суб'єкта господарювання. В основі вибору ІС повинні лягти такі ознаки: функціональність та інтегрованість; можливість підтримки корпоративного управління; галузь діяльності, організаційна структура та тип виробництва; архітектура, можливість інтеграції з іншими програмними продуктами, можливість підтримки оперативного і стратегічного управління. Поряд з тим, що впровадження ІС потребує значних витрат, які, на жаль, на сьогодні суб'єкти господарювання не готові понести, та й термін окупності є досить великим, економічний ефект від їх впровадження очевидний: зменшення часу для рутинного опрацювання облікових даних, доступність даних різного рівня, ефективність та оперативність прийняття управлінських рішень, оптимізація бізнес-процесів.

Література

1. Бенько М.М. Новітні інформаційні технології в бухгалтерському обліку / М.М. Бенько // Вісник Львівської комерційної академії. – Сер.: Економічна. – Львів : Вид-во ЛКА. – 2011. – Вип. 35. – С. 29-33.
2. Бухгалтер 911. [Електронний ресурс]. – Доступний з http://buhgalter911.com/Res/PO/ avtomat.aspx – Назва з екрану. – Дата звернення: 25.02.2015.
3. Гаврилов Л.П. Информационные технологии в коммерции : учеб. пособ. / Л.П. Гаврилов. – М. : Изд-во "Инфра-М", 2010. – 238 с.
4. Гаркуша С.А. Автоматизація облікових процесів: впровадження та переваги роботи системи / С.А. Гаркуша // Вісник Сумського національного аграрного університету : наук.-метод. журнал. – Сер.: Економіка і менеджмент. – Суми : Вид-во СНАУ. – 2012. – Вип. 4 (52). – С. 60-65.
5. Гончарук Я.А. Інформаційні системи і технології в обліку : навч. посіб. / Я.А. Гончарук., Н.С. Марушко, Д.С. Лозовицький, Г.М. Воляник. – Львів : Вид-во "Магнолія 2006", 2014. – 400 с.
6. Клепікова О.А. Сучасний стан і місце інформаційних технологій в управлінні підприємством / О.А. Клепікова // Науковий вісник Міжнародного гуманітарного університету : зб. наук. праць. – Сер.: Економіка і менеджмент. – Одеса : Вид-во МГУ. – 2013. – Вип. 5. – С. 74-77.
7. Кузьміна Н.М. Деякі методичні аспекти навчання використання інформаційних систем в управлінні підприємством / Н.М. Кузьміна // Науковий часопис НПУ ім. М.П. Драгоманова : зб. наук. праць. – Сер., № 2: Комп'ютерно-орієнтовані системи навчання. – К. : Вид-во НПУ ім. М.П. Драгоманова. – 2009. – № 7(14). – С. 110-118.
8. Левицька С.О. Інформаційне забезпечення системи бухгалтерського обліку / С.О. Левицька, О.В. Король // Вісник Національний університет водного господарства та природокористування : зб. наук. праць. – Сер.: Економіка. – Рівне : Вид-во НУВГП. – 2009. – Вип. 3(47).Ч. 1. – С. 367-372.
9. Пікуліна Н.Ю. Тенденції розвитку інформаційних технологій, що застосовуються в бухгалтерському обліку, аудиті та внутрішньому контролі / Н.Ю. Пікуліна, Л.А. Шило // Проблеми економіки транспорту : зб. наук. праць Дніпропетровського НУЗТ ім. акад. В. Лазаряна. – 2013. – Вип. 6. – С. 68-75.
10. Харитонов С.А. Информационные системы бухгалтерского учета : учеб. пособ. / С.А. Харитонов, Д.В. Чистов, Е.Л. Шуремов. – М. : Изд-во "Инфра-М", ФОРУМ, 2010. – 160 с.
11. Шипунова О.В. Автоматизація управління підприємством: основні принципи, функції та підходи / О.В. Шипунова, Ю.В. Єльнікова // Проблеми і перспективи розвитку банківської системи України : зб. наук. праць. – Суми : Вид-во УАБС НБУ. – 2011. – Вип. 31. – С. 303-316.
12. Шквір В.Д. Інформаційні системи і технології в обліку та аудиті : підручник / В.Д. Шквір, А.Г. Загородній, О.С. Височан. – Львів : Вид-во НУ "Львівська політехніка", 2012. – 400 с.

