УДК 004.056

ИГРОВАЯ МОДЕЛЬ ДЛЯ АНАЛИЗА ХАРАКТЕРИСТИК СИСТЕМЫ АКТИВНОЙ ЗАЩИТЫ СЕТЕВЫХ РЕСУРСОВ

[1]Надеждин Е.Н., [2]Сурков Е.В., [2]Шершакова Т.Л.

[1]Государственный научно-исследовательский институт информационных технологий и телекоммуникаций, Москва, e-mail: e.nadezhdin@informika.ru;

[2]Шуйский филиал Ивановского государственного университета, Шуя, e-mail: vokrys@mail.ru, tshershakova@mail.ru

Настоящая статья посвящена исследованию влияния характеристик механизма защиты информации на защищённость сетевых ресурсов от информационных атак злоумышленника. Базовыми компонентами перспективной системы безопасности корпоративной информационной сети являются интеллектуальные механизмы активной и пассивной защиты сетевых ресурсов. Согласованное использование этих механизмов с учётом характеристик существующих угроз и особенностей защищаемых объектов позволит существенно уменьшить риски информационной безопасности. Классическая задача анализа защищённости сетевых ресурсов сформулирована с позиций метода игрового моделирования информационных конфликтов и интерпретирована в терминах статистической динамики систем управления. Объектом исследования является формальная динамическая система «система защиты ресурсов – злоумышленник». Для конкретных ситуаций информационного противоборства методом моделирования построена фазовая траектория динамической системы и рассчитаны терминальные значения частных показателей относительного ущерба. По результатам вычислительного эксперимента оценено влияние механизма активной защиты на защищённость сетевых ресурсов и сформулированы рекомендации, направленные на ослабление влияния информационных атак злоумышленника.

Ключевые слова: корпоративная информационная сеть, информационная атака, сетевые ресурсы, игровая модель, динамическая система «система защиты ресурсов – злоумышленник», активная и пассивная защита, совокупный относительный ущерб

GAME MODEL FOR ANALYSIS CHARACTERISTICS OF SYSTEM ACTIVE PROTECTION OF NETWORK RESOURCES

[1]Nadezhdin E.N., [2]Surkov E.V., [2]Shershakova T.L.

[1]State Institute of Information Technologies and Telecommunications, Moscow, e-mail: e.nadezhdin@informika.ru;

[2]Shuya branch of Ivanovo State University, Shuya, e-mail: vokrys@mail.ru, tshershakova@mail.ru

This article is devoted to the investigation of the influence of the characteristics of the information protection mechanism on the security of network resources against information attacks of an attacker. The basic components of promising security of corporate information networks are the intellectual mechanisms of active and passive protection of network resources. Consistent use of these mechanisms based on the characteristics of existing threats and the characteristics of protected objects, will significantly reduce the risks of information security. A classical problem of security analysis of network resources is formulated from the point of view of the method of gaming simulation of the conflict and interpreted from the perspective of statistical dynamics of control systems. The object of study is a formal dynamic system «system resource protection – intruder». For specific situations information warfare through simulation constructed the phase trajectory of the dynamic system and calculated the terminal values of the partial indicators of the relative damage. According to the results of computational experiment evaluated the influence of the mechanism of active protection on the security of network resources and formulate recommendations aimed at easing the impact of information attacks the attacker.

Keywords: corporate information network, information attack, network resources, game model, dynamic system «System resource protection – attacker», active and passive protection, the cumulative relative damage

В условиях непрерывного расширения сетевой инфраструктуры корпоративных систем и повышения роли информации в современном постиндустриальном обществе назрела необходимость критического анализа и пересмотра ключевых позиций существующей парадигмы обеспечения информационной безопасности (ИБ) государственных и коммерческих организаций. В современных системах защиты информации (СЗИ) корпоративных информационных сетей (КИС) для гарантированного отражения массированных информационных атак на важные сетевые ресурсы всё чаще используются гибкие механизмы с элементами активной и пассивной информационной защиты [1]. В последние годы значительно вырос поток публикаций, посвящённых вопросам синтеза интеллектуальных механизмов интегрированной защиты информационного и программного обеспечения, которые рассматриваются в контексте общей проблемы ситуационного управления рисками ИБ на основе базовых принципов кибернетики и искусственного интеллекта [2]. Однако вопросам

обоснования и выбора механизмов комплексирования методов и средств защиты ресурсов КИС, основанных на различных физических принципах, пока не уделяется должного внимания.

Целью статьи является операционное моделирование процесса функционирования системы интегрированной защиты информационных и программных ресурсов КИС и обоснование целесообразности введения в её состав активных элементов для осуществления адресных информационных контратак по объектам автоматизации, являющимся источниками информационных угроз.

