А.С. Крюковский[1]
Т.В. Лебедева[2]

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА ХРАНЕНИЯ И ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В представленной работе рассматриваются непрерывные математические модели, описывающие процессы поступления, хранения, потери и передачи конфиденциальных данных в информационной системе. К вышеописанным процессам были применены следующие виды математических моделей: линейная, синусоидальная и параболическая. Рассмотрены потоки конфиденциальной информации в условиях маскировки. Для каждой из изученных моделей показано, какое влияние оказывают изменения таких параметров, как доля потерь и число итераций, на количество конфиденциальных данных в информационной системе при различных дополнительных условиях.

Ключевые слова: *математическая модель, конфиденциальная информация, модель хранения информации, доля потерь.*

A.S. Kryukovsky
T.V. Lebedeva

MATHEMATICAL MODELING OF THE CONFIDENTIAL INFORMATION STORAGE AND TRANSMISSION

In the present paper, the continuous mathematical models describing the process of receiving, storage, and transmission loss of sensitive data in the information system are considered. By the above processes following mathematical models: linear, sinusoidal and parabolic have been applied. The flow of confidential information in disguise is considered. For each of these models what impact changes in parameters such as the share of losses and the number of iterations, the number of sensitive data in the information system under various additional conditions is shown.

Keywords: *mathematical model, the confidential information, the model of information storage, the percentage of losses.*

В настоящее время отмечается увеличение доли информации в составе активов большинства компаний. Это происходит за счет роста объемов и стоимости информации, которой владеет предприятие [1]. В связи с этим возникает важный вопрос о сохранности конфиденциальных данных. Для оценки текущего уровня защищенности информации от актуальных угроз разрабатываются модели хранения информации, учитывающие процессы поступления и потери конфиденциальных данных в информационной системе, модели угроз, модели злоумышленников, методики оценок рисков (подробно рассмотрена в работе [2]), а также методики оценок возможного ущерба от потери конфиденциальной информации [3].

В работе [4] рассмотрены дискретные математические модели. В настоящей работе разработаны непрерывные математические модели, описывающие процесс хранения, потери и передачи конфиденциальной информации.

Рассмотренные модели позволяют прогнозировать динамику изменения объема конфиденциальной информации, что, в свою очередь, является одной из основных составляющих политики формирования информационной безопасности предприятия.

Постановка задачи

Рассмотрим процесс хранения данных в информационной системе. Ограничимся дискретным случаем. Данный процесс тесно связан с процессом поступления в систему информации, а также с процессом потери данных. Эту взаимосвязь можно изобразить в виде блок-схемы.

[1] Доктор физико-математических наук, профессор, декан факультета информационных систем и компьютерных технологий НОУ ВПО «Российский новый университет».

[2] Аспирантка НОУ ВПО «Российский новый университет».

Буквами *f(t)* обозначен объем конфиденциальной информации, поступающий в систему в момент времени *t* (плотность потока информации). В силу ряда причин (к которым могут быть отнесены как действия злоумышленников, так и естественная «диссипация» информации), часть информации *(d)* перестает быть конфиденциальной и в этом качестве теряется. Именно в этом смысле мы будем писать ниже о «потере» информации.

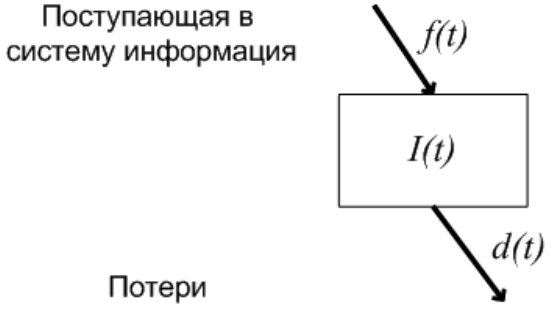

Рис. 1. Блок-схема процесса хранения данных в информационной системе

Предполагается, что в системе в начальный момент времени при $t = t_0$ имеется некоторый объем конфиденциальной информации $\mathrm{I}_s(t_0) = \mathrm{I}_0$. Тогда в некоторый момент времени *t* изменение количества конфиденциальной информации в системе можно определить по формуле:

$$\Delta \mathrm{I}_s = -i(t)\,\mathrm{I}_s(t)\Delta t + f(t)\Delta t, \qquad (1)$$

