Аналогичная информация содержится и в работе [7], где c≠0 и c≠–2. Следовательно, в таких случаях следует уточнить п. 3 приведенного алгоритма относительно времени окончания его работы.

Естественно, что возврат к п. 1 или п. 2 алгоритма в принципе может быть многократным, хотя в работе [10] и предполагается, что при значениях c, не совпадающих с 0, 1 и –2 и при подходящих начальных условиях случаев зацикливания быть не должно. Поэтому первой поставленной задачей было определение числа возвратов к п. 1 для множества вариантов N, которые выбирались как произведение простых чисел p и q.

Численные эксперименты по определению количества изменений отображения. В качестве базового отображения f: Z/(N)→Z/(N) выбиралась функция $f(x) = x^2 - c$. Числа N определялись как произведение двух простых чисел p и q, где p=mp[lp], q=mp[lq], mp[*] – массив простых чисел (mp[0]=0, mp[1]=1, mp[2]=2, mp[3]=3, mp[4]=5, mp[5]=7 и т.д.), а параметры циклов lp и lq находились в диапазонах lp – от 120 до 4000 (с шагом 1); lq – от lp+1 до 9800-1.25·lp (с шагом 1). Общее число вариантов чисел N равно 20045475.

Для случая функций вида $f(x) = x^2 - c$ (0<c<=20) при условии, что множители числа N не найдены, новое отображение выбиралось $f(x) = x^2 - c - 1$. Если и в этом случае множители не найдены, то новой функцией была $f(x) = x^2 - c - 2$ и т.д. Каждый раз при этом начальное приближение равнялось последнему из значений x_j, найденных при предыдущем отображении. В качестве первичного начального приближения для отображения $f(x) = x^2 - c$ (0<c<=20) и всех вариантов чисел N принималось $x_{0,1}$=120.

Обозначим:

v_0 – число вариантов значений N из общего их числа 20045475, для которых N удалось разложить на множители без изменения отображения;

v_k – число вариантов значений N, для которых N удалось разложить на множители за счет изменения отображения k раз;

i00 – среднее число итераций ρ-метода Полларда для общего количества 20045475 вариантов чисел N.

Среднее число итераций i00 и значения $v_0 \div v_4$ для отображений вида $f(x) = x^2 - c$, при 0<c<=20 определялись на основании численных экспериментов. Для определения средних значений числа итераций i00 рассчитывалось суммарное число итераций по всем исследуемым вариантам чисел N и делилось на 20045475 их вариантов. Полученные результаты приведены в табл. 1.

Из полученных результатов расчетов следует, что в среднем множитель числа N определяется при использовании только исходного отображения – функции $f(x) = x^2 - c$ для 99,84% вариантов N. Наилучшим (по числу итераций) оказалось значение c=4. При c=2 оказалось, что множитель N определяется по функции $f(x) = x^2 - 2$ для 99,71% вариантов N, хотя среднее число итераций увеличивается более чем в четыре раза. Аналогичные результаты для c=2 получались и при других

исследованиях и поэтому в дальнейшем вариант отображения $f(x) = x^2 - 2$ не анализировался.

Таблица 1

Результаты расчетов для функций вида $f(x) = x^2 - c$ при начальном приближении $x_{0,1}=120$

c	i00	v_0	v_1	v_2	v_3	v_4
1	169.67	20014374	30596	481	24	0
2	772.59	19987402	57913	157	3	0
3	168.87	20012930	32112	428	5	0
4	164.83	20013622	31481	371	1	0
5	170.42	20013444	31556	464	11	0
6	166.58	20013777	30017	1672	8	1
Среднее для c=7÷20	169,53	20013974	30969	526	7	0

Неожиданными оказались результаты о количестве повторных обращений к смене отображения. В среднем это характерно для 0,157% вариантов чисел N. При этом возможны как трехкратные, так даже и четырехкратные возвраты. Поэтому высказанное в [10] предположение о том, что для нового отображения при иных значениях c, не совпадающих с 0, 1 и –2, случаев зацикливания быть не должно, при предложенном варианте выбора начального приближения не подтвердилось.

Важным при этом оказывается тот факт, что при примерно одинаковом количестве вариантов первого обращения к формированию нового отображения число вариантов чисел N для двух разных c (не только соседних), для которых такое обращение имеет место, существенно уменьшается (в среднем примерно в 80 раз).

