

УДК 621.34

С.Г. Семенов, В.В. Босько, И.А. Березюк

*Национальный технический университет «ХПИ», Харьков**Кировоградский национальный технический университет, Кировоград*

МОДЕЛЬ СПЕЦИАЛЬНОЙ ФУНКЦИИ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Проанализирована динамическая модель защищенной информационно-телекоммуникационной системы. Выявлены характерные особенности ее функционирования. Проведено моделирование специальной функции оценки защищенности информационно-телекоммуникационной системы. Сформированы одномерные фазовые портреты информационного трафика различных телекоммуникационных услуг. Проведены исследования зависимости специальной функции (квазипотенциала) от значений интенсивности входного потока данных. Выявлены достоинства и недостатки смоделированной специальной функции.

Ключевые слова: защищенность информационно-телекоммуникационной системы, экспоненциальная устойчивость, квазипотенциал, функция Ляпунова.

Постановка проблемы

В современных условиях интенсификации и глобализации информационных отношений существует необходимость усовершенствования существующих и создания новых (региональных, государственных) информационно-телекоммуникационных систем (ИТС). В то же время решение поставленных задач без эффективных механизмов защиты информации не представляется возможным. Высокая эффективность систем защиты информации может быть обеспечена только при условии оптимизации их структурных и функциональных характеристик, которая в свою очередь невозможна без предварительного решения задачи структурной идентификации. Особенно важной данная задача представляется в условиях априорной неопределенности внешних воздействий вызывающих деструктивные изменения внутренних характеристик ИТС.

Анализ литературы показал, что в настоящее время существует ряд подходов математического моделирования сложных технических систем [1 – 8]. В том числе систем, характеризующихся априорной неопределенностью некоторых структурных и функциональных характеристик [5]. Однако большинство этих математических моделей имеют обобщенный характер, кроме того в них отсутствуют математические показатели, которые могли бы определить защищенность ИТС от внешних воздействий.

В этом контексте конструирование функции, позволяющей оценить уровень защищенности ИТС, а также ее исследование в условиях внешних воздействий является актуальной научной задачей.

Основная часть

В работ [5] предложена математическая модель защищенной ИТС, учитывающая влияние

входного сигнала, внешних воздействий, малых внутренних возмущений и ошибок измерения параметров на выходные характеристики исследуемой системы. В рассмотренной модели свойства защищенности ИТС к внешним воздействиям можно исследовать на примере следующей системы:

$$\dot{\bar{x}}(t) = A(t)x(t) + B(t)u(t) + E(t)\chi(t), \quad (1)$$

$$y(t) = C(t)x(t) + D(t)u(t) + E(t)\chi(t) + \zeta(t), \quad (2)$$

$$x(t_0) = x_0, \quad (3)$$

где $\bar{x}(t) \in \bar{X}$ – измеряемый m -мерный вектор координат состояния системы, $x(t) \in X$ – m -мерный вектор координат состояния системы, $u(t) \in U$ – k -мерный вектор управления, $A(t)$, $B(t)$, $E(t)$, $C(t)$, $D(t)$, $\zeta(t)$ – непрерывные матрицы ненаблюдаемых ошибок измерения, $\chi(t)$ – m -мерный вектор неконтролируемых внешних воздействий. При этом влияние внешних воздействий, а также изменений, вызванных этими воздействиями можно исследовать с помощью функции чувствительности:

$$\dot{\chi}_j = E(t)\chi_j, \quad (j=1, \dots, J) \quad (4)$$

где функция χ_j оценивается как $\chi_j = \frac{\partial x}{\partial p_{внj}}$, а

$p_{внj}$ – параметр чувствительности системы к внешним воздействиям.

Проведенный анализ динамической модели исследуемой технической системы показал, что при решении системы уравнений 1-3 одной из наиболее сложных задач является задача определения и математического описания процессов, протекающих внутри системы (описание состояния системы). Данная задача заключается в определении передаточных функций $f_1(Z_1, Z_2, \dots, Z_n)$, характеризующей внутреннее состояние, и $f_2(Z_1, Z_2, \dots, Z_n)$ описывающей

взаимовлияние внутренних характеристик системы (Z_1, Z_2, \dots, Z_n – внутренние параметры системы).