где *i(t)* – доля потери конфиденциальной информации в единицу времени. Поделив обе части уравнения (1) на Δt и перейдя к пределу при $\Delta t \to 0$, получаем линейное неоднородное дифференциальное уравнение первого порядка:

$$\mathrm{I}'_s(t) = -i(t)\,\mathrm{I}_s(t) + f(t). \qquad (2)$$

Решение дифференциального уравнения (2) с начальным условием

$$\mathrm{I}_s(t_0) = \mathrm{I}_0 \qquad (3)$$

хорошо известно:

$$\mathrm{I}_s(t) = \frac{1}{\mu(t)}\left(\int_{t_0}^{t} \mu(\eta) f(\eta)\,\mathrm{d}\eta + \mathrm{I}_0\right), \qquad (4)$$

где

$$\mu(\eta) = \exp\left(\int_{t_0}^{\eta} i(\xi)\,\mathrm{d}\xi\right). \qquad (5)$$

Очевидно, что общий объем конфиденциальной информации, поступившей в систему за временной интервал $t - t_0$, равен:

$$\mathrm{I}_{полн}(t) = \int_{t_0}^{t} f(\xi)\,\mathrm{d}\xi + \mathrm{I}_0\ . \qquad (6)$$

Тогда величина суммарных потерь определяется формулой:

$$D(t) = \mathrm{I}_{полн}(t) - \mathrm{I}_s(t), \qquad (7)$$

а величина потерь в единицу времени как:

$$d(t) = \frac{i(t)}{\mu(t)}\left(\int_{t_0}^{t} \mu(\eta) f(\eta)\,\mathrm{d}\eta + \mathrm{I}_0\right). \qquad (8)$$

Рассмотрим различные частные случаи.

1. Равномерный поток информации, доля потерь постоянна

Предположим, что в систему в каждый момент времени поступает один и тот же объем конфиденциальной информации, то есть плотность потока информации постоянна: $f(t) = f = const$. Будем считать, что доля потери конфиденциальной информации в единицу времени также постоянна: $i(t) = i = const$. Тогда из (4) и (5) получаем:

$$\mathrm{I}_s(t) = \frac{f}{i}\left(1 - \exp(-i(t - t_0))\right) + \mathrm{I}_0 \exp(-i(t - t_0)). \qquad (8)$$

Объем конфиденциальной информации, теряющийся и остающийся в системе в единицу времени, определяется соответственно формулами:

$$d(t) = i\,\mathrm{I}_s(t), \quad y(t) = (1 - i)\,\mathrm{I}_s(t). \qquad (9)$$

Из формул (8) и (9) можно показать, что при $t \to \infty$:

$$\mathrm{I}_s \cong \frac{f}{i}, \quad y_\infty = \frac{(1-i)}{i} f, \quad d_\infty = f, \qquad (10)$$

то есть в системе устанавливается постоянный объем конфиденциальной информации, равной объему информации, поступающей в систему в каждый период, деленный на долю потерь, причем из системы уходит ровно столько конфиденциальной информации, сколько и поступает.

При малых значениях времени *t* и малой доле потерь *i*

$$\mathrm{I}_s \cong \mathrm{I}_0 + (f - i\,\mathrm{I}_0)(t - t_0). \qquad (11)$$

Если в начальный момент времени в системе отсутствует конфиденциальная информация ($\mathrm{I}_0 = 0$), то объем конфиденциальной информации первоначально увеличивается, как в случае, когда потерь не было, поскольку

$$\mathrm{I}_{полн} = f(t - t_0) + \mathrm{I}_0\ . \qquad (12)$$

На рисунке 2 показана зависимость объема конфиденциальной информации от времени при $\mathrm{I}_0 = 0$ (рис. 2а) и $\mathrm{I}_0 = 2$ (рис. 2б). В обоих случаях

$f = 1$, $t_0 = 0$. Тонкой линией показан рост объема информации в отсутствие потерь.