Также анализировались варианты, в которых ρ-методом Полларда определялось не p а q при p<q. Как оказалось, значение q как НОД($x_j - x_k$, N) определялось в случаях, когда длина цикла для чисел $(x_j - x_k) \bmod q$ меньшая чем для $(x_j - x_k) \bmod p$.

Влияние начального приближения. На основании численных экспериментов было установлено, что аналогичные приведенным в табл. 1 результаты получаются и при других начальных приближениях вида $x_{0,1} = const$. Определим начальное приближение по правилу $x_{0,2} = \left\lceil \sqrt{N} \right\rceil + 1$ и проведем те же вычисления. Результаты расчетов приведены в табл. 2.

Полученные результаты показывают, что начальное приближение $x_{0,2} = \left\lceil \sqrt{N} \right\rceil + 1$ несущественно влияет на результаты расчетов, хотя при этом несколько увеличилось среднее значение числа обращений к смене отображения разной кратности.

Таблица 2

Результаты расчетов для функций вида $f(x) = x^2 - c$ при начальном приближении $x_{0,2} = \left\lceil \sqrt{N} \right\rceil + 1$

c	i00	v_0	v_1	v_2	v_3	v_4
1	169.67	20011944	30662	2661	208	0
3	168.29	20012015	31918	1528	14	0
4	164.52	20010959	33952	561	1	2
5	168.12	20012003	31744	1714	14	0
6	166.47	20010762	33078	1621	14	0
Среднее для c=7÷20	169.01	20011725	32503	1241	7	0

Известно [10, 11], что при факторизации чисел методом Ферма существенное ускорение алгоритма достигается при прореживании пробных значений x в соотношении $x^2 = N + y^2$.

По аналогии с [11] исследовался вариант начального приближения вида $x_{0,3} = \left\lceil \sqrt{N} \right\rceil + m$, где m наименьшее положительное число такое, что $x_{0,3}$ является решением уравнения

$$(x^2 = N + y^2) \bmod B, \qquad (3)$$

а B – база (основание модуля). В исследованиях использовалось значение B=60.

Полученные результаты приведены в табл. 3.

Таблица 3

Результаты расчетов для функций вида $f(x) = x^2 - c$ при начальном приближении $x_{0,3} = \left\lceil \sqrt{N} \right\rceil + m$

c	i00	v_0	v_1	v_2	v_3	v_4
1	106.094	20022373	22979	96	27	0
3	102.580	20022557	22812	103	3	0
4	98.7063	20023343	22036	93	3	0
5	105.204	20021899	23484	86	5	1
6	98.7884	20023842	21480	149	4	0
Среднее для c=7÷20	104.701	20022458	22915	99	3	0

Приведенные в табл. 3 результаты расчетов при их сравнении с данными табл. 2 для исследуемых вариантов чисел N позволяют утверждать, что при использовании начального приближения $x_{0,3}$ значительно (в среднем более чем на 38% и более чем на треть для каждого из c=3÷20 в отдельности) уменьшается среднее число итераций в методе Полларда, где среднее вычислялось как по всем вариантам чисел N=p·q, так и по значениям c=3÷20. В этом случае уменьшилось примерно на треть и число обращений к переопределению отображения f.

В работе [10] приводится предельная оценка по количеству итераций метода Полларда, где их число ограничивается сверху величиной $12\sqrt{p}$.

Для случая начального приближения $x_{0,3}=\left[\sqrt{N}\right]+m$ при численных экспериментах оценивалось соотношение z_N числа итераций к $p^{1/2}$. Как оказалось, максимальное такое соотношение $z_{N,max}$ для анализируемых вариантов чисел N превосходило $12\sqrt{p}$. В случае c=3÷20 значение $Z_{N,max}$ находилось в пределах от 25.10 (c=6, p=6673, q=17027, среднее значение для всех N – 0.91219) до 55.47 (c=15, p=5647, q=14143, среднее значение для всех N – 0.967807), при среднем значении $z_{N,ср}$=0.97 для c=3÷20. Полученное несоответствие в оценках связано как с выбором начального приближения, так и способом выбора номеров итерационных значений для сравнения, а также изменением отображения f: Z/(N)→Z/(N) вида $f(x)=x^2-c$, для случая, когда для анализируемых номеров j, k равными оказывались итерационные значения $x_j=x_k$. В таком случае равными оказываются длины циклов (равны 9) для чисел $(x_j-x_k)\bmod q$ и $(x_j-x_k)\bmod p$. Данные по такому варианту приведены в табл. 4 для p=653 q=673 при c=4 и $x_0=x_{0,1}=120$.