Проведенные исследования показали, что в настоящее время существует множество подходов для определения и описания передаточных функций. Одним из наиболее распространенных, является подход, основанный на теории фазового пространства.

Исследования фазовых портретов информационно-технических систем показали, что большинство из них представляют собой набор траекторий заключенных в определенной области. Границы этой области фазового портрета изменяются в зависимости от начальных условий и режимов функционирования системы. На рис. 1 приведен пример одномерного фазового портрета подсистемы информационного обмена ИТС, на котором в качестве параметра, определяющей состояние системы выступает интенсивность входного потока информации $I_{вх}$.

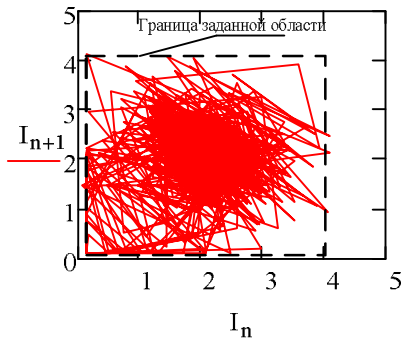


Рис. 1. Одномерный фазовый портрет подсистемы информационного обмена ИТС

Рассмотрим систему 1-3 с учетом того, что в стационарном состоянии Y является инвариантным вектором выходных координат системы $y(t)$ ($y(t) \in Y, Y \subset R^{n \times n}$). Пусть вектор выходных состояний Y является экспоненциально устойчивым (Э-устойчивым) (инвариантный вектор Y называется экспоненциально устойчивым для системы (1-3) в окрестности \tilde{Y} , если при некоторых $K > 0, \ell > 0$ для всех $t \geq 0$ выполняется условие $\|\Delta(y(t))\| \leq Ke^{-\ell t} \|\Delta(y_0)\|$, где $y(t)$ – решение системы 1-3 начальным условием $y(0) = y_0 \in \tilde{Y}$ [5]). С целью упрощения математического описания системы 1-3 в процессе исследования чувствительности вектора Y к изменениям управляющего воздействия U и неуправляемым деструктивным внешним возмущениям χ , трансформируем ее в систему дифференциальных уравнений Ито [7]:

$$dy = f(y)dt + a\sigma(y)dv(t), \quad (5)$$

где $v(t)$ – n - мерный винеровский процесс, $\sigma(y)$ – $n \times n$ -матричная функция, задающая зависимость возмущений от состояния защищенности системы, a – параметр интенсивности возмущений.

В результате действия неконтролируемых внешних возмущений ($\chi(t)|_{M \neq 0}$) случайные траектории системы покидают заранее известное положение (область пространства), определяемое вектором Y и формируют вокруг или около него некоторую структуру. На практике очень часто возникает задача оценки отклонения траектории системы от заданного пространства (области) с целью определения устойчивости и чувствительности системы к внешним воздействиям. Анализ работ [2, 8] и проведенные исследования показали, что для решения данной задачи, а также нахождения асимптотики ряда стохастических характеристик выхода $y(t)$ из установившегося режима (сформированной траектории) целесообразно использовать специально конструируемую функцию, называемую квазипотенциалом.

Рассмотрим асимптотику стационарной плотности распределения случайных траекторий системы (5) вокруг вектора Y . Для малых воздействий эта асимптотика имеет вид [2, 8]

$$\rho(y, a) \approx Ke^{\left(-\frac{\varpi(y)}{a^2}\right)}, \quad (6)$$

где $\varpi(y) = -\lim_{a \rightarrow 0} a^2 \ln \rho(y, a)$ – квазипотенциал.

