Xodjabekov Muradjon Usarovich (Samarqand davlat Arxitektura-qurilish universiteti;
E-mail: uzedu@inbox.ru),
Qudratov Anvar Ergashevich (Samarqand davlat Pedagogika instituti; a_qudratov1985@mail.ru)

ELASTIK DISSIPATIV XARAKTERISTIKALI STERJEN VA DINAMIK SO‘NDIRGICHLARNING BIRGALIKDAGI TEBRANISHLARI USTUVORLIGI

Annotatsiya. *Ushbu ishda elastik dissipativ xarakteristikali sterjen va chiziqli elastik xarakteristikali dinamik so‘ndirgichlarning birgalikdagi ko‘ndalang tebranishlari ustuvorligi Lyapunovning birinchi yaqinlashish usuli yordamida tekshirilgan. Xususan, mexanik yo‘qotish koeffitsiyentining o‘zgarishi bilan ustuvorlik shartlarining o‘zgarishi tahlil qilingan va tavsiyalar berilgan.*

Kalit so‘lar*: elastik dissipativ sistema, gisterezis, sterjen, tebranish,*

ПРИОРИТЕТНОСТЬ СОВМЕСТНЫХ КОЛЕБАНИЙ УПРУГО-ДИССИПАТИВНОГО СТЕРЖНЯ И ДИНАМИЧЕСКИХ ГАСИТЕЛЕЙ КОЛЕБАНИЙ

Аннотация. *В данной работе методом первого приближения Ляпунова исследована устойчивость совместных поперечных колебаний стержня с упруго-диссипативной характеристикой и динамического гасителя с линейно-упругой характеристикой. Условия устойчивости определены в аналитическом виде в зависимости от параметров системы, и для них проведен численный анализ в частности, исследовано влияние изменения коэффициента механических потерь на условия устойчивости, а также представлены соответствующие рекомендации.*

Ключевые слова. *упруго-диссипативная система, гистерезис, стержень, колебания, динамический гаситель.*

PRIORITY ANALYSIS OF THE JOINT VIBRATIONS OF AN ELASTIC-DISSIPATIVE ROD AND DYNAMIC DAMPERS

Annotation. *This study investigates the stability of coupled transverse vibrations of a beam with elastic-dissipative characteristics and a dynamic absorber with linear elastic characteristics using Lyapunov's first approximation method. Stability conditions are obtained analytically as functions of the system parameters and analyzed numerically. In particular, the influence of variations in the mechanical loss coefficient on the stability conditions is examined, and corresponding recommendations are provided.*

Keywords. *elastic-dissipative system, hysteresis, beam, vibrations, dynamic absorber.*

Kirish. Texnika va qurilish sohalarida egiluvchan sterjen (balka)lar tipidagi ko‘plab elementlardan foydalaniladi. Shuning uchun turli tashqi yuklamalar ta’sirida balkalarning tebranma harakatlarini o‘rganish, zararli tebranishlarini pasaytirish dolzarb masalalardan hisoblanadi. [1] ishda ikkita dinamik so‘ndirgich o‘rnatilgan, sterjen uchlaridan simmetrik joylashtirilgan sterjenlarning tebranishlari bo‘yicha eks-perimental tadqiqotlar va taqqoslovchi tahlillar olib borilgan. [2] ishda energiyaning gisterezisli tarqalishi mavjud bo‘lgan sterjenning ko‘ndalang tebranishlarining ustuvorligi masalasi ko‘rib chiqilgan. [3] ishda sterjen va gisterezis tipidagi elastik-dissipativ xossalarga ega dinamik so‘ndirgichdan iborat sistema dinamikasi tahlil qilingan.