Таблица 4

Пример варианта зацикливания итерационного процесса

Номер итерации i	x_i	$x_i \bmod p$ (p=653)	$x_i \bmod q$ (q=673)
11	254913	243	519
12	311756	275	157
13	157899	526	417
14	138889	453	251
15	102031	163	408
16	183285	445	229
17	380861	162	616
18	7956	120	553
19	14396	30	263
20	254913	243	519

Выводы. ρ-метод Полларда является эффективным средством факторизации чисел при наличии малых делителей и используется как составная часть других известных алгоритмов. Для данного метода проводились многочисленные исследования и получены оценки его эффективности и условия сходимости. В то же время отсутствуют рекомендации по выбору начального приближения. Вычислительные затраты (число итераций метода) оцениваются по длине цикла для $(x_j) \bmod p$. Не конкретизированы и способы обеспечения сходимости метода. На основании проведенных численных экспериментов установлено следующее.

1. Для обеспечения сходимости метода Полларда может потребоваться многократное изменение отображения f: Z/(N)→Z/(N) вида $f(x)=x^2-c$.

2. При начальном приближении $x_{0,3}=\left[\sqrt{N}\right]+m$ для всех исследуемых 20045475 вариантов чисел N=p·q, где p и q простые и при базовом отображении f: Z/(N)→Z/(N) вида $f(x)=x^2-c$ при c=3÷20 снижается оценка среднего числа итераций для ρ-метода Полларда с $2\sqrt{p}$ до $\sqrt{p}$, число итераций для каждого из c=3÷20 число итераций уменьшается более чем на треть и почти на треть уменьшалось число обращений к переопределению отображения вида $f(x)=x^2-c$.

ЛИТЕРАТУРА

[1]. Саломаа А. Криптография с открытым ключом: пер. с англ. / А. Саломаа. – М.: Мир, 1996. – 318 с.

[2]. Song Y. Yan. Cryptanalytic attacks on RSA / Song Y. Yan. – Springer Science and Business Media, Inc. 2008. – P. 255.

[3]. Ростовцев А.Г. Теоретическая криптографія / А.Г. Ростовцев, Е.Б. Маховенко. – СПб: АНО НПО «Профессионал», 2004. – 480 с.

[4]. Горбенко И.Д. Анализ каналов уязвимости системы RSA / И.Д. Горбенко, В.И. Долгов, А.В. Потий, В.Н. Федорченко // Безопасность информации. – 1995. – № 2. – С.22 – 26.

[5]. Daniel R.L. Brown. Breaking RSA May Be As Difficult As Factoring [Электронный ресурс]. – Режим доступа: http://www.pgpru.com/novosti/2005/1026vzlomrsabezfaktorizaciirealennoneeffektiven. – Название с экрана.

[6]. Василенко О.Н. Теоретико–числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.

[7]. Кормен Т. Алгоритмы: построение и анализ / [Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К.]. – [2-е изд.]. – М.: Вильямс, 2011. – 1296 с.

[8]. Brent R.P. An improved Monte Carlo factorization algorithm / R.P. Brent // BIT. – 1980. – V. 20. – Pp. 176-184.

[9]. Pollard J.M. A Monte Carlo method for factorization / J.M. Pollard // BIT. – 1975. – V. 15. – Pp. 331 – 334.

[10]. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы / Д. Кнут. – М.: Вильямс, 2000. – 788 с.

[11]. Винничук С.Д. Алгоритм Ферма факторизации чисел вида N=pq методом прореживания / С.Д. Винничук, А.В. Жилин, В.Н. Мисько // Электронное моделирование, 2014. – Т. 36, № 2. – С. 3-14.

REFERENCES

[1]. Salomaa A. (1995), «Public-Key Cryptography: translation from english», M., Myr, 318 p.

[2]. Song Y. (2008), «Cryptanalytic attacks on RSA», Springer Science and Business Media, 255 p.

[3]. Rostovtsev A., Makhovenko E. (2004), «Theoretical kriptografiya», SPb: ANO NPO «Professyonal», 480 p.

[4]. Horbenko Y., Dolhov Y., Potyy A., V. Fedorchenko (1995), «Channel analysis system vulnerabilities RSA», Security of information, pp. 22-26.