Определение 1. Функция $\varpi(y)$ называется Y -квадратичной, если при некоторых $k_1 > 0, k_2 > 0$ для всех $y \in \tilde{Y}$ выполняется неравенство [5]:

$$k_1 \|\Delta(y)\|^2 \leq \varpi(y) \leq k_2 \|\Delta(y)\|^2, \quad (7)$$

где $\|\bullet\|$ – евклидова норма.

Проведенные исследования [2-4, 8] показали, что если функции $\varpi(y)$ является Y -квадратичной, то для экспоненциальной устойчивости вектора выходного сигнала защищенной ИТС Y (системы (5)) в окрестности \tilde{Y} необходимо существование некоторой Y -квадратичной функции $\omega(y)$ такой, что

$$L\varpi(y) = -\omega(y), \quad (8)$$

где

$$L\varpi(y) = \left(f(y), \frac{\partial \varpi}{\partial y}(y) \right) + \frac{1}{2} \sum_r \left(\sigma_r(y), \frac{\partial^2 \varpi}{\partial y^2}(y) \sigma_r(y) \right). \quad (9)$$

Утверждение 1. Свойство защищенности системы от ряда внешних злоумышленных воздействий может вытекать из свойства экспоненциальной устойчивости вектора Y системы (5) в случае, когда окрестность \tilde{Y} вектора Y не превышает допустимого размера $\tilde{Y}_{доп}$.

Исходя из вышеперечисленных факторов, сформулируем следующую теорему.

Теорема 1. Если квазипотенциал $\varpi(y)$ в окрестности \tilde{Y} вектора Y является Y -квадратичной функцией Ляпунова, и вектор Y является экспонен-

циально-устойчивым, то с помощью функции $\varpi(y)$ можно установить состояние защищенности системы.

Доказательство. Пусть функция $\varpi(y)$ является решением уравнения Гамильтона-Якоби [3]. Тогда в соответствии с (10) квазипотенциал $\varpi(y)$ удовлетворяет соотношению:

$$\left(f(y), \frac{\partial \varpi}{\partial y} \right) = -\omega(y), \quad (10)$$

$$\text{где } \omega(y) = \frac{1}{2} \left(\frac{\partial \varpi}{\partial y}, \sigma(y) \sigma^T(y) \frac{\partial \varpi}{\partial y} \right)$$

Исходя из свойств уравнения Гамильтона-Якоби [3], функция $\omega(y)$ также как и $\varpi(y)$ является квадратичной, что доказывает экспоненциальную устойчивость вектора \dot{Y} . Экспоненциальная устойчивость вектора \dot{Y} дает основания использования приведенных выше предположений для исследования и оценки защищенности ИТС. Исходя из определения 1, существует зависимость размера окрестности \tilde{Y} от функции $\varpi(y)$, т.е. в случае злоумышленных либо иных внешних воздействий, когда окрестность \tilde{Y} вектора Y превысит допустимый размер $\tilde{Y}_{\text{доп}}$, функция $\varpi(y)$ так же превысит допустимые границы функционирования. И это изменение функции $\varpi(y)$ может дать основание для принятия решения о возникающих деструктивных внешних воздействиях. Таким образом, приведенные факторы доказывают возможность функции $\varpi(y)$ определять состояние защищенности системы.

Используем представленный выше подход динамического моделирования технических систем с

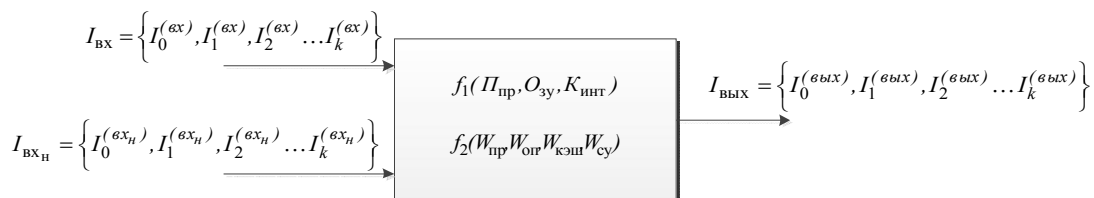


Рис. 2. Структурная схема математической модели подсистемы информационного обмена защищенной ИТС

Проведем исследования и оценим возможности квазипотенциала $\varpi(y)$ в определении защищенности информационно-телекоммуникационной системы, упрощенная структура которой представлена на рис. 3.