Марушко Н.С., Воляник Г.М. **Информационные системы ведения учета: современное состояние и тенденции развития**

Дана оценка состояния использования современных информационных систем ведения учета на предприятиях. Обоснована необходимость внедрения корпоративных информационных систем на предприятиях. Осуществлен обзор состояния рынка информационных систем ведения учета и управления предприятием в Украине. Описаны основные требования, выдвинутые отечественными предприятиями в корпоративных

информационных систем. Осуществлен обзор тенденции развития интегрированных корпоративных информационных систем на отечественном рынке.

Ключевые слова: бизнес-процессы, информационные системы, интегрированные корпоративные информационные системы, программные продукты, бизнес-процессы, системы: ERP, CRM, SCAM, PSA.

Marushko N.S., Volyanyk G.M. **Information Systems for Accounting: Current Status and Trends for Development**

The assessment of the use of modern information systems for accounting firms is described. The necessity of introducing corporate information systems in the business is justified. Nowadays accounting support is supposed to be unthinkable without electronic data processing. Using Information Systems, accounting significantly improves the quality of information provision and provides effective support scheduling and control. The need for an integrated system of processing accounting information that would provide priority management accounting as the basis for a successful business in the future formation data for financial and tax accounting is emphasized. This integrated system of accounting would single database input information, which is formed at the stage of collecting primary data. Undoubtedly, the successful execution of these tasks is possible through the use of modern information technology systems and accounting and management. These systems act today as integrated corporate information systems. Some basic requirements for introducing corporate information systems and technologies by domestic enterprises are described. The overview of market information systems for accounting and business management in Ukraine is made. We applied software that belongs to corporate information systems and is adapted to modern conditions of doing business in Ukraine. Some trends in the development of integrated corporate information systems in the modern business environment are also studied.

Keywords: business processes, information systems, integrated corporate information systems, software, business processes, systems: ERP, CRM, SCAM, PSA.

УДК 01.05.02:05.[13.06+13.21]

Доц. Т.Є. Рак, д-р техн. наук;
ст. викл. Ю.О. Борзов – Львівський ДУ БЖД

ЛІНІЙНІ ФОРМИ З ЕЛЕМЕНТАМИ АЛГОРИТМУ RSA І ДОДАТКОВЕ ЗАШУМЛЕННЯ У ЗАХИСТІ ПІВТОНОВИХ ЗОБРАЖЕНЬ

Розглянуто проблеми захисту зображень від несанкціонованого доступу. Сформульовано вимоги до методів шифрування у разі їх використання стосовно зображень – повна зашумленість зашифрованого зображення. Описано використання елементів алгоритму RSA і лінійних форм для використання під час шифрування – дешифрування зображень за наявності додаткового зашумлення. Запропоновану модифікацію базового алгоритму RSA можна застосовувати під час шифрування як для півтонових, так і для кольорових зображень. Стійкість до несанкціонованого дешифрування запропонованого алгоритму забезпечується стійкістю базового алгоритму RSA з додатковою стійкістю, яка надається використанням лінійних форм.

Ключові слова: шифрування, дешифрування, алгоритм RSA, лінійна форма.

Вступ. Зображення – відтворення виду, форми і кольору предмета світловими променями, що пройшли оптичну систему з центрованих сферичних поверхонь, які мають одну загальну оптичну вісь. Якщо зображення предмета утворено перетинанням самих променів, то його називають дійсним, якщо їхнім продовженням – уявним. При цьому можливі такі варіанти: у разі розташування предмета за подвійною фокусною відстанню від системи його зображення, розташоване за першим фокусом у просторі зображень, буде дійсним, зменшеним і зворотним; у разі розташування предмета на подвійній фокусній відстані від

системи його зображення, розташоване в просторі зображень також на подвійній фокусній відстані від системи, буде дійсним, рівним самому предмету і зворотним; якщо предмет розташований між першим і другим фокусами, його зображення, отримане в просторі зображень за подвійним фокусом, буде дійсним, збільшеним, зворотним; якщо предмет розташований між переднім фокусом і системою, його зображення, отримане також у просторі предметів, буде уявним, прямим і збільшеним.