[5]. Daniel R. L. Brown. Breaking RSA May Be As Difficult As Factoring. http://www.pgpru.com/novosti/2005/1026vzlomrsabezfaktorizaciirealennoneeffektiven.

[6]. Vasylenko O. (2003), «Number-theoretic algorithms in cryptography», M.: MTsNMO, 328 p.

[7]. Kormen T., Leyzerson Ch., Ryverst R., Shtayn K. (2011), «Algorithms: construction and analysis», M.: Vyl'yams, 1296 p.

[8]. Brent R. (1980), «An improved Monte Carlo factorization algorithm», BIT, V. 20, pp. 176-184.

[9]. Pollard J. (1975), «A Monte Carlo method for factorization», BIT, V. 15, pp. 331-334.

[10]. Knuth D. (2000), «The Art of Computer Programming», Volume. 2. Seminumerical algorithms, M.: Vyl'yams, 788 p.

[11]. Vynnychuk S., Zhylyn A., Mys'ko V. (2014), «Fermat's factorization Algorithm for numbers of the form N = pq by decimation. Electronic simulation», V. 36, № 2, pp. 3-14.

ОЦІНКА ОБЧИСЛЮВАЛЬНИХ ЗАТРАТ ρ-МЕТОДУ ПОЛАРДА В ЗАЛЕЖНОСТІ ВІД ВИБОРУ ВІДОБРАЖЕННЯ ТА ПОЧАТКОВОГО НАБЛИЖЕННЯ ДЛЯ МАЛИХ ФАКТОРИЗОВАНИХ ЧИСЕЛ

Для ряду задач захисту інформації криптостійкість використовуваних алгоритмів пов'язана з вирішенням обчислювальної задачі розкладання на множники (факторизації) багаторозрядних чисел. Алгоритми сучасних методів факторизації можуть використовувати, як складову, інші відомі алгоритми. Тому дослідження властивостей відомих методів та розробка способів прискорення їх роботи є актуальною задачею. Для ρ-методу Полларда факторизації відомі загальні оцінки для числа ітерацій, але не представлені результати досліджень щодо впливу на нього початкового наближення. Для оцінки такого впливу запропоновано визначати середнє число ітерацій для ρ-метода Полларда на прикладі $2*10^7$ варіантів чисел, що не перевищують 2^{31}, виду $N=p\cdot q$, де p и q прості. При визначенні середніх значень числа ітерацій розраховувалось сумарне число ітерацій для всіх досліджуваних варіантів чисел N, яке ділилось на число цих варіантів. Для забезпечення розкладання чисел на множники кожен раз, коли ітераційний процес зациклювався, константа c в поліномі, що реалізує ітераційний процес $x_{k+1}=(x_k^2-c) \bmod N$, збільшувалась на одиницю. Проведені дослідження з оцінки середнього значення числа ітерацій в залежності від вибору константи c в поліномі, а також від вибору початкового наближення. Визначено, що для досліджуваних варіантів чисел середнє значення числа ітерацій менше ніж відомі оцінки, а за рахунок вибору початкового наближення воно може бути зменшене більш ніж на третину.

Ключові слова: факторизація, ρ-метод Полларда, початкове наближення, відображення в кільці відрахувань, обчислювальна складність.

INEQUALITY OF COMPUTATIONAL EFFORT OF POLLARD P-METHOD ACCORDING TO DISPALY SELECTION AND INITIAL ESTIMATE FOR SMALL-SCALE FACTORIZABLE AMOUNTS

For a range of information security tasks the cryptostrength of algorithms applied is linked to solving a computational problem of multi-digit numbers factorization. Algorithms of modern factorization methods can use existing algorithms as integral part. That is why a research of existing methods and development of the way to accelerate their work is considered to be a highly topical problem. For Pollard ρ factorization method general evaluation of iterations number is known, but the results of initial approximation influence study have not been presented. To evaluate such influence it is suggested to define the average number of iterations for Pollard ρ factorization method in the context of numbers options of $2*10^7$ not exceeding 2^{31}, of the N=p*q type, where p and q are prime factors. While defining the average iterations number the total iterations count for all options of N under study was calculated and divided by the number of these options. To provide factoring constant c in the polynomial was increased by one whenever iteration process ran into a cyclic path. Studies are conducted to evaluate the average iterations number depending on the choice of constant c in the polynomial, representing iteration process $x_{k+1}=(x_k^2-c) \bmod N$, as well as on initial estimate. It has been defined that for the number options under study the average iterations number is lower than existing evaluations, and it can be decreased by one third, due to the initial estimate.