Одномерные фазовые портреты информационного трафика различных телекоммуникационных услуг (*torrent*-услуг, *IP*-телефонии, потокового видео) представлены на рис. 4. Следует заметить, что рис 4 (а) иллюстрирует загрузку сетевой карты системы в защищенном режиме (установленные средства защиты позволяют нейтрализовать *Dos*-атаки).

Рис. 4 (б, в) иллюстрирует загрузку сетевой карты в условиях злоумышленных внешних воздействий (*Dos*-атак) частично (рис. 4 (б)) или полностью (рис. 4 (в)) достигших своей цели.

несколькими входами для математического моделирования защищенной ИТС. Исходя из указанных выше ограничений, представим вектор $u(t)$ управляющих воздействий подсистемы в виде массива данных интенсивности входного информационного потока $I_{\text{BX}} = \{I_0^{(\text{BX})}, I_1^{(\text{BX})}, I_2^{(\text{BX})}, \dots, I_k^{(\text{BX})}\}$, а вектор неконтролируемых входных возмущений в виде множества $I_{\text{BXH}} = \{I_0^{(\text{BXH})}, I_1^{(\text{BXH})}, I_2^{(\text{BXH})}, \dots, I_k^{(\text{BXH})}\}$.

При математическом представлении внутреннего состояния системы ($x(t)$) необходимо учитывать факт ее разбиения на множества Q_1 – статических и Q_2 – динамических характеристик. При этом вектор $x(t)$ может ассоциироваться с такими параметрами как производительность процессора $P_{\text{пр}}$, максимальный объем запоминающего устройства $O_{\text{з}}$, количество входных/выходных интерфейсов $K_{\text{инт}}$ и др. (для множества Q_1), или загрузка процессора $W_{\text{пр}}$, оперативной памяти $W_{\text{оп}}$ и КЭШа $W_{\text{кэш}}$, сетевого устройства W_{cy} и др. (для множества Q_2). Вектор выходных характеристик $y(t)$ подсистемы информационного обмена защищенной ИТС чаще всего представляется в виде массива данных интенсивности выходного информационного потока $I_{\text{ВЫХ}} = \{I_0^{(\text{ВЫХ})}, I_1^{(\text{ВЫХ})}, I_2^{(\text{ВЫХ})}, \dots, I_k^{(\text{ВЫХ})}\}$.

С учетом вышеизложенного упрощенную структурную схему математической модели подсистемы информационного обмена защищенной ИТС можно представить в виде рис. 2.

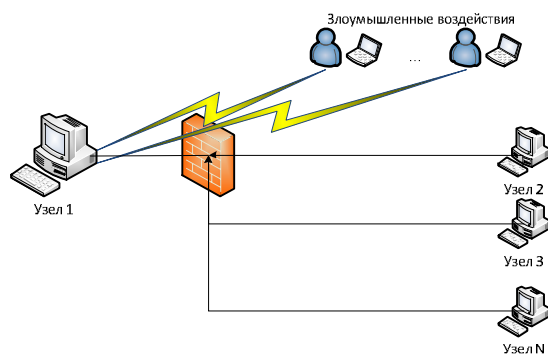


Рис. 3. Упрощенная структура ИТС моделирования

В качестве вектора выходных координат $y(t)$ в рассматриваемом примере выступает множество

значений интенсивности входного потока информации I_1, I_2, I_3 . Как видно из рис. 4 фазовый портрет трафика данных, поступающего в защищенную ин-

формационно-телекоммуникационную систему представляет собой хаотическую структуру, заключенную в некоторой области пространства.