Materiallar va metodlar. Elastik dissipativ xarakteristikali sterjen va chiziqli elastik xarakteristikali dinamik so‘ndirgichlarning birgalikdagi ko‘ndalang tebranishlari harakat differensial tenglamalar sistemasi [4]ning xususiy holi ko‘rinishida quyidagicha ifodalanadi:

$$\ddot{q}_i + (1 + j\eta_c)p_i^2 q_i - \mu_1\mu_{0i}n_1^2 u_{i1}\zeta_1 - \mu_2\mu_{0i}n_2^2 u_{i2}\zeta_2 = -d_i W_0;$$
$$u_{i1}\ddot{q}_i + \ddot{\zeta}_1 + n_1^2\zeta_1 = -W_0;\ \ u_{i2}\ddot{q}_i + \ddot{\zeta}_2 + n_2^2\zeta_2 = -W_0, \qquad (1)$$

bu yerda: $q_i = q_i(t)$ – vaqtning funksiyasi; $j^2 = -1$; η_c – sterjen materialining mexanik yo‘qotish koeffitsiyenti; p_i– sterjenning xususiy chastotasi; $\mu_1 = \frac{m_1}{m_c}$; $\mu_2 = \frac{m_2}{m_c}$; $\mu_{0i} = \frac{l}{d_{2i}}$; $d_i = \frac{d_{1i}}{d_{2i}}$; $d_{1i} = \int_0^l u_i dx$; $d_{2i} = \int_0^l u_i^2 dx$; $m_c = \rho F l$ – sterjenning massasi; ρ, F–mos ravishda, seterjen materialining zichligi va ko‘ndalang kesimi yuzi; l – sterjenning uzunligi; m_1, m_2 – dinamik so‘ndirgichlar massalari; $u_i(x)$ – sterjen xususiy tebranishlari formalari; W_0–asosning tezlanishi; $u_{i1} = u_i(x_1)$; $u_{i2} = u_i(x_2)$; x_1, x_2–dinamik so‘ndirgichlar o‘rnatilgan nuqtalar; $n_1 = \sqrt{\frac{c_1}{m_1}}$ va $n_2 = \sqrt{\frac{c_2}{m_2}}$ – dinamik so‘ndirgichlarning xususiy chastotalari; c_1, c_2 – dinamik so‘ndirgichlar elastik elementlarining bikrlik koeffitsiyentlari; ζ_1, ζ_2– sterjenga nisbatan dinamik so‘ndirgichlarning ko‘chishlari.

Qaralayotgan elastik dissipativ xarakteristikali sterjen va chiziqli elastik xarakteristikali dinamik so‘ndirgichlarning birgalikdagi ko‘ndalang tebranishlari ustuvorligini tekshirish maqsadida, garmonik qo‘zg‘alishlar uchun asosning tezlanishini quyidagicha olamiz:

$$W_0 = w_0 \cos \omega t, \quad (2)$$

bu yerda w_0 –asos tezlanishinig amplitudaviy qiymati bo‘lib, $w_0 \ll 1$; ω – chastota. (1) harakat differensial tenglamar sistemasining yechimlarini quyidagicha izlaymiz:

$$q_i = a_i \cos(\omega t + \theta_i), \zeta_1 = a_{1*} \cos(\omega t + \theta_{1*}); \quad \zeta_2 = a_{2*} \cos(\omega t + \theta_{2*}) \quad (3)$$

bu yerda $a_i, \theta_i, a_{1*}, \theta_{1*}, a_{2*}\theta_{2*}$-lar amplituda va fazalar sekin o‘zgaruvchan funksiyalar [5;8–10-b.]. (3) yechimlardan tegishli hosilalarni hisoblab, (1) harakat differensiyal tenglamar sistemasiga qo‘ysak hamda (2) asosning tezlanishi ifodasini hisobga olsak, u holda (1) harakat differensiyal tenglamalar sistemasiga mos keluvchi normal ko‘rinishdagi tenglamalar sistemasini olamiz:

$$\begin{aligned}
\dot{a}_i &= -\frac{1}{2\omega}\left[-d_i w_0 \sin\theta_i + \eta_c p_i^2 a_i - \mu_1\mu_{0i} n_1^2 u_{i1} a_{1*} \sin\varphi_1 - - \mu_2\mu_{0i} n_2^2 u_{i2} a_{2*} \sin\varphi_2\right];\\
\dot{\theta}_i &= -\frac{1}{2\omega a_i}\left[-d_i w_0 \cos\theta_i + \left(\omega^2 - p_i^2\right)a_i + \mu_1\mu_{0i} n_1^2 u_{i1} a_{1*} \cos\varphi_1\right.\\
&\qquad \left. + \mu_2\mu_{0i} n_2^2 u_{i2} a_{2*} \cos\varphi_2\right];\\
\dot{a}_{1*} &= -\frac{1}{2\omega}\left[-(1 - d_i u_{i1}) w_0 \sin\theta_{1*} - u_{i1} a_i p_i^2 (\eta_c \cos\varphi_1 - \sin\varphi_1)\right.\\
&\qquad \left. + \mu_2\mu_{0i} n_2^2 u_{i1} u_{i2} a_{2*} \sin\varphi_3\right]; \qquad (4)\\
\dot{\theta}_{1*} &= -\frac{1}{2\omega a_{1*}}\left[-(1 - d_i u_{i1}) w_0 \cos\theta_{1*} + \left(\omega^2 - n_1^2\left(1 + \mu_1\mu_{0i} u_{i1}^2\right)\right) a_{1*}\right.\\
&\qquad \left. + u_{i1} a_i p_i^2 (\eta_c \sin\varphi_1 + \cos\varphi_1) - \mu_2\mu_{0i} n_2^2 u_{i1} u_{i2} a_{2*} \cos\varphi_3\right];\\
\dot{a}_{2*} &= -\frac{1}{2\omega}\left[-(1 - d_i u_{i2}) w_0 \sin\theta_{2*} - u_{i2} a_i p_i^2 (\eta_c \cos\varphi_2 - \sin\varphi_2)\right.\\
&\qquad \left. - \mu_1\mu_{0i} n_1^2 u_{i1} u_{i2} a_{1*} \sin\varphi_3\right];\\
\dot{\theta}_{2*} &= -\frac{1}{2\omega a_{2*}}\left[-(1 - d_i u_{21}) w_0 \cos\theta_{2*} + \left(\omega^2 - n_2^2\left(1 + \mu_2\mu_{0i} u_{i2}^2\right)\right) a_{2*}\right.\\
&\qquad \left. + u_{i2} a_i p_i^2 (\eta_c \sin\varphi_2 + \cos\varphi_2) - \mu_1\mu_{0i} n_1^2 u_{i1} u_{i2} a_{1*} \cos\varphi_3\right]
\end{aligned}$$

bu yerda $\varphi_1 = \theta_{1*} - \theta_i, \varphi_2 = \theta_{2*} - \theta_i = \varphi_2, \varphi_3 = \theta_{2*} - \theta_{1*}$.

(4) tenglamalar sistemasini variatsiyalab, qo‘zg‘atilgan harakat differensial tenglamalar sistemasiga ega bo‘lamiz. Qo‘zg‘atilgan harakat differensial tenglamalar sistemasining yechimini quyidagicha olamiz:

$$\delta a_i = h_1 e^{\lambda_1 t}; \ \delta\theta_i = h_2 e^{\lambda_1 t}; \ \delta a_{1*} = h_3 e^{\lambda_1 t}; \ \delta\theta_{1*} = h_4 e^{\lambda_1 t}; \ \delta a_{2*} = h_5 e^{\lambda_1 t}; \ \delta\theta_{2*} = h_6 e^{\lambda_1 t}, \quad (5)$$

bu yerda $h_1, h_2, h_3, h_4, h_5, h_6$ -lar koeffitsiyentlar; $\lambda = 2\omega\lambda_1$.

(5) yechimlarni (4) sistemaga qo‘yib, noldan farqli yechimga ega bo‘lish shartidan yozamiz. Bundan quyidagi xarakteristik tenglamaga ega bo‘lamiz:

$$\lambda^6 + \Delta_1\lambda^5 + \Delta_2\lambda^4 + \Delta_3\lambda^3 + \Delta_4\lambda^2 + \Delta_5\lambda + \Delta_6 = 0, \quad (6)$$

bu yerda $\Delta_1 = 2p_i^2\eta_c$;

$\Delta_2 = 3\omega^4 - 2\left(p_i^2 + l_1u_{i1} + l_2u_{i2} + n_1^2 + n_2^2\right)\omega^2 + l_1^2u_{i1}^2 + 2u_{i1}\left(p_i^2 + l_2u_{i2} + n_1^2\right)$
$+l_2^2u_{i2}^2 + 2l_2n_2^2u_{i2} + (\eta_c^2 + 1)p_i^4 + n_1^4 + n_2^4$;