Для формального описания процесса информационного противоборства воспользуемся известным игровым подходом, в основе которого лежат аксиоматика и инструментарий метода динамики средних (МДС) [3, 4]. Опираясь на базовую вычислительную схему МДС, сформулируем на содержательном уровне задачу операционного моделирования противоборства двух информационных систем. Пусть требуется построить игровую модель процесса информационного противоборства комплексной СЗИ КИС и злоумышленника и на её основе дать количественную оценку эффективности используемых средств активной и пассивной защиты сетевых ресурсов.

Под злоумышленником (ЗЛ) в настоящей статье понимается группа профессионально подготовленных, технически оснащённых и мотивированных сотрудников фирмы-конкурента, стремящихся взломать систему защиты активов организации-жертвы, получить доступ к её конфиденциальной информации и нарушить управление бизнес-процессом.

Следуя рекомендациям опубликованных работ В.М. Гаврилова [3], Г.А. Остапенко [5], С.И. Макаренко [6], А.Ф. Белого [7] и основываясь на накопленном опыте операционного моделирования информационных процессов [8, 9], введём ряд дисциплинирующих условий. Во-первых, отметим, что перспективная СЗИ должна не только обнаруживать факты нарушения целостности информации, определять степень ущерба и оперативно восстанавливать повреждённые информационные и программные ресурсы, но также целенаправленно выявлять и оценивать новые угрозы и адресно применять активные способы защиты в виде информационных контратак. Во-вторых, примем рабочую гипотезу о том, что информационная атака злоумышленника является многоцелевой и осуществляется из двух внешних узлов информационной сети. В-третьих, взаимодействие конфликтующих сторон *A* и *B* осуществляется по заранее определённому сценарию, задаваемому операционной схемой, при этом информационные атаки и контратаки проводятся по фиксированным объектам (целям) с постоянными интенсивностями.

Принципиальной особенностью используемого в статье модельного подхода является формальное представление объекта исследования как динамической системы «*Система защиты ресурсов – злоумышленник*» («СЗР-ЗЛ»), изолированной от внешней среды и функционирующей на заданном интервале времени $[t_0, t_N]$. Вектор фазовых координат динамической системы (ДС) $\forall\, t \in [t_0, t_N]$ имеет вид: $Z = (z_1, z_2, ...z_k, ..., z_n)^T$, где z_k – численность состояния элемента (средства) *k*-го типа. Пошаговая (во времени) численная оценка вектора состояния $Z(t)$ $\forall\, t \in (t_0, t_N]$ на основе формального описания и имитационного моделирования процесса функционирования позволяет получить исчерпывающую информацию о подпроцессах, протекающих в подсистемах (элементах) этой ДС. При исследовании воспользуемся авторской методикой операционного моделирования процесса информационного противоборства, получившей развитие в авторских работах [8, 9]. Известная методика даёт возможность для заданных условий и сценария информационного конфликта оценить частные показатели, отражающие снижение потенциала средств каждого типа и *совокупный риск* (в нашем случае – *ущерб*) каждой стороны (подсистемы).

Текущее состояние средств, выделенных в составе формальной ДС, предлагается оценивать с помощью частного показателя потерь ΔZ_i, под которым понимают величину относительного ущерба, нанесенного средству z_i в результате целенаправленного информационного воздействия со стороны других средств ДС. Фактические потери – это результат воздействия информационных атак, организованных средствами противодействующей стороны (конфликтующей подсистемы). Показатель относительного ущерба ΔZ_i, $i = \overline{1,n}$, определяется по формуле

$$\Delta Z_i(t^*) = \frac{z_i(t_0) - z_i(t^*)}{z_i(t_0)} \cdot 100\%, \qquad (1)$$

где t^* – момент выхода из цикла операционного моделирования;

$\Delta Z_i(t^*)$ – относительный ущерб для средства z_i на момент времени t^*;

$z_i(t_0)$ – исходный потенциал средства z_i в момент времени t_0.