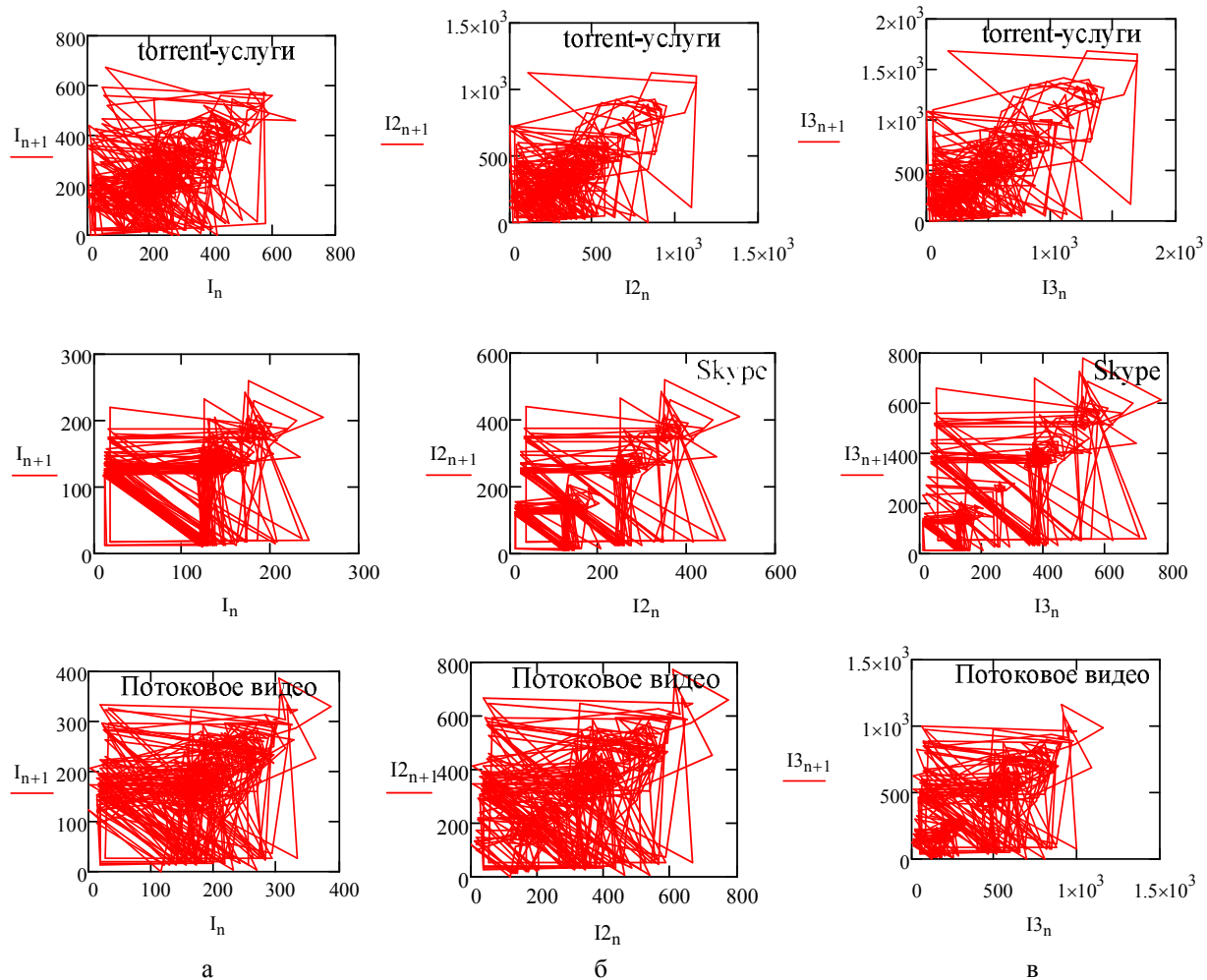


Рис. 4. Одномерные фазовые портреты информационного трафика различных телекоммуникационных услуг

В случае внешних злоумышленных воздействий траектория движения точек с координатами I_2, I_2, I_{2+1} (I_3, I_{3+1}) претерпевает определенных изменений и покидает заданную изначально область пространства. Оценку изменений, происходящих в фазовом портрете вектора выходных координат, проведем с помощью заданной в выражении 6 функции $\varpi(y)$.