$\Delta_3 = 4(\omega^4 - (l_2u_{i2} + n_1^2 + n_2^2)\omega^2 + \frac{1}{2}l_2^2u_{i2}^2 + l_2(l_1u_{i1} + n_2^2)u_{i2} + \frac{1}{2}n_1^4$
$+\frac{1}{2}l_1n_1^2u_{i1} + \frac{1}{2}n_2^4)p_i^2\eta_c$;

$\Delta_4 = 3\omega^8 - 4\left(p_i^2 + l_1u_{i1} + l_2u_{i2} + n_1^2 + n_2^2\right)\omega^6 + (2(\eta_c^2 + 1)p_i^4 +$
$+4\left(p_i^2 + l_1u_{i1} + l_2u_{i2} + n_1^2 + n_2^2\right)p_i^2 + 2(l_1u_{i1} + l_2u_{i2} + n_1^2 + n_2^2)^2)\omega^4 +$
$+(-2(\eta_c^2 + 1)(l_2u_{i2} + n_1^2 + n_2^2)p_i^4 + (-2n_2^4 - 4(l_1u_{i1} + l_2u_{i2})n_2^2 -$
$-8l_1l_2u_{i1}u_{i2} - 2l_1n_1^2u_{i1} - 2l_2^2u_{i2}^2 - 2n_1^4)p_i^2 - 2\left((l_1u_{i1} + n_1^2)n_2^2 + l_2n_1^2u_{i2}\right) \times$
$\times (l_1u_{i1} + l_2u_{i2} + n_1^2 + n_2^2)\omega^2 + 2(\eta_c^2 + 1)(l_1l_2u_{i1}u_{i2} + \frac{1}{2}l_2^2u_{i2}^2 + l_2n_2^2u_{i2} +$
$+\frac{1}{2}n_1^4 + \frac{1}{2}n_2^4)p_i^4 + 2u_{i1}\left(n_2^4 + 2l_2n_2^2u_{i2} + l_2u_{i2}(l_1u_{i1} + l_2u_{i2})\right)p_i^2 +$
$+((l_1u_{i1} + n_1^2)n_2^2 + l_2n_1^2u_{i2})^2$;