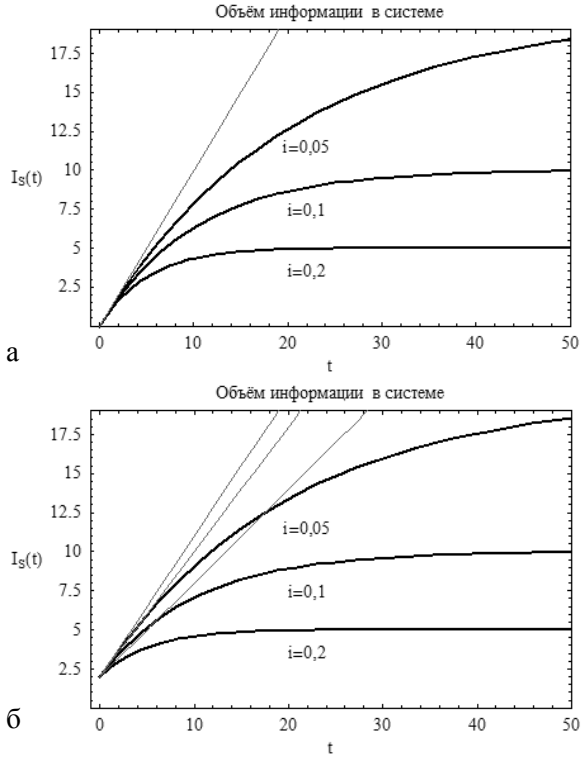

Рис. 2. Зависимость объема конфиденциальной информации от времени. Равномерный поток данных. $I_0 = 0$ – рис. 2а, $I_0 = 2$ – рис. 2б

Из рисунка 2 видно, что вначале объем конфиденциальной информации в системе резко возрастает, однако в дальнейшем темпы прироста информации падают и наступает «насыщение». Это объясняется тем, что в системе устанавливается постоянный объем конфиденциальной информации, равной объему информации, поступающей в систему в каждый период, деленный на долю потерь, причем из системы уходит ровно столько конфиденциальной информации, сколько и поступает.

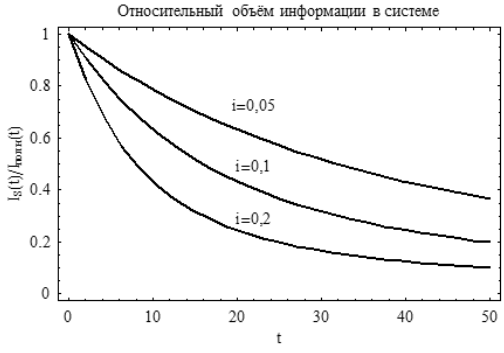

Рис. 3. Относительный объем информации в системе. Равномерный поток данных, $I_0 = 0$

На рисунке 3 показана зависимость относительного объема конфиденциальной информации от времени. Это отношение объема информации в системе, сохранившей свою конфиденциальность, ко всей поступившей к этому моменту конфиденциальной информации.

Видно, что относительный объем сначала резко падает, а потом плавно стремится к нулю.

2. Поток информации линейно растет, доля потерь постоянна

Рассмотрим вариант, когда в систему в каждый момент времени поступает некоторый объем конфиденциальной информации, при этом величина данных, поступающих в каждый последующий момент времени, превышает количество поступившей информации на некоторую постоянную величину: $f(t) = f_0 + \beta\, t$. Будем по-прежнему считать, что доля информации, которая перестает быть конфиденциальной в единицу времени, остается постоянной: $i(t) = i = const$. Тогда, проводя вычисления по формулам (4) и (5) при $t_0 = 0$, находим:

$$\mathrm{I}_s(t) = \frac{f_0}{i}\left(1 - \mathrm{e}^{-it}\right) + \mathrm{I}_0 \mathrm{e}^{-it} + \frac{\beta}{i^2}\left(it - 1 + \mathrm{e}^{-it}\right). \qquad (13)$$

Из формул (7) и (8) можно сделать ряд выводов. При $t \to \infty$

$$\mathrm{I}_{s,\infty} \cong \frac{f_0}{i} - \frac{\beta}{i^2} + \frac{t\beta}{i}, \quad d_\infty \cong f_0 - \frac{\beta}{i} + t\beta, \qquad (14)$$

то есть, в системе объем конфиденциальной информации равномерно увеличивается, при этом линейно растут и потери в системе.

При малых значениях времени t и малой доле потерь i

$$\mathrm{I}_s \cong \mathrm{I}_0 + t\, f_0, \qquad d \cong i(\mathrm{I}_0 + t\, f_0), \qquad (15)$$

то есть, объем конфиденциальной информации увеличивается как в случае, если потерь не было. Однако между этими двумя областями существует переходная зона. Если вначале скорость роста это f_0, то при больших t скорость роста β / i.