На рис. 5. представлены графики зависимости квазипотенциала от значений интенсивности входного потока данных ($\varpi(I_1, I_2, I_3)$) в узел 1 (см. рис. 3) различных сетевых протоколов (*HTTP, Skype, RTCP*) в условиях злоумышленных воздействий (*Dos-атаки*) с нескольких направлений соответственно (интенсивность атаки во всех трех практических случаях одинакова). Кривая 1 графиков рис. 5 (а, б, в) является иллюстрацией квазипотенциала $\varpi(I)$, характеризующего функционирование защищенной системы (атака не достигает своего результата). Кривая 2 графиков иллюстрирует поведение

функции $\varpi(I_2)$, в условиях, когда злоумышленные атаки на информационно-телекоммуникационную систему достигли своего результата с двух направлений. Кривая 3 графиков иллюстрирует ситуацию, когда *Dos-атаки* на информационно-телекоммуникационную систему сразу с трех направлений достигли своего результата.

Как видно из рис. 5 в нормальном режиме функционирования (*Dos-атаки* не достигли результата) квазипотенциал $\varpi(I_1, I_2, I_3)$ в области определений $I \rightarrow 0$ имеет максимальные значения для всех без исключения практических случаев поступления информационного трафика. В то же время аномальное воздействие на информационно-телекоммуникационную систему *Dos-атаки* приводит к снижению значений квазипотенциала в области $I_1, I_2, I_3 \rightarrow 0$ до 1,4 раза в случае обеспечения телекоммуникационных услуг по протоколу *HTTP*, до 2 раз при информационном обмене по протоколу *Skype*, и до 1,7 раза в случае использования протокола *RTCP*.

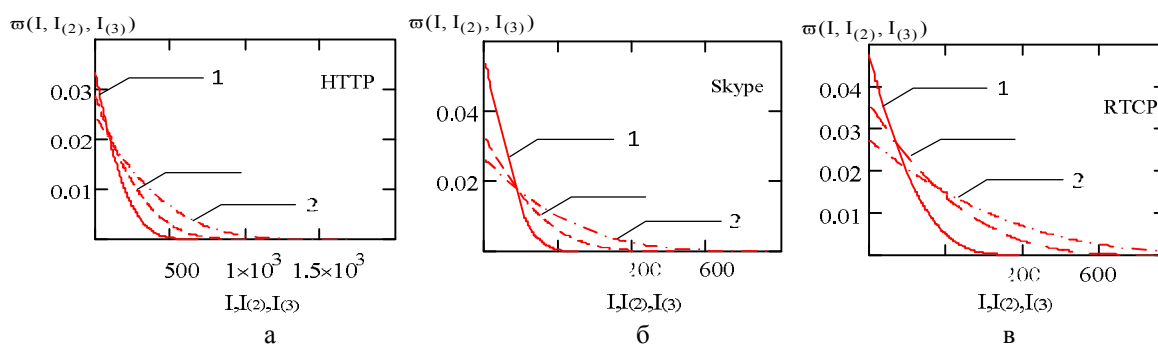


Рис 5. Графики зависимости квазипотенциала от значений интенсивности входного потока данных

Следует заметить, что квазипотенциал $\varpi(I, I_{(2)}, I_{(3)})$ может оценивать уровень защищенности информационно-телекоммуникационной системы не только в области $I, I_{(2)}, I_{(3)} \rightarrow 0$, но и на остальном интервале исследуемой области интенсивности входных данных. Так при снижении уровня защищенности информационно-телекоммуникационной системы функция $\varpi(I, I_{(2)}, I_{(3)})$ замедляет спад своих значений. Это в конечном итоге приводит к тому, что в незащищенных информационно-телекоммуникационных системах значения функции $\varpi(I, I_{(2)}, I_{(3)})$ стремятся к нулю при интенсивностях $I_{(3)} > I_{(2)} > I$.