$$\Delta_5 = 2\eta_c p_i^2(\omega^8 - 2(l_2u_{i2} + n_1^2 + n_2^2)\omega^6 + (n_1^4 + (l_1u_{i1} + 4l_2u_{i2} + 4n_2^2)n_1^2$$
$$+l_2^2u_{i2}^2 - 2u_{i2}(l_1u_{i1} - n_2^2)l_2 + n_2^4)\omega^4 + 2(l_1u_{i1} + l_2u_{i2} + n_1^2 + n_2^2) \times$$
$$\times \left((-l_2u_{i2} - n_2^2)n_1^2 + l_1l_2u_{i1}u_{i2}\right)\omega^2 - ((l_2u_{i2} + n_2^2)n_1^2 + l_1n_2^2u_{i1}) \times$$
$$\times ((-l_2u_{i2} - n_2^2)n_1^2 + l_1l_2u_{i1}u_{i2}));$$
$$\Delta_6 = \omega^{12} - 2\left(p_i^2 + l_1u_{i1} + l_2u_{i2} + n_1^2 + n_2^2\right)\omega^{10} + ((\eta_c^2 + 1)p_i^4 +$$
$$+(2l_1u_{i1} + 4l_2u_{i2} + 4n_1^2 + 4n_2^2)p_i^2 + n_1^4 + (2l_1u_{i1} + 4l_2u_{i2} + 4n_2^2)n_1^2 +$$
$$+l_2^2u_{i2}^2 + 2u_{i2}(l_1u_{i1} + n_2^2)l_2 + l_1^2u_{i1}^2 + 4u_{i1}n_2^2l_1 + n_2^4)\omega^8 + (-2(\eta_c^2 + 1) \times$$
$$\times (l_2u_{i2} + n_1^2 + n_2^2)p_i^4 + (-2n_1^4 + (-2l_1u_{i1} - 8l_2u_{i2} - 8n_2^2)n_1^2 - 4u_{i1}n_2^2l_1$$
$$-2l_2^2u_{i2}^2 - 4l_2n_2^2u_{i2} - 2n_2^4)p_i^2 - 2\left((l_2u_{i2} + n_2^2)n_1^2 + l_1n_2^2u_{i1}\right)(l_1u_{i1} + l_2u_{i2}$$
$$+n_1^2 + n_2^2))\omega^6 + (-2(\eta_c^2 + 1)(-\frac{1}{2}n_1^4 - 2(l_2u_{i2} + n_2^2)n_1^2 - \frac{1}{2}l_2^2u_{i2}^2 +$$
$$+u_{i2}(l_1u_{i1} - n_2^2)l_2 - \frac{1}{2}n_2^4)p_i^4 + (4(l_2u_{i2} + n_2^2)n_1^4 + (4u_{i1}n_2^2l_1 + 4l_2^2u_{i2}^2 +$$
$$+8l_2n_2^2u_{i2} + 4n_2^4)n_1^2 - 2l_1u_{i1}\left(l_1l_2u_{i1}u_{i2} + l_2^2u_{i2}^2 - n_2^4\right))p_i^2 +$$
$$+((l_2u_{i2} + n_2^2)n_1^2 + l_1n_2^2u_{i1})^2)\omega^4 + 2\left((-l_2u_{i2} - n_2^2)n_1^2 + l_1l_2u_{i1}u_{i2}\right)p_i^2 \times$$
$$\times \left((\eta_c^2 + 1)(l_2u_{i2} + n_1^2 + n_2^2)p_i^2 + (l_2u_{i2} + n_2^2)n_1^2 + l_1n_2^2u_{i1}\right)\omega^2 + (\eta_c^2 + 1) \times$$
$$\times \left((-l_2u_{i2} - n_2^2)n_1^2 + l_1l_2u_{i1}u_{i2}\right)^2 p_i^4, \qquad l_1 = \mu_1\mu_{0i}n_1^2u_{i1};\ l_2 = \mu_2\mu_{0i}n_2^2u_{i2}.$$

Natijalar va ularning muhokamasi. Qaralayotgan sistema statsionar tebranishlari ustuvor bo‘lishi uchun (6) xarakteristik tenglama ildizlarining haqiqiy qismi manfiy bo‘lishi yetarli hisoblanadi [6]. Gurvits kriteriyasi yordamida xarakteristik tenglama ildizlarining haqiqiy qismi manfiy bo‘lishini ko‘rsatamiz. Buning uchun dastlab (6) xarakteristik tenglamadan matritsani tuzib olamiz.

Qaralayotgan sistemaning statsionar harakati ustuvor bo‘lishi uchun aniqlangan matritsaning bosh minorlari musbat aniqlangan bo‘lishi shart, shunga asosan, quyidagi ustuvorlik shartlarini hosil qilamiz:

$$\Delta_1 > 0, \quad \Delta_1\Delta_2 - \Delta_3 > 0, \quad -\Delta_1^2\Delta_4 + \Delta_1\Delta_2\Delta_3 + \Delta_1\Delta_5 - \Delta_3^2 > 0 \qquad (7)$$

$$\Delta_1^2\Delta_2\Delta_6 - \Delta_1^2\Delta_4^2 - \Delta_1\Delta_2^2\Delta_5 + \Delta_1\Delta_2\Delta_3\Delta_4 - \Delta_1\Delta_3^2\Delta_6 + 2\Delta_1\Delta_4\Delta_5 + \Delta_2\Delta_3\Delta_5 - \Delta_3^2\Delta_4 - \Delta_5^2 > 0 \qquad (8)$$

$$-\Delta_1^3\Delta_6^2 + 2\Delta_1^2\Delta_2\Delta_5\Delta_6 + \Delta_1^2\Delta_3\Delta_4\Delta_6 - \Delta_1^2\Delta_4^2\Delta_5 - \Delta_1\Delta_2^2\Delta_5^2 - \Delta_1\Delta_2\Delta_3^2\Delta_6 + \Delta_1\Delta_2\Delta_3\Delta_4\Delta_5 -$$
$$-3\Delta_1\Delta_3\Delta_5\Delta_6 + 2\Delta_1\Delta_4\Delta_5^2 + \Delta_3^3\Delta_6 - \Delta_3^2\Delta_4\Delta_5 - \Delta_5^3 > 0 \qquad (10)$$