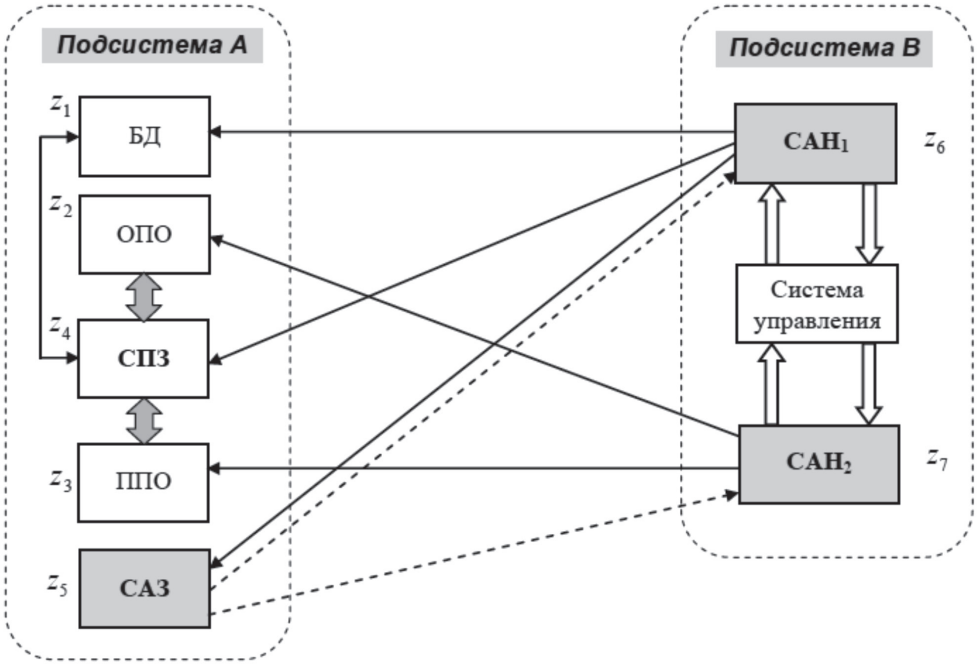

Рис. 1. Операционная схема процесса информационного противоборства средств в динамической системе «Система защиты ресурсов – злоумышленник»

Совокупный риск (ущерб) противоборствующих сторон (подсистем) *A* и *B* может быть определён в произвольный момент времени $t \in (t_0, t_N]$ на основе следующих соотношений:

$$W_A = \sum_{i \in I_A} \alpha_i \cdot \Delta Z_i \; ; \; W_B = \sum_{i \in I_A} \beta_i \cdot \Delta Z_i \; , \qquad (2)$$

где α_i и β_i – весовые коэффициенты; ΔZ_i – показатель относительного ущерба для средства *i*-го типа на момент времени *t*; I_A и I_B – множества, содержащие индексы фазовых переменных, относящихся соответственно к сторонам *A* и *B*.

Рассмотрим особенности построения модели задачи исследования. К сетевым ресурсам КИС будем относить информационное обеспечение (ИО), общее и прикладное программное обеспечение. Учитывая сложность архитектуры перспективной комплексной СЗИ, в составе её модели выделим два обобщённых компонента: средства пассивной защиты (СПЗ) и средства активной защиты (САЗ).

На рис. 1 представлена укрупнённая операционная схема многоканального информационного взаимодействия подсистем исследуемой динамической системы «СЗР-ЗЛ». При этом введены следующие обозначения: подсистема *A* – СЗР; подсистема *B* – злоумышленник, стремящийся преодолеть защиту и получить доступ к сетевым ресурсам подсистемы *A*. В структуре СЗР (*подсистема A*) выделены следующие элементы: база данных (БД), общее программное обеспечение (ОПО), прикладное программное обеспечение (ППО), средства пассивной защиты /средства восстановления/ и средства активной защиты. Будем полагать, что СПЗ используются для обнаружения, локализации и восстановления повреждённых информационных элементов и программных модулей [9]. В модели злоумышленника (*подсистема B*) выделены: средства активного нападения первого и второго типов (САН$_1$ и САН$_2$) и система управления ими.

Для отображения динамики восстановления повреждённых информационных элементов БД и программных модулей ОПО и ППО воспользуемся рекомендациями теории автоматического управления. Динамическую модель процесса восстановления средства z_i представим в виде инерционного звена первого порядка, которое опишем на основе линейного дифференциального уравнения [10, с. 39–42]:

$$\dot{y}_i(t) = -\frac{1}{T_i} \cdot y_i(t) + \frac{k_i}{T_i} \cdot z_i(t) \, ,$$

где y_i – приращение численности состояния z_i за счёт реализации процедуры восстановления повреждённых компонентов; k_i и T_i – соответственно коэффициент передачи и постоянная времени инерционного

звена. Указанной моделью воспользуемся для описания восстановления численностей состояний z_1, z_2 и z_3. При этом коэффициенты передачи k_i $(i=1,2,3)$ характеризуют интенсивности восстановления численностей состояний z_1, z_2 и z_3, а постоянные времени T_i $(i=1,2,3)$ определяют длительности переходных процессов.

Для формализованного представления состояний ДС «СЗИ-ЗЛ» введём переменные $z_i, i=1,...,7$, под которыми будем понимать численности состояний соответственно следующих элементов: базы данных z_1, общего программного обеспечения z_2, прикладного программного обеспечения z_3, средств пассивной z_4 и активной защиты z_5 подсистемы A, а также средств активного нападения первого типа z_6 и средств активного нападения второго типа z_7 подсистемы B. Состояние динамической системы «СЗР-ЗЛ» в целом в каждый момент времени $t \in (t_0, t_N]$ характеризуется системой обыкновенных дифференциальных уравнений, в которой в качестве переменных рассматриваются численности состояний $z_i, i=1,...,10$:

$$\begin{cases} \dfrac{dz_1(t)}{dt} = \dot{z}_1(t) = -b_1 \cdot p_{1,6}\lambda_6 \cdot z_6(t) + h(z_1, Z_1^*) \cdot z_8(t); \\ \dfrac{dz_2(t)}{dt} = \dot{z}_2(t) = -c_1 \cdot p_{2,7} \cdot \lambda_7 \cdot z_7(t) + h(z_2, Z_2^*) \cdot z_9(t); \\ \dfrac{dz_3(t)}{dt} = \dot{z}_3(t) = -c_2 \cdot p_{3,7} \cdot \lambda_7 \cdot z_7(t) + h(z_3, Z_3^*) \cdot z_{10}(t); \\ \dfrac{dz_4(t)}{dt} = \dot{z}_4(t) = -b_2 \cdot p_{4,6} \cdot \lambda_6 \cdot z_6(t); \\ \dfrac{dz_5(t)}{dt} = \dot{z}_5(t) = -b_3 \cdot p_{5,6} \cdot \lambda_6 \cdot z_6(t); \\ \dfrac{dz_6(t)}{dt} = \dot{z}_6(t) = -a_1 \cdot p_{6,5} \cdot \lambda_5 \cdot z_5(t); \\ \dfrac{dz_7(t)}{dt} = \dot{z}_7(t) = -a_2 \cdot p_{7,5} \cdot \lambda_5 \cdot z_5(t); \\ \dfrac{dz_8(t)}{dt} = \dot{z}_8(t) = -1/T_1 \cdot z_8(t) + k_1/T_1 \cdot z_4(t); \\ \dfrac{dz_9(t)}{dt} = \dot{z}_9(t) = -1/T_2 \cdot z_9(t) + k_2/T_2 \cdot z_4(t); \\ \dfrac{dz_{10}}{dt} = \dot{z}_{10}(t) = -1/T_3 \cdot z_{10}(t) + k_3/T_3 \cdot z_4(t). \end{cases} \quad (3)$$

Здесь $h(z_1, Z_1^*)$ – процедура проверки условия активации механизма пассивной защиты, связанного с введением резерва или восстановлением (пополнением) численности состояний z_1. Аналогично $h(z_2, Z_2^*)$ и $h(z_3, Z_3^*)$ – процедуры проверки условий активации механизма пассивной защиты, связанного с введением резерва или восстановлением (пополнением) численности состояний z_2 и z_3; Z_1^*, Z_2^*, Z_3^* – значения порогов включения соответствующих механизмов пассивной защиты.

Условие активации пассивной защиты для численности состояния z_r запишем с помощью логической функции:

$$h(z_r, Z_r^*) = \begin{cases} 1, \text{ если } z_r(t) \le Z_r^*; \\ 0, \text{ если } z_r(t) > Z_r^*. \end{cases} \quad (4)$$

Введём вспомогательные переменные $A_k, k=1,...,13$ для обозначения коэффициентов дифференциальных уравнений, определяемые на основе расчётных соотношений, приведённых в табл. 1.

Здесь λ_5, λ_6 и λ_7 – интенсивности атак (контратак), выполняемых средствами z_5, z_6 и z_7 соответственно; p_{ij} – вероятность поражения единицы средства z_i в результате атаки со стороны средства z_j; b_1, b_2 и b_3 – доли средств z_3 подсистемы B, участвующих в подавлении средств z_1, z_4 и z_5 подсистемы A соответственно; c_1 и c_2 – доли средств z_7 подсистемы B, участвующих в подавлении соответственно средств z_2 и z_3 подсистемы A; a_1 и a_2 – доли средств z_5 подсистемы A, участвующих в подавлении соответственно средств z_6 и z_7 подсистемы B; при этом

должны выполняться дисциплинирующие условия

$$a_1 + a_2 \le 1;\ b_1 + b_2 + b_3 \le 1;\ c_1 + c_2 \le 1.$$

Известно, что имеющиеся уязвимости модулей ППО способствуют повышению результативности информационных атак злоумышленника на информационные ресурсы и ОПО. Для учёта данного эффекта в математическую модель (3) введём весовую функцию:

$$V(N_0, \mu_k, z_3) = \exp\left[\mu_k \cdot (N_0 - z_3) / N_0\right], \quad (5)$$

где N_0 и $z_3 = z_3(t)$ – исходный ресурс и текущее значение численности состояния средства z_3 соответственно; μ_k – коэффициент, учитывающий влияние уязвимости на защищённость модуля средства z_k.

В динамике противоборства при использовании элементов активной защиты сетевых ресурсов стороной А средства z_6 и z_7 стороны В теряют часть своего потенциала. Это, в свою очередь, снижает интенсивность информационных атак стороны *B* на средства стороны *A*. Для учёта данного эффекта в математическую модель (3) введём весовую функцию:

$$L(N_0, d_k, z_k) = \exp\left[-\rho_k \cdot \frac{(N_0 - z_k)}{N_0}\right], \quad (6)$$

где N_0 и $z_k = z_k(t)$ – исходный ресурс и текущее значение численности состояния атакующего средства z_k стороны *B*; ρ_k – коэффициент, учитывающий влияние снижения потенциала z_k на интенсивность λ_k исходящей от него атаки.