На рисунке 4 показана зависимость объема конфиденциальной информации от времени t при разных значениях β. Тонкими линиями показаны асимптотические зависимости и зависимость в отсутствие потерь ($\mathrm{I}_0 = 0, f_0 = 1$).

Из рисунка 4 видно, что вначале объем конфиденциальной информации в системе резко возрастает, однако темпы прироста информации падают, становятся постоянными («насыщение»

темпов роста), и после этого объем данных возрастает линейно. Это объясняется тем, что в системе объем конфиденциальной информации равномерно увеличивается, при этом линейно растут и потери в системе.

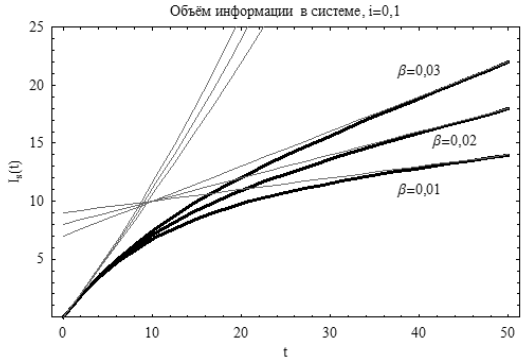

Рис. 4. Зависимость объема конфиденциальной информации от времени при разных значения параметра β . Случай линейно-нарастающего потока данных

На рис. 5 представлены зависимости объема конфиденциальной информации от времени t при различных значениях доли потерь i и параметре $\beta = 0{,}01$.

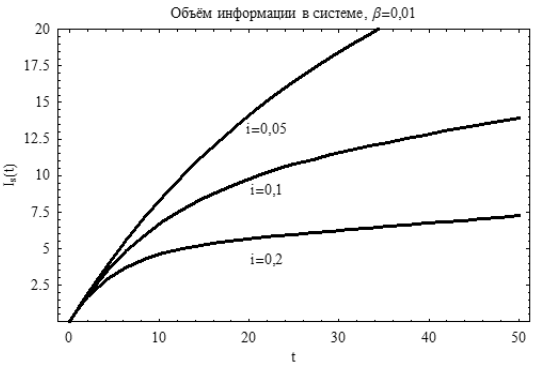

Рис. 5. Зависимость объема конфиденциальной информации от времени при разных значениях параметра i. Линейно-нарастающий поток данных

Наконец, на рисунке 6 показана зависимость относительного объема конфиденциальной информации от времени t. Как и в случае равномерного потока, это отношение конфиденциальной информации в системе к поступившей к этому моменту всей конфиденциальной информации.

Видно, что относительный объем сначала резко падает, а потом медленно стремится к нулю, поскольку полный объем конфиденциальной информации ($t_0 = 0$), поступившей в систему, равен:

$$\mathrm{I}_{полн}(t) = \mathrm{I}_0 + f_0 t + \frac{t^2 \beta}{2}. \qquad (16)$$

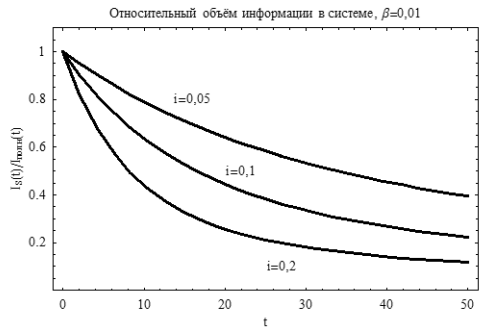

Рис. 6. Зависимость относительного объема информации в системе от числа периодов. Линейно-нарастающий поток данных

3. Поток информации растет по параболическому закону, доля потерь постоянна

Следующий рассмотренный нами случай – это вариант, когда в систему в каждый момент времени поступает некоторый объем конфиденциальной информации, причем величина данных, поступающих в каждый последующий момент времени, нарастает по параболическому закону: $f(t) = f_0 + at + bt^2$. Будем считать, что доля информации, которая в единицу времени перестает быть конфиденциальной, остается попрежнему постоянной: $i(t) = i = const$. На рисунке 7 показана зависимость объема конфиденциальной информации от времени.