Выводы

Таким образом, в результате математического моделирования на основе функции-квазипотенциала была сконструирована специальная функция оценки защищенности ИТС. Анализ и исследования данной функции на примере информационного обмена в ИТС в условиях Dos-атаки показали, что ее использование позволяет оценить границы фазового портрета системы, и сигнализировать об отклонении текущих траекторий от установленных границ. Среди недостатков данной функции следует отметить низкую ее чувствительность при оценке защищенности в случае воздействия атак, интенсивность которых значительно ниже интенсивности входного потока данных.

МОДЕЛЬ СПЕЦІАЛЬНОЇ ФУНКЦІЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

С.Г. Семенов, В.В. Босько, І.А. Березюк

Проаналізована динамічна модель захищеної інформаційно-телекомунікаційної системи. Виявлені характерні особливості її функціонування. Проведено моделювання спеціальної функції оцінки захищеності інформаційно-телекомунікаційної системи. Сформовані одновимірні фазові портрети інформаційного трафіка різних телекомунікаційних послуг. Проведені дослідження залежності спеціальної функції (квазіпотенціалу) від значень інтенсивності вхідного потоку даних. Виявлені достоїнства і недоліки змодельованої спеціальної функції.

Ключові слова: захищеність інформаційно-телекомунікаційної системи, експоненціальна стійкість, квазіпотенціал, функція Ляпунова.

MODEL OF THE SPECIAL FUNCTION OF INFOTELECOMMUNICATION SYSTEMS PROTECTED ESTIMATION

S.G. Semenov, V.V. Bos'ko, I.A. Berezyuk

The dynamic model of the protected informatively-telecommunication system is analysed. The characteristic features of its functioning are exposed. The design of the special function of estimation of protected of the informatively-telecommunication system is conducted. The unidimensional phase portraits of informative traffic of different telecommunication services are formed. Researches of dependence of the special function (quasi-potential) are conducted from the values of intensity of input stream of information. Dignities and lacks of the modelled special function are exposed.

Keywords: protected of the informatively-telecommunication system, exponential stability, quasi-potential, Lyapunov function.

Список литературы

1. Васильев К.К. Математическое моделирование систем связи : учебное пособие / К.К. Васильев, М.Н. Служивый. – Ульяновск: УлГТУ, 2008. – 170 с.
2. Вентцель А.Д. Флуктуации в динамических системах под действием малых случайных возмущений / А.Д. Вентцель, М.И. Фрейдлин. – М.: Наука, 1979. – 424 с.
3. Парс Л.А. Аналитическая динамика / Л.А. Парс // М.: Наука, 1971. – 636 с.
4. Ряшко Л.Б. Об управлении стохастической чувствительностью [Электронный ресурс] / Л.Б. Ряшко, И.А. Баширцева // Автоматика и телемеханика. – 2008. – № 7. – С. 78-89. – Режим доступа: <http://www.mathnet.ru/links/113b65d94e32bfed567fb0649acee0bc/at688.pdf>.
5. Семенов С.Г. Структурно-информационный портрет информационной системы в условиях неопределенности на примере Dos-атаки / С.Г. Семенов // Всеукраинский межведомственный научно-технический сборник «Радиотехника» Тематичний випуск: Інформаційна безпека. – Х.: ХНУРЕ, 2011. – № 166. – С. 99-106.
6. Томович Р. Общая теория чувствительности / Р. Томович, М. Вукобратович. – М.: Сов. радио, 1972. – 240 с.
7. Arnold L. Stochastic Differential Equations: Theory and Applications / L. Arnold. – New York: Wiley, 1974. – 228 p.
8. Day M.V. Regularity of boundary quasi-potentials for planar systems / M.V. Day // Appl. Mathematics and Optimization. – 1994. – V. 30. – P. 79.

Поступила в редколлегию 12.12.2012

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет им. Ю. Кондратюка, Полтава.