После преобразований системы дифференциальных уравнений (3) с учётом введённых обозначений (4), (5), (6) и коэффициентов (табл. 1) получим систему уравнений:

$$\begin{cases} \dot{z}_1(t) = A_1 \cdot V(N_3, \mu_1, z_3) \cdot L(N_6, d_1, z_6) \cdot z_6 + h(z_1, Z_1^*) \cdot z_8; \\ \dot{z}_2(t) = A_2 \cdot V(N_3, \mu_2, z_3) \cdot L(N_7, d_2, z_7) \cdot z_7 + h(z_2, Z_2^*) \cdot z_9; \\ \dot{z}_3(t) = A_3 \cdot L(N_7, d_3, z_7) \cdot z_7 + h(z_3, Z_3^*) \cdot z_{10}; \\ \dot{z}_4(t) = A_4 \cdot z_6; \\ \dot{z}_5(t) = A_5 \cdot z_6; \\ \dot{z}_6(t) = A_6 \cdot z_5; \\ \dot{z}_7(t) = A_7 \cdot z_5; \\ \dot{z}_8(t) = A_8 \cdot z_8 + A_9 \cdot z_4; \\ \dot{z}_9(t) = A_{10} \cdot z_9 + A_{11} \cdot z_4; \\ \dot{z}_{10}(t) = A_{12} \cdot z_{10} + A_{13} \cdot z_4. \end{cases} \quad (7)$$

Соотношения $b_1/b_2/b_3$ и c_1/c_2 определяют стратегию стороны *B* в организации информационных атак на средства стороны *A*. Соотношение a_1/a_2 определяет стратегию стороны *A* в осуществлении информационных контратак на средства z_6 и z_7 стороны *B*.

В целях удобства алгоритмизации введём *дополнительные условия*:

1. Резерв для пополнения (восстановления) элементов в состоянии z_1 используется при выполнении условия: $z_1(t) \le 80\,\% \times z_1(t_0)$; резерв для пополнения элементов в состоянии z_2 используется при выполнении условия: $z_2(t) \le 90\,\% \times z_2(t_0)$; резерв для пополнения элементов в состоянии z_2 используется при выполнении условия: $z_3(t) \le 95\,\% \times z_3(t_0)$.

2. Каждое из средств z_i, $i = \overline{1,7}$, имеет только два состояния: рабочее и нерабочее.

3. Начальные условия:

$$z_k(t_0) = 100\ \forall\ k = \overline{1,7};\ z_8(t_0) = z_9(t_0) = z_{10}(t_0) = 0.$$

4. Интенсивности атак принимаются следующими:

$$\lambda_5 = 0{,}06\ldots0{,}30\ \text{мин}^{-1};\ \lambda_6 = 0{,}12\ \text{мин}^{-1};\ \lambda_7 = 0{,}06\ \text{мин}^{-1}.$$

5. С учётом анализа информационных угроз и имеющегося опыта исследования СЗИ приняты фиксированные стратегии игроков *A* и *B*:

$$a_1 = 0{,}25;\ a_2 = 0{,}75;\ c_1 = 0{,}6;\ c_2 = 0{,}4;\ b_1 = 0{,}25;\ b_2 = 0{,}25;\ b_3 = 0{,}5.$$

Значения вероятностей поражения одной единицы средств игроков *A* и *B* примем в соответствии с данными табл. 2.

Таблица 1

Расчётные соотношения для коэффициентов дифференциальных уравнений

A_1	A_2	A_3	A_4	A_5	A_6	A_7
$-\lambda_6 \cdot p_{16} \cdot b_1$	$-\lambda_7 \cdot p_{27} \cdot c_1$	$-\lambda_7 \cdot p_{37} \cdot c_2$	$-\lambda_6 \cdot p_{46} \cdot b_2$	$-\lambda_6 \cdot p_{56} \cdot b_3$	$-\lambda_5 \cdot p_{65} \cdot a_1$	$-\lambda_5 \cdot p_{75} \cdot a_2$
A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	
$-\frac{1}{T_1}$	$\frac{k_1}{T_1}$	$-\frac{1}{T_2}$	$\frac{k_2}{T_2}$	$-\frac{1}{T_3}$	$\frac{k_3}{T_3}$	

Таблица 2

Вероятности поражения элементов

Подсистема А					Подсистема В	
p_{16}	p_{27}	p_{37}	p_{46}	p_{56}	p_{65}	p_{75}
0,010	0,040	0,030	0,010	0,015	0,020	0,015

Таблица 3

Показатели относительного ущерба (%) для средств сторон в контрольной точке $t^* = T = 120$ (мин.), опыт 1: $\lambda_5 = 0{,}06$ (1/мин)