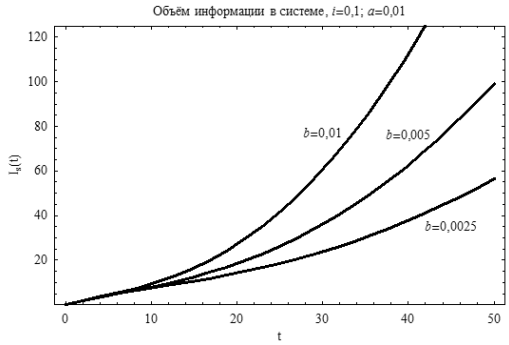

Рис. 7

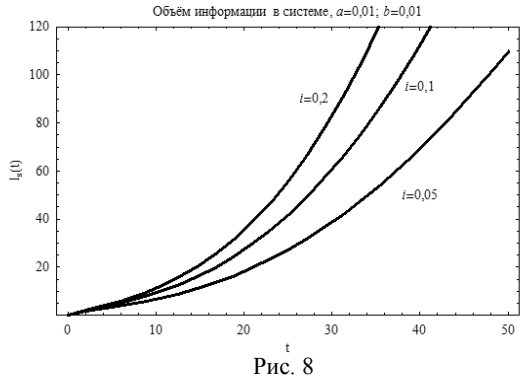

Рис. 8

Зависимость объема конфиденциальной информации от времени при разных значениях параметра b (рис. 7) и параметра i (рис. 8). Поток данных нарастает по параболическому закону

Из рисунков 7 и 8 видно, что по сравнению с линейной зависимостью характер кривых значительно изменился: темпы роста объема конфиденциальной информации в этом случае растут (кривые выпуклы вниз), а в предыдущем случае убывали (кривые выпуклы вниз). Видно, что вначале объем конфиденциальной информации в системе медленно возрастает, однако в дальнейшем, так как темпы прироста информации возрастают, объем данных возрастает параболически.

На рисунке 9 показана зависимость относительного объема конфиденциальной информации от числа периодов. Это отношение конфиденциальной информации в системе к поступившей к этому моменту всей конфиденциальной информации.

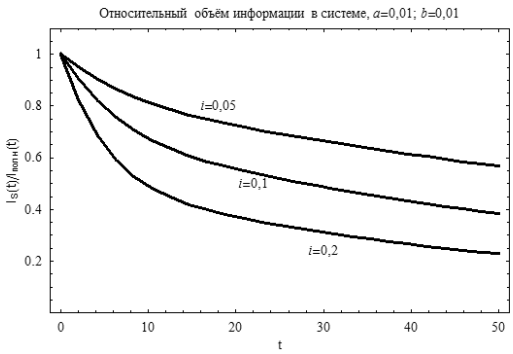

Рис. 9. Относительный объем информации в системе. Поток данных нарастает по параболическому закону

Видно, что относительный объем сначала резко падает, а затем медленно убывает.

4. Поток информации меняется по синусоидальному закону, доля потерь постоянна

Следующий рассматриваемый вариант развития событий – это случай, когда величина поступающего в систему в каждый момент времени объема конфиденциальной информации изменяется по синусоидальному закону: $f(t) = f_0(1 + a\sin(\omega t))$. Будем считать, что доля информации, которая перестает быть конфиденциальной в единицу времени, как и в предыдущих случаях, постоянна: $i(t) = i = const$. На рисунке 10 показана зависимость объема конфиденциальной информации от времени при $i = 0{,}1$, круговой частоте $\omega = \dfrac{\pi}{6}$ и при различных значениях глубины модуляции $a = 0{,}1;\ 0{,}5;\ 1$.

Из рисунка 10 видно, что колебания объема конфиденциальной информации в системе происходят относительно той же кривой роста, которая имела бы место в отсутствие модуляции (сравните с рис. 2). Затуханий колебаний не наблюдается.

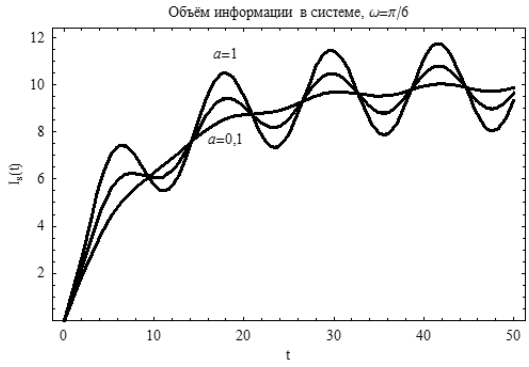

Рис. 10. Зависимость объема конфиденциальной информации от времени при разных значениях глубины модуляции a. Параметр $i = 0{,}1$. Поток данных меняется по синусоидальному закону. Кривая при $a = 0{,}5$ – промежуточная

На рис. 11 показана зависимость объема конфиденциальной информации от времени при $i = 0{,}1$, глубине модуляции $a = 0{,}5$ и различных значениях частоты $\omega = \dfrac{\pi}{12}, \dfrac{\pi}{6}, \dfrac{\pi}{3}$.