Keywords: factorization, Pollard ρ factorization method, initial estimate, presentation in the residue ring, computational complexity.

Винничук Степан Дмитрович, доктор технічних наук, виконуючий обов'язки завідувача відділом №8, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.
E-mail: vynnychuk@i.ua

Винничук Степан Дмитриевич, доктор технических наук, исполняющий обязанности заведующего отделом №8, Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины.

Vynnychuk Stepan, doctor of technical sciences, acting head of department, Pukhov Institute for Modelling in Energy Engineering, National Academy of Sciences of Ukraine.

Максименко Євген Васильович, аспірант Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.
E-mail: iszzi@i.ua
Максименко Евгений Васильевич, аспирант Института проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины.

Maksymenko Evhenyy, postgraduate student Pukhov Institute for Modelling in Energy Engineering, National Academy of Sciences of Ukraine.

Віталій Миколайович Міський, аспирант Института проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины.
E-mail: vitalik560@yandex.ru
Мисько Виталий Николаевич, аспирант Института проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины.
Misko Vitaliy Nikolaevich, postgraduate student Pukhov Institute for Modelling in Energy Engineering, National Academy of Sciences of Ukraine.

УДК 621.391

ДОСЛІДЖЕННЯ МОДЕЛЕЙ РОЗПОВСЮДЖЕННЯ РАДІОХВИЛЬ ВСЕРЕДИНІ ПРИМІЩЕННЯ ДЛЯ ПРОЕКТУВАННЯ ЖИВУЧИХ СИСТЕМ ОХОРОНИ ПОБУДОВАНИХ НА СТАНДАРТІ ZIGBEE

Сергій Родін

В цій статті наведено основні види моделей, що описують розповсюдження радіохвиль та обґрунтовано доцільність застосування цих моделей для моделювання. Розглянуто відомі моделі розповсюдження радіохвиль всередині приміщення, а саме: OSM(one-slope model), модель Keenan-Motley, COST 231 Multi-Wall Model. Проведені теоретичні розрахунки за цими моделями. Описано методика та засоби проведення експериментальних досліджень розповсюдження радіохвиль стандарту ZigBee. Наведені результати експериментальних досліджень, які були зіставлені з теоретичними розрахунками ослаблення сигналу. Опрацьовано та проаналізовано зведені результати дослідження. Перевірено придатність відомих моделей для проектування бездротової системи охорони, побудованої на стандарті ZigBee. Запропоновано новий підхід для проектування та проведення моделювання бездротових систем, що може підвищити такі їхні характеристики, як надійність та живучість.

Ключові слова: *системи охорони, розповсюдження радіохвиль всередині приміщення, моделі розповсюдження радіохвиль, бездротові, живучість, ZigBee, RSSI.*

Вступ. Застосування сучасних бездротових технологій ґрунтується на можливості їх швидкого розгортання і застосування. Їх зручно й легко використовувати в системах різного призначення як на відкритому просторі, так і в умовах забудови, зокрема всередині приміщень.

Бездротові технології щораз ширше застосовуються у системах моніторингу розподілених у просторі об'єктів, зокрема у системах охорони. Особливістю бездротових систем охорони, з одного боку, є низькі вимоги щодо обсягів та швидкості передачі даних, а з іншого – підвищені вимоги щодо надійності та живучості. Для забезпечення безперебійної роботи бездротових систем потрібно, щоб рівень сигналу в приймальній антені пристрою був на достатньому рівні.

Тому для підвищення живучості бездротових систем охорони, ще на етапі проектування системи, проводиться моделювання розташування приймачів та передавачів. Для моделювання застосовують моделі розповсюдження радіохвиль.

Існують кілька видів моделей для поширення радіохвиль, які наведені нижче[5]:

– статистичні моделі, які не потребують докладної інформації про приміщення, окрім загального опису його типу, наприклад, виробниче приміщення, готель, лікарня, торговий центр, приміщення старої забудови і т.п.;

– емпіричні (одно- чи багатопроменеві) моделі, які засновані на аналізі одного або декількох променів, що з'єднують передавальну й приймальну антени з метою оцінки рівня прийнятого сигналу;