Средства стороны А					Средства стороны В	
$\Delta Z_1(t^*)$	$\Delta Z_2(t^*)$	$\Delta Z_3(t^*)$	$\Delta Z_4(t^*)$	$\Delta Z_5(t^*)$	$\Delta Z_6(t^*)$	$\Delta Z_7(t^*)$
3,30	13,93	6,81	3,54	10,61	3,41	7,67

6. Численное решение системы дифференциальных уравнений осуществляется стандартным методом Рунге – Кутты в цикле на полуинтервале времени $t \in (t_0, t_N]$: $t_0 = 0$ мин, $t_N = 120$ мин с шагом $\Delta t = 0{,}05$ мин.

7. Выход из цикла моделирования (решения) осуществлялся в одном из следующих случаев: [$z_1 \le 60$; $z_2 \le 60$; $z_3 \le 60$; $z_4 \le 30$; $z_5 \le 30$; $z_6 \le 45$; $z_7 \le 45$].

В качестве выходных данных моделирования фиксируются: время решения задачи $t_{реш}$, тождественно равное времени t^* информационного взаимодействия $t_{реш} \equiv t^*$; фазовые траектории $z_i = f_i(t)$, $i = \overline{1,10}$; $t \in (t_0, t^*]$; численные значения показателей $\Delta Z_i(t^*)$, $i = \overline{1,7}$.

На рис. 2 и 3 представлены изменения численностей состояний сетевых ресурсов на указанном полуинтервале времени.

Используя данные об изменении численностей состояний динамической системы во времени $T \equiv t$ (мин), для заданного момента времени t^* можно вычислить относительный ущерб $\Delta Z_i(t^*)$ по формуле (1) по каждому средству z_i, $i = \overline{1,7}$, сторон *A* и *B*. Результаты расчёта показателей относительного ущерба $\Delta Z_i(t^*)$ для фиксированных исходных данных приведены в табл. 3. Данные цифрового моделирования фазовой траектории ДС в виде таблиц или графиков изменения во времени фазовых координат z_i, $i = \overline{1,7}$ позволяют проследить динамику взаимодействия СЗИ со злоумышленником и косвенно оценить результативность используемых механизмов комплексной защиты ресурсов КИС.

Для рассмотренной задачи совокупный ущерб противоборствующих подсистем *A* и *B*, вычисленный по формулам (2) при учёте данных табл. 2 для случая равных весовых коэффициентов $\alpha_i = \text{const} = 1$ и $\beta_i = \cos t = 1$, составил

$$W_A = \sum_{i=1}^{3} \alpha_i \cdot \Delta Z_i = 38{,}18\ \%$$

и

$$W_B = \sum_{i=4}^{6} \beta_i \cdot \Delta Z_i = 11{,}07\ \%.$$

В ходе исследования проанализировано влияние интенсивности контратак стороны *A* на защищённость ресурсов КИС, на ресурс СЗР и на ресурс стороны (игрока) *B*. При этом интенсивность контратак изменялась в отрезке $\lambda_5 \in [0{,}03; 0{,}30]$ мин.$^{-1}$ с шагом 0,03. Результаты вычислительного эксперимента представлены на рис. 4.

Средний коэффициент эластичности $\overline{Э}$, определяемый по известной формуле [11] для линейной регрессионной модели ре-

грессии $f(x) = -1,649 \cdot x + 26,947$ составил величину

$$\overline{Э} = f'(x) \cdot \frac{\overline{x}}{y} = -0,015,$$

что свидетельствует о малой силе влияния интенсивности λ_5 информационных контратак на снижение ресурса атакующей стороны *B*.

По результатам операционного моделирования можно оценить результативность используемых механизмов защиты сетевых ресурсов для различных стратегий действия и сценариев противоборства сторон *A* и *B*. В авторской работе [9] ранее было установлено, что прямой способ повышения эффективности МЗР через снижение уязвимости средств z_1, z_2 и z_3 не является продуктивным. Из анализа результатов вычислительного эксперимента следует, что прямое увеличение интенсивности контратак СЗИ также не даёт значительного приращения защищённости информационных и программных ресурсов. Кроме того, усиление мощности информационных контратак, инициируемых подсистемой *A*, связано с большими затратами внутренних вычислительных ресурсов КИС и в ряде случаев может способствовать быстрому вскрытию злоумышленником (стороной *B*) характеристик СЗИ.