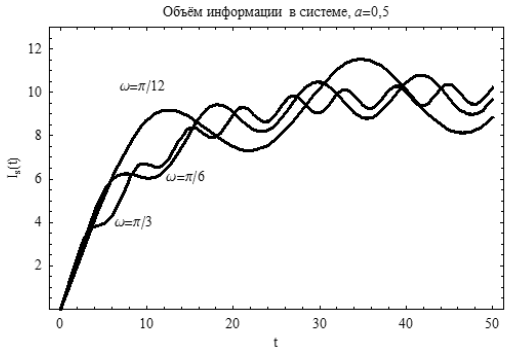

Рис. 11. Зависимость объема конфиденциальной информации от времени при разных значениях частоты ω. Параметр $i = 0{,}1$. Поток данных меняется по синусоидальному закону

Следует отметить, что описанная выше тенденция сохраняется при различных значениях круговой частоты ω, однако размах колебаний с уменьшением частоты растет.

На рисунке 12 показана зависимость относительного объема конфиденциальной информации от времени. Это отношение конфиденциальной информации в системе к поступившей к этому моменту времени всей конфиденциальной информации.

Кривые в целом отражают зависимость, показанную на рис. 3. Однако с увеличением глубины модуляции на рисунке возникают провалы, повторяющиеся с характерной частотой.

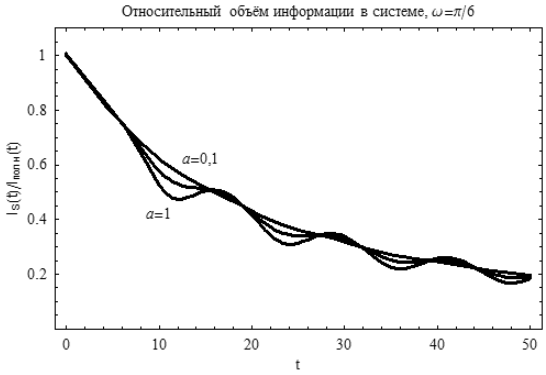

Рис. 12. Зависимость относительного объема информации в системе от числа периодов при различных значениях глубины модуляции a. Параметр $i = 0{,}1$. Круговая частота $\omega = \frac{\pi}{6}$. Поток данных меняется по синусоидальному закону

5. Поток информации постоянный, доля потерь – колеблющаяся величина

Предположим, что в систему в единицу времени поступает один и тот же объем конфиденциальной информации $f(t) = f_0$. Будем считать, что доля информации $i(t)$, которая перестает быть конфиденциальной в единицу времени, меняется по синусоидальному закону, то есть действия злоумышленника носят колебательный характер:

$$i(t) = i_0\left(1 + a\sin(\omega t)\right). \qquad (17)$$

На рисунке 13 показана зависимость объема конфиденциальной информации от времени при частоте $\omega = \frac{\pi}{6}$ и различных значениях параметра a ($i_0 = 0{,}1; f_0 = 1; x_0 = 0$).

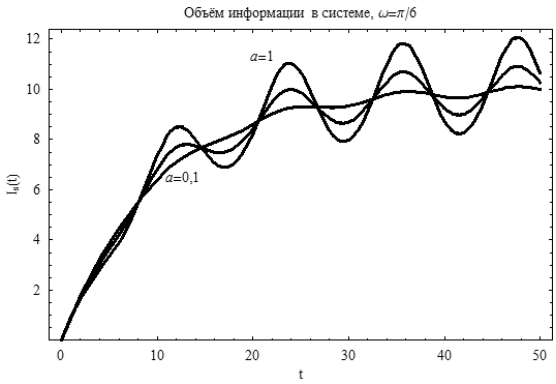

Рис. 13. Зависимость объема конфиденциальной информации от времени при разных значениях глубины модуляции a. Поток данных постоянный. Кривые с $a = 1$ и с $a = 0{,}1$ подписаны. Кривая с $a = 0{,}5$ не подписана и лежит между ними

Из рисунка 13 видно, что колебания объема конфиденциальной информации в системе происходят относительно той же кривой роста, которая возможна при постоянной величине доли потерь, причем внешне рисунки 13 и 10 похожи, хотя на рис.10 колебательный характер имеет не доля потерь, а объем поступающей конфиденциальной информации. С увеличением числа периодов амплитуда колебаний возрастает.