Як стохастичний сигнал зображення є одним із найбільш уживаних видів інформації. Але зображення є сигналом, який володіє, у додаток до типової інформативності, ще й візуальною інформативністю. Відповідно, актуальною задачею є захист таких зображень від несанкціонованого доступу та використання. Це призводить до використання відомих класичних методів шифрування у разі шифрування зображень.

Алгоритм RSA є одним із найбільш уживаних промислових стандартів шифрування сигналів. На відміну від симетричного кодування, за якого процедура розшифровки легко відновлюється за процедурою шифрування і в зворотному напрямку, у схемі кодування з відкритим ключем неможливо обчислити процедуру дешифрування, знаючи процедуру шифрування. Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі – відкритий і секретний, разом відкритий і відповідний йому секретний ключі утворюють пару ключів. Така інформативність із сучасними методами оброблення зображень дає можливість для реалізації несанкціонованого доступу. Організація атаки на зашифроване зображення можлива у двох варіантах: через традиційний злом методів шифрування або через методи візуального оброблення зображень (методи фільтрації, виділення контурів тощо). У зв'язку з цим до методів шифрування у разі їх використання стосовно зображень висувається ще одна вимога – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів візуального оброблення зображень.

Мета роботи. Відносно зображення актуальною задачею є таке модифіковане використання алгоритму RSA, щоб: не зменшити криптографічну стійкість алгоритму RSA; забезпечити повну зашумленість зображення, з метою унеможливити використання методів візуального оброблення зображень. Одним із шляхів створення такої модифікації є поєднання елементів алгоритму RSA і лінійних форм у програмній реалізації.

Характеристики зображення. Є два способи формування зображення технічними засобами: матричний (растровий) і векторний. В основу матричного способу формування зображення покладено принцип розкладання його на елементи скінчених розмірів, зазвичай, у формі точки або прямокутника. Елемент зображення піксель за матричного способу створення зображення не може мати структури, а тільки колір і/або яскравість.

Матричний спосіб створення зображення використовують у телебаченні, для передавання зображень за допомогою факсимільних апаратів тощо. З погляду інформаційної ємності, матричне зображення має значну надлишковість, тобто передається багато інформації, необов'язкової для сприйняття графічного образу. Наприклад, для створення суцільного тла, фону картини, зовсім необов'язково передавати інформацію окремо про колір та яскравість кожного пікселя фону.

Нехай задано рисунок P зі ширини l і висоти h. Його можна розглядати як матрицю інтенсивностей пікселів

$$\boldsymbol{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,l} \\ \dots & \dots & \dots \\ c_{h,1} & \dots & c_{h,l} \end{pmatrix}, \qquad (1)$$

де c_{ij} – значення інтенсивності пікселя. Під градацію яскравості звичайно приділяється 1 байт, причому 0 – чорний колір.

Задача виділення контуру вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашують області постійних рівнів яскравості, тобто контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними. Тому виділення контуру означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через що контури залишаються в зображенні під час шифрування у системі RSA, оскільки шифрування тут базується на піднесенні до степеня по модулю деякого натурального числа. При цьому, на контурі і на сусідніх до контуру пікселях піднесення до степеня значення яскравостей дає ще більший розрив.

Опис алгоритму шифрування. Шифрування по шести рядках матриці зображення. Нехай P,Q,R,T,W,U – три пари довільних простих чисел і $N=P\cdot Q$, $M=R\cdot T$, $N=P\cdot Q, M=R\cdot T$, $L=W\cdot V, j(N)=(P-\mathbf{1})(Q-\mathbf{1})$, $j(M)=(R-\mathbf{1})(T-\mathbf{1})$, $j(M)=(R-\mathbf{1})(T-\mathbf{1})$, $j(N)=(U-\mathbf{1})(W-\mathbf{1})$. Шифрування відбувається поелементно з використанням такого перетворення елементів матриці зображення C:

1. Випадково вибирається натуральне число $e<j(N)$ і знаходиться таке натуральне d, щоб виконувалася конгруенція $ed=\mathbf{1}(\mathbf{mod}j(N))$.
2. Випадково вибирається натуральне число $s<j(M)$ і знаходиться таке натуральне t, щоб виконувалася конгруенція $st=\mathbf{1}(\mathbf{mod}j(M))$.
3. Випадково вибирається натуральне число $u<j(L)$ і знаходиться таке натуральне w, щоб виконувалася конгруенція $uw=\mathbf{1}(\mathbf{mod}j(L))$.
4. Для кожного $k=\mathbf{6}*i, i=\mathbf{0},\mathbf{1},\mathbf{2},\ \dots$ і кожного елемента $c_{k,j}$, $\mathbf{0}\le j\le l$ будується число $b_{k,j}=c^{e}_{(k,j)}(mod(N))$.
5. Для кожного $n=\mathbf{6}*i+\mathbf{1}, i=\mathbf{0},\mathbf{1},\mathbf{2},\ \dots$ і кожного елемента $c_{n,j}$, $\mathbf{0}\le j\le l$ будується число $a_{n,j}=c^{d}_{(n,j)}(mod\ \varphi(N))+b_{k,j}+f(j)$, де $f(j)$ – функція зашумлення.
6. Для кожного $k=\mathbf{6}*i+\mathbf{2}, i=\mathbf{0},\mathbf{1},\mathbf{2},\ \dots$ і кожного елемента $c_{k,j}$, $\mathbf{0}\le j\le l$ будується число $b_{k,j}=c^{s}_{(k,j)}(mod(M))$.
7. Для кожного $n=\mathbf{6}*i+\mathbf{3}, i=\mathbf{0},\mathbf{1},\mathbf{2},\ \dots$ і кожного елемента $c_{n,j}$, $\mathbf{0}\le j\le l$ будується число $a_{n,j}=c^{t}_{(n,j)}(mod\ \varphi(M))+b_{k,j}+g(j)$, де $g(j)$ – функція зашумлення.

8. Для кожного $k = \mathbf{6}*i+\mathbf{4}, i = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots$ і кожного елемента $c_{k,j}$, $\mathbf{0} \le j \le l$ будується число $b_{k,j} = c^{u}_{(k,j)}(mod(L))$.
9. Для кожного $n = \mathbf{6}*i+\mathbf{5}, i = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots$ і кожного елемента $c_{n,j}$, $\mathbf{0} \le j \le l$ будується число $a_{n,j} = c^{w}_{(n,j)}(mod\ \varphi(L)) + b_{k,j} + h(j)$, де $h(j)$ – функція зашумлення.
10. Зашифрованим є зображення після вибору всіх стрічок вхідного зображення.
11. Усі числа $b_{k,j}$, $a_{n,j}$ послідовно записуються в таку матрицю:

$$\boldsymbol{V} = \begin{pmatrix} b_{1,1} & \ldots & b_{1,l} \\ \ldots & \ldots & \ldots \\ b_{h,1} & \ldots & b_{h,l} \end{pmatrix}.$$

Дешифрування. Дешифрування виконується в оберненому порядку з використанням властивостей алгоритму RSA. Результати наведено на рис. 1-3 при $P = \mathbf{23}, Q = \mathbf{37}, S = \mathbf{73}, T = \mathbf{37}, U = \mathbf{97}, W = \mathbf{37}$. Функції зашумлення мають вигляд $f(j) = -j, g(j) = -j^2, h(j) = j^3$.

Рис. 1. Початкове зображення

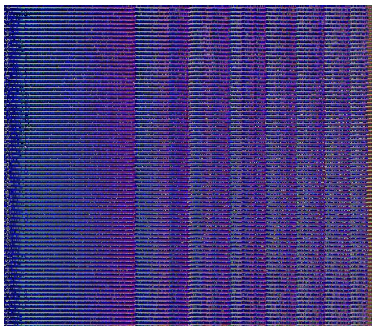

Рис. 2. Зашифроване зображення

Рис. 3. Дешифроване зображення

Результати з іншим зашумленням наведено на рис. 4-6 при $P = \mathbf{43}$, $Q = \mathbf{37}$, $S = \mathbf{73}$, $T = \mathbf{37}$, $U = \mathbf{97}$, $W = \mathbf{37}$. Функції зашумлення мають вигляд $f(j) = -j^3, g(j) = -j^3, h(j) = j^3$.