$$(-\Delta_1^3\Delta_6^2 + 2\Delta_1^2\Delta_2\Delta_5\Delta_6 + \Delta_1^2\Delta_3\Delta_4\Delta_6 - \Delta_1^2\Delta_4^2\Delta_5 - \Delta_1\Delta_2^2\Delta_5^2 - \Delta_1\Delta_2\Delta_3^2\Delta_6 + \Delta_1\Delta_2\Delta_3\Delta_4\Delta_5 -$$
$$-3\Delta_1\Delta_3\Delta_5\Delta_6 + 2\Delta_1\Delta_4\Delta_5^2 + \Delta_2\Delta_3\Delta_5^2 + \Delta_3^3\Delta_6 - \Delta_3^2\Delta_4\Delta_5 - \Delta_5^3)\Delta_6 > 0 \qquad (11)$$

(7) - (11) tengsizliklar gisterezis tipidagi elastik dissipativ xarakteristikali sterjenning ikkita dinamik so‘ndirgichlar bilan statsionar ko‘ndalang tebranishlari ustuvorlik shartlari hisoblanadi. Aniqlangan tengsizliklar yordamida ustuvorlik shartlari va sohalarini qaralayotgan tebranishlardan himoyalanuvchi sterjen va dinamik so‘ndirgich parametrlari bog‘liq holda aniqlash va tahlil qilish mumkin.

Xulosa. Elastik dissipativ xarakteristikali sterjen va dynamik so‘ndirgichlarning birgalikdagi ko‘ndalang tebranishlari ustuvorlik shartlari va chegaralari sistema parametrlariga bog‘liq holda, Lyapunovning birinchi yaqinlashish usuli yordamida analitik ifodalandi hamda sonli tahlil qilinib xulosalar olindi. Mexanik yo‘qotish koeffitsiyentining o‘zgarishi bilan ustuvorlik shartlarining o‘zgarishi tahlil qilindi. Mexanik yo‘qotish koeffitsiyentining pasayishi ustuvorlik shartlarini ifodalovchi funksiyalarning noustuvorlik chegarasiga yaqinlashishini ta’minlaydi va qaralayotgan sistema statsionar tebranishlarining noustuvor bo‘lishiga olib keladi.

Foydalanilgan adabiyotlar ro‘yxati:

(1). Рыжков Л.М. О стационарных поперечных колебаниях стержня с гистерезисным рассеянием энергии. “Проблемы прочности”, № 4, с. 102–105.

(2). Дусматов О.М., Мамзенко Ю.А. Колебания несовершенно упругого стержня с динамическим гасителем при гармонических и случайных воздействиях. Тезисы докладов I научно-технической конференции молодых ученых, специалистов и студентов «Фундаментальные и прикладные проблемы космонавтики». Киев, 1988.

(3). Брискин Е.С. Демпфирование колебаний механических систем динамическими гасителями с полостями, частично заполненными сыпучими средами. “Известия вузов”, Машиностроение. 1980, №2, с. 27–30.
(4). Брискин Е.С. О демпфировании колебаний одной группой динамических гасителей двух близких резонансных состояний механической системы. “Известия вузов”, Строительство и архитектура, 1980, № 12.
(5). Дусматов О.М. Моделирование динамики виброзащитных систем. Ташкент, “Фан”, 1997, 168 с.
(6). Стрелков С.П. Введение в теорию колебаний. Изд. “Наука”, Москва. 1964, 440 с.
(7). Писаренко Г.С., Яковлев А.П., Матвеев В.В. Вибропоглощающие свойства конструкционных материалов: справочник. Киев, “Наукова думка”, 1971, 327 с.
(8).Dusmatov O., Buranov K., Kudratov A. Stability of an Elastic Rod with Dynamic Absorbers under Harmonic Transverse Vibrations. AIP Conference Proceedings. 2025, vol. 3177, 080002.https://doi.org/10.1063/5.0294900
(9). Khodjabekov M.U., Buranov Kh.M., Kudratov A.E. Modal Mass and Stiffness of Hysteresis Type Elastic Dissipative Characteristic Plate. AIP.
(10). Conference Proceedings. 2022, vol. 2637, 050004. https://doi.org/10.1063/5.0118292