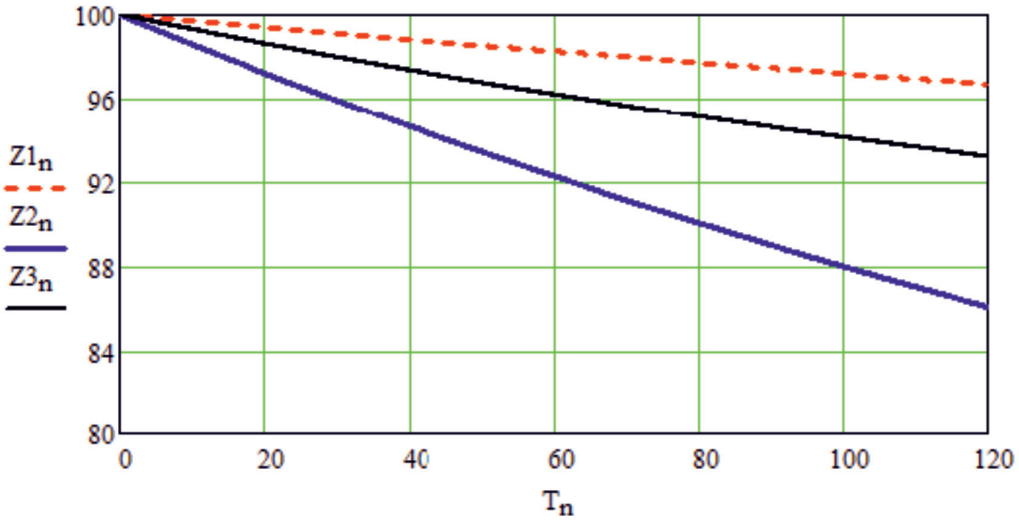

Рис. 2. Изменение численности состояний z_1, z_2, z_3 от времени информационного контакта T (мин) сторон A и B (без механизма восстановления)

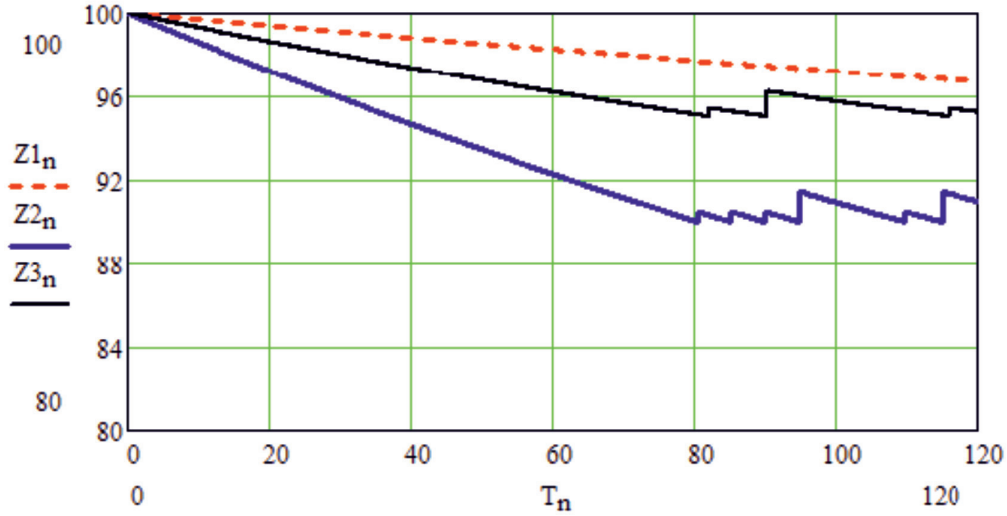

Рис. 3. Изменение численности состояний z_1, z_2, z_3 от времени информационного контакта T (мин) сторон A и B (с механизмом восстановления численностей z_2 и z_3)

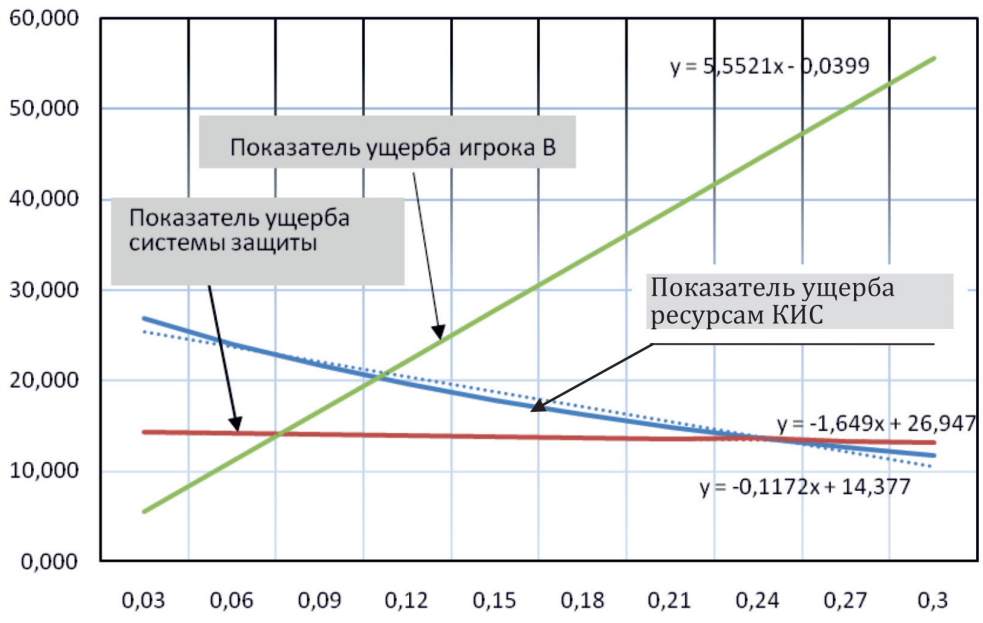

Рис. 4. Зависимости показателей относительного ущерба от интенсивности контратак λ_5 (1/мин) стороны А