Рис. 4. Початкове зображення

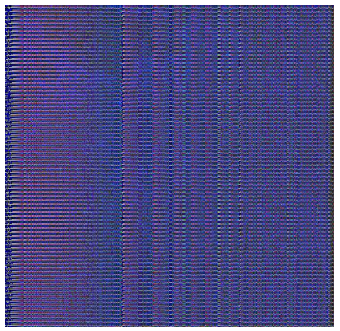

Рис. 5. Зашифроване зображення

Рис. 6. Дешифроване зображення

Після візуального порівняння рис. 2 і 5 видно, що структура зашифрованого зображення залежить від вигляду функцій зашумлення і значень простих чисел P, Q, R, T, W, U. Контури в обох зашифрованих зображеннях відсутні. Початкове і дешифроване зображення незначно відрізняються рівнем яскравості.

Висновки. Запропоновану модифікацію шифрування можна використовувати як для півтонових, так і для кольорових зображень і ґрунтується вона на використанні ідей базового алгоритму RSA. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення може зрости розмір шифрованого зображення.

Стійкість до несанкціонованого дешифрування запропонованого алгоритму забезпечується стійкістю базового алгоритму RSA з додатковою стійкістю, яка надається використанням лінійних форм.

Література

1. Павлидис Т. Алгоритмы машиной графики и обработки изображений / Т. Павлидис. – М. : Изд-во "Радио и связь", 1986. – 399 с.
2. Яне Б. Цифровая обработка изображений / Б. Яне. – М. : Изд-во "Техносфера", 2007. – 583 с.
3. Брюс Шнайер. Прикладная криптография / Шнайер Брюс. – М. : Изд-во "Триумф", 2003. – 815 с.
4. Рашкевич Ю.М. Модифікація алгоритму RSA для деяких класів зображень / Ю.М. Рашкевич, Д.Д. Пелешко А.М. Ковальчук, М.З. Пелешко // Технічні вісті : зб. наук. праць. – 2008/1(27), 2(28). – С. 59-62.
5. Ковальчук А. Бінарні операції та елементи алгоритму RSA при шифруванні – дешифруванні кольорових зображень / А. Ковальчук, Д. Пелешко, Ю. Борзов // Вісник Національного

університету "Львівська політехніка". – Сер.: Комп'ютерні науки та інформаційні технології. – Львів : Вид-во НУ "Львівська політехніка". – 2013. – № 771. – С. 121-126.

Рак Т.Е., Борзов Ю.А. **Линейные формы с элементами алгоритма RSA и дополнительное зашумление в защите полутоновых изображений**

Рассмотрены проблемы защиты изображений от несанкционированного доступа. Сформулированы требования к методам шифрования в случае их использования относительно изображений – полная зашумленность зашифрованного изображения. Описано использование элементов алгоритма RSA и линейных форм для использования при шифровании – дешифровании изображений при наличии дополнительного зашумления. Предложенная модификация базового алгоритма RSA может применяться для шифрования как для полутоновых, так и для цветных изображений. Стойкость к несанкционированному дешифрованию предложенного алгоритма обеспечивается стойкостью базового алгоритма RSA с дополнительной стойкостью, которая предоставляется использованием линейных форм.

Ключевые слова: шифрование, дешифрование, алгоритм RSA, линейная форма.

Rak T.Ye., Borzov Yu.O. **Linear forms with elements of the RSA algorithm and additional noise in defense of grayscale images**

This article deal with the problem of image protection from unauthorized access. The requirements to encryption methods in the case of images – full noisy encrypted image. The using of elements of the RSA algorithm and linear forms for images encrypting-deciphering in case of additional noise is described. A modification of the basic algorithm of RSA encryption can be used for grayscale and color images. Resistance to unauthorized decryption of the proposed algorithm is provided by the basic stability RSA algorithm with additional stability provided by the use of linear forms.

Keywords: encryption, decryption, the RSA algorithm, linear form.

УДК 614.843(075.32)

Проректор И.О. Мовчан, канд. техн. наук – Львовский ГУ БЖД

МЕТОДИКА ОПРЕДЕЛЕНИЯ РИСКА УВЕЛИЧЕНИЯ ПРОДОЛЖИТЕЛЬНОСТИ ВРЕМЕНИ ЛИКВИДАЦИИ ПОЖАРА

Разработан метод определения риска увеличения продолжительности времени процесса ликвидации пожара на объекте защиты с использованием основных положений теории надежности с разработкой функциональных моделей риска каждой технологической операции процесса ликвидации пожара, на основании которых получена математическая модель риска увеличения продолжительности времени ликвидации пожара с установлением влияния составляющих риска на обеспеченность проектами и программами каждой технологической операции, которая влияет на эффективность тушения пожара.