Qurbonova Mahzuna Ro‘ziboyevna (Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetining “Axborot xavfsizligi” kafedrasi, “05.01.02-Tizimli tahlil, boshqaruv va axborotlarni qayta ishlash” mutaxassisligi tayanch doktoranti (PhD); E-mail: mahzuna1214@icloud.com)

OCHIQ KALITLI KRIPTOGRAFIK ALGORITMLARNING XAVFSIZLIK MODELLARI ASOSIDA QIYOSIY BARDOSHLILIK TAHLILI

Annotatsiya. *Maqolada RSA va El-Gamal ochiq kalitli algoritmlari matematik asoslari va zamonaviy xavfsizlik modellari (IND-CPA, IND-CCA) bo‘yicha qiyosiy tahlil qilingan. RSAning kichik maxfiy ko‘rsatkichga asoslangan zaifligi Wiener hujumi misolida davomli kasrlar usulida isbotlangan, shuningdek, uning determinizm sababli IND-CPA xavfsiz emasligi ko‘rsatilgan. El-Gamal uchun DDH farazi asosida IND-CPA xavfsizligi isbotlangan, ammo malleability xususiyati tufayli IND-CCA modellarida zaifligi aniqlangan. Natijalar resurslari cheklangan qurilmalar uchun yengil kriptografik yechimlar zarurligini ko‘rsatadi.*

Kalit so‘zlar: *RSA; El-Gamal, ochiq kalitli kriptografiya, IND-CPA xavfsizligi, IND-CCA xavfsizligi, Wiener hujumi, DDH farazi, malleability.*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ СОВРЕМЕННЫХ МОДЕЛЕЙ БЕЗОПАСНОСТИ

Аннотация. *В статье проведён сравнительный анализ криптографических алгоритмов с открытым ключом RSA и Эль-Гамаль на основе их математических основ и современных моделей безопасности (IND-CPA, IND-CCA). Уязвимость RSA при малом секретном показателе доказана на примере атаки Винера методом цепных дробей, а также показана недостаточность RSA для IND-CPA из-за детерминированности. Для Эль-Гамаль доказана IND-CPA-безопасность на основе предположения DDH, однако выявлена уязвимость в моделях IND-CCA из-за свойства malleability. Результаты указывают на необходимость лёгких криптографических решений для ресурсоограниченных устройств.*

Ключевые слова: *RSA, Эль-Гамаль, криптография с открытым ключом, безопасность IND-CPA, безопасность IND-CCA, атака Винера, предположение DDH, malleability.*

COMPARATIVE ANALYSIS OF PUBLIC-KEY CRYPTOGRAPHIC ALGORITHMS BASED ON MODERN SECURITY MODELS

Annotation. *This article presents a comparative analysis of the RSA and El-Gamal public-key algorithms based on their mathematical foundations and modern security models (IND-CPA, IND-CCA). RSA’s vulnerability under a small private exponent is proven via Wiener’s attack using continued fractions, and its determinism is shown to violate IND-CPA security. For El-Gamal, IND-CPA security is proven under the DDH assumption, while its malleability property is shown to break IND-CCA security. The findings highlight the need for lightweight cryptographic solutions for resource-constrained devices.*

Keywords: *RSA, El-Gamal, public-key cryptography, IND-CPA security, IND-CCA security, Wiener’s attack, DDH assumption, malleablility.*

Kirish. Axborot xavfsizligi sohasida asimmetrik kriptografiya algoritmlari shifrlash, raqamli imzo va autentifikatsiyaning asosiy vositasi hisoblanadi. So‘nggi yillarda IoT qurilmalari, simsiz sensor tarmoqlari va mobil platformalarning keng qo‘llanilishi natijasida kriptografik algoritmlarning xavfsizlik bilan bir qatorda, hisoblash samaradorligiga bo‘lgan talab ham ortib bormoqda. Shu sababli klassik ochiq kalitli al-