На рис. 14 показана зависимость объема конфиденциальной информации от времени при глубине модуляции $a = 0{,}5$ и различных значениях частоты $\omega = \frac{\pi}{12}; \frac{\pi}{6}; \frac{\pi}{3}$.

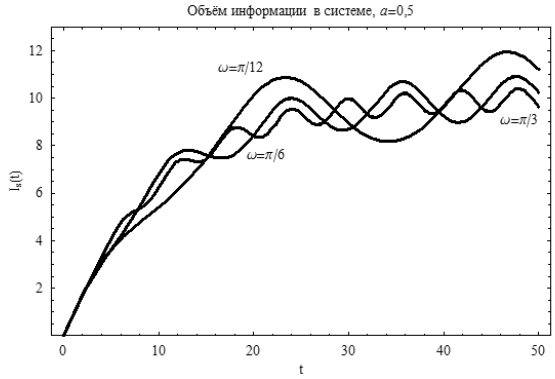

Рисунок 14. Зависимость объема конфиденциальной информации от времени при разных значениях частоты $\omega = \frac{\pi}{12}; \frac{\pi}{6}; \frac{\pi}{3}$. Поток данных постоянный

Как и следовало ожидать, рисунок 14 аналогичен рисунку 11. При уменьшении частоты размах колебаний увеличивается.

На рисунке 15 показана зависимость относительного объема конфиденциальной информации от времени. Это отношение конфиденциальной информации в системе к поступившей к этому моменту времени всей конфиденциальной информации.

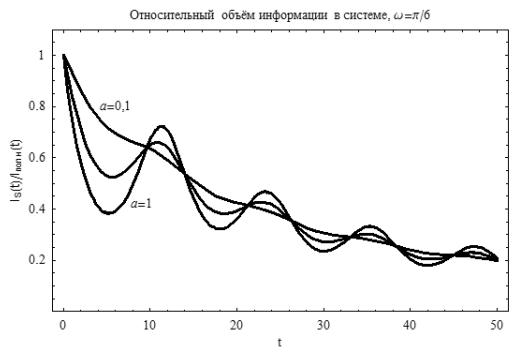

Рис. 15. Зависимость относительного объема конфиденциальной информации в системе от времени при разных значениях глубины модуляции a. Поток данных постоянный. Кривые с $a = 1$ и с $a = 0{,}1$ подписаны. Кривая с $a = 0{,}5$ не подписана и лежит между ними

Кривые в целом отражают зависимость, показанную на рис. 12. Следует отметить, что абсолютные величины максимумов и провалов (минимумов) уменьшаются со временем.

6. Поток информации постоянный, но первоначальный объем существенно превосходит поступления

Кратко рассмотрим случай, когда первоначальный объем конфиденциальной информации существенно отличается от нуля ($x_0 = 10$).

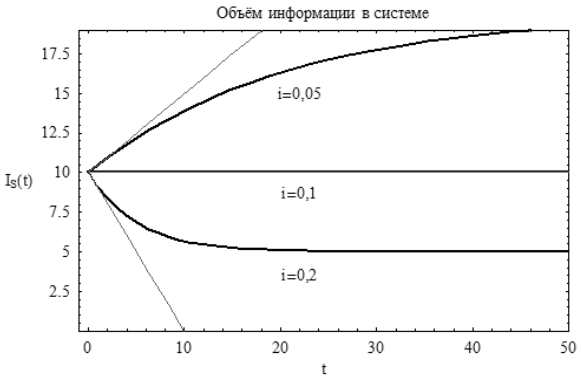

Рис. 16

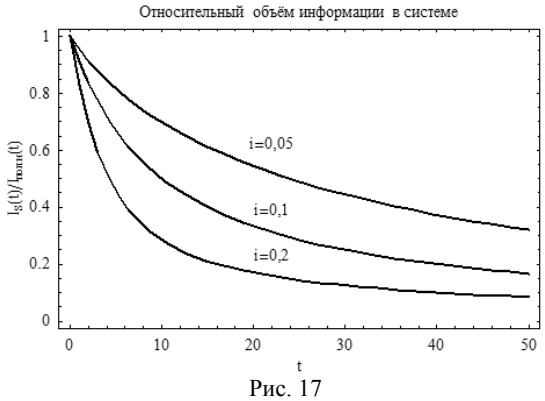

Рис. 17

Зависимость объема конфиденциальной информации от времени в случае значительного объема первоначальной информации. Рис.16 – абсолютные значения, рис. 17 – относительные