Ключевые слова: пожар, ликвидация пожара, риск увеличения продолжительности времени ликвидации пожара, математическая модель, распределение Вейбулла, экспоненциальное распределение, нормальное распределение, информационные технологии.

Постановка проблемы. В сфере пожарной безопасности пользуются термином "пожарный риск", то есть это мера возможности реализации пожарной опасности объектов защиты и ее последствий для людей и материальных ценностей. Гарантирование пожарной безопасности объектов защиты, а также гарантия ликвидации пожара, в случае его возникновения, состоит из определения, анализа и оценивания пожарного риска, что позволяет разрабатывать и внедрять соответствующие мероприятия для его уменьшения до допустимого значения. Согласно рекомендациям Всемирной организации здравоохранения и

Постановления Кабинета Министров Украины [1, 2] пожарные риски классифицируют так: 1) незначительный риск $\varepsilon \le 10^{-6}$; 2) средний риск $\varepsilon = 10^{-6} \ldots 5 \cdot 10^{-5}$; 3) высокий (терпимый) риск $\varepsilon = 5 \cdot 10^{-5} \ldots 5 \cdot 10^{-4}$; 4) неприемлемый риск $\varepsilon > 5 \cdot 10^{-4}$. В свою очередь, пожарный риск указывает на соответствующую вероятность возникновения пожара на объекте.

Относительно определения пожарного риска для объектов в настоящее время проделана значительная научно-исследовательская работа, на основании которой получены положительные результаты. Значительный вклад в решение этого вопроса внесли Н.Н. Брушлинский, В.В. Холщевников, Д.А. Самошин (Россия), Э.Н. Гулида, И.А. Мовчан, А.Д. Кузык, Я.И. Хомяк, Е.Ф. Якименко, Р.В. Климась (Украина) и многие другие. Однако практически отсутствуют данные по определению риска ликвидации пожара, который может возникнуть на том или ином объекте. В следствии этого очень сложно предложить необходимые мероприятия для управления проектами и программами системы ликвидации пожаров на объектах защиты, которые бы уменьшали последствия от пожара. Поэтому возникает проблема в определении риска процесса ликвидации пожара с использованием математических моделей.

Анализ последних достижений и публикаций. Первые теоретические исследования по установлению риска ликвидации пожара были выполнены Н.Н. Брушлинским [3]. Результаты статистических исследований [3] показывают, что длительность тушения пожара τ_T, описывается с помощью распределения Эрланга

$$\phi(\tau_T) = \mu \frac{(\mu\tau_T)^r}{r!} e^{-\mu\tau} \quad (\tau > 0;\ r = 0, 1, 2, \ldots), \tag{1}$$

где: μ – постоянный параметр; r – порядок распределения Эрланга.

Для нормирования продолжительности времени тушения пожара рекомендуют [4, 5] рассматривать вероятность противоположного случайного события, то есть вероятность того, что τ_T будет не меньшим некоторого значения τ. С учетом пожарного риска $\varepsilon_{л.п}$, то есть с учетом части пожаров от общего их количества, продолжительность времени тушения которых выходит за границу некоторого нормативного значения $\tau_н$, можно определить количество пожаров, которые будут превышать это время. В этом случае, если $\varepsilon_{л.п} = 0{,}01$, то лишь для одного пожара из 100, продолжительность времени тушения будет превышать нормативное время $\tau_н$, то есть

$$P\{\tau_T \ge \tau_н\} \le \varepsilon_{л.п}. \tag{2}$$

Результаты анализа зависимости (2) показывают, что с уменьшением значения пожарного риска нормативное время тушения пожара увеличивается. Для усовершенствования и повышения эффективности работы пожарно-спасательных подразделений при тушении пожаров была предложена работа, которая состояла в разработке имитационной модели "ТИГРИС" в Академии ГПС МВД России [6]. Подобная имитационная модель была также разработана в Нью-Йоркском Ренд-институте [7].

При всех своих положительных характеристиках данные модели имеют один общий функциональный недостаток. Фактически основной показатель, который характеризует результативность действий пожарно-спасательных под-