7. Поток информации постоянный, но доля потерь зависит от объема хранимой информации

Рассмотрим случай, когда доля потерь зависит от текущего объема конфиденциальной информации. Тогда формула (2) преобразуется к виду:

$$I'_s(t) = -\alpha \frac{(I_s(t))^2}{I_0 + \int_{t_0}^{t} f(t)\,dt} + f(t) \cdot \qquad (18)$$

Этот случай соответствует ситуации, когда уже фактически рассекреченная информация продолжает храниться как конфиденциальная, а злоумышленник не знает об этом.

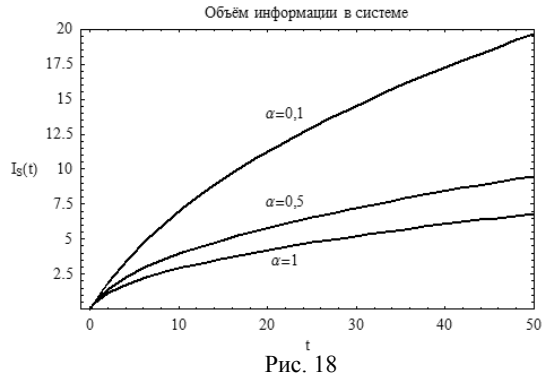

Рис. 18

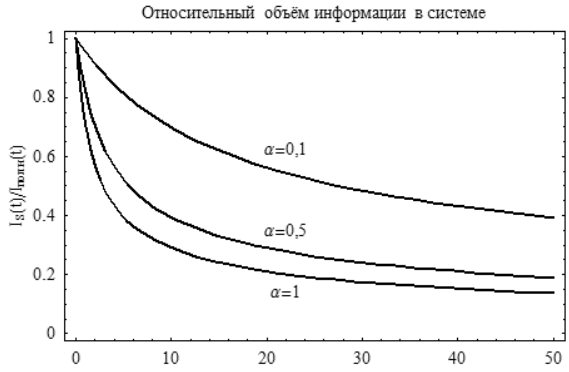

Рис. 19

Зависимость объема конфиденциальной информации от времени в случае, когда доля потерь зависит от объема информации. Рис. 18 – абсолютные значения, рис. 19 – относительные.

На рис. 18 и 19 показаны временные зависимости абсолютного и относительного объемов информации. Если сравнить эти рисунки с рисунками 2 и 3, то видно значительное улучшение показателей. По-видимому, такой способ защиты данных является достаточно эффективным.

Заключение

Таким образом, в настоящей работе авторами был исследован процесс хранения и передачи конфиденциальных данных в информационной системе, получен ряд математических моделей, описывающих данную процедуру.

Использование описанных моделей позволяет экспертам получить оценку объема конфиденциальных данных в информационной системе, что является одним из главных критериев, применяемых при оценке рисков потери конфиденциальной информации.

Литература

1. Лебедева, Т.В. Риски : оценка и управление рисками // Вестник Российского нового университета. – 2010. – Выпуск 3. – С. 64–66.

2. Крюковский, А.С., Лебедева, Т.В. Оценка информационных рисков и экспертный анализ // Сборник научных трудов по материалам международной научно-практической конференции «Современные направления теоретических и прикладных исследований» – Одесса – 2011. – Том 3.– С. 18–21.

3. Крюковский, А.С., Лебедева, Т. В. Методики оценки стоимости конфиденциальной информации и экспертный анализ // Материалы Всероссийской конференции студентов и молодых ученых с международным участием «Молодежная наука в развитии регионов» – Пермь : Березниковский филиал ПГТУ, 2011. – С. 38–41.

4. Крюковский, А.С., Лебедева, Т.В. Математическая модель процессов хранения, передачи и потери конфиденциальной информации //Вестник Марийского государственного технического университета. Серия «Радиотехнические и инфокоммуникационные системы» – Йошкар-Ола : МарГТУ. – 2012. – № 1 (14). – С. 25–36.