Установлено, что при больших интенсивностях информационных контратак ($\lambda_5/(\lambda_6+\lambda_7)\geq 1,0$) происходит относительно быстрое снижение потенциала подсистемы *B* и тем самым уменьшается степень информационного воздействия средств z_6 и z_7 на ресурсы КИС. Визуально данный нелинейный эффект можно проследить на графиках рис. 5, на котором показаны фазовые траектории численностей состояний средств $z_1(t)$, $z_2(t)$, $z_3(t)$.

Таким образом, в результате исследования установлено, что наиболее значительного приращения эффективности МЗР следует ожидать в случае комплексного (согласованного по целям, задачам и времени) применения нескольких способов пассивной и активной защиты сетевых ресурсов КИС. Закономерным итогом комплексирования способов и средств защиты будет существенное снижение уязвимости средств z_1, z_2 и z_3 игрока А при одновременном уменьшении интенсивности информационных атак со стороны средств z_6 и z_7. По данным моделирования, совместное использование СПЗ (для восстановления повреждённых массивов ИО и модулей ОПО и ППО) и САЗ способно снизить относительный ущерб для сетевых ресурсов на 11…24%.

Выводы

На современном этапе эволюции системы информационной безопасности в составе комплексной СЗИ доминируют традиционные средства пассивной защиты информационного и программного обеспечения. Для достижения заданного политикой безопасности уровня защищённости сетевых ресурсов в условиях вероятных сетевых атак предлагается дополнительно включить в состав СЗИ элементы активной защиты, способные реализовать информационные контратаки на выявленные источники потенциальных угроз в целях пресечения их деятельности. Для повышения эффективности САЗ могут быть применены следующие способы:

1) согласование характеристик и синхронизация работы средств пассивной и активной защиты под управлением интеллектуальной системы управления ИБ;

2) применение гибкой стратегии защиты, заключающейся в концентрации усилий на поражении наиболее опасных компонентов подсистемы *B*;

3) выявление фактов и идентификация характеристик системы захвата (злоумышленником) управления узлами КИС, через которые в последующем могут осуществляться систематические информационные атаки на сетевые ресурсы;

4) планирование и реализация стороной *A* упреждающих информационных контратак, преимущественно на начальном этапе информационного противоборства в целях максимального ослабления потенциала злоумышленника (стороны *B*) и принуждения его к отказу от преступных замыслов.

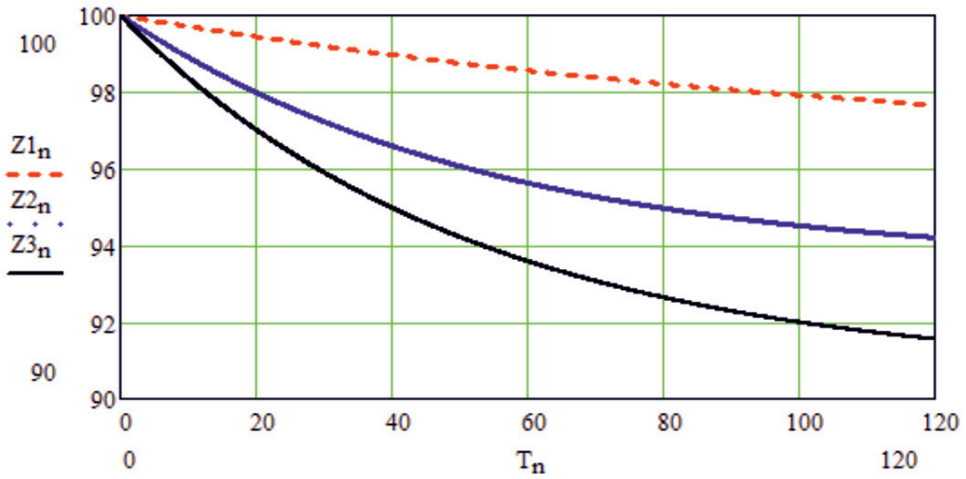

Рис. 5. Изменение численностей состояний подсистемы А во времени с учётом эффекта ослабления атакующего потенциала подсистемы В (случай λ_5 = 0,27 1/мин)

В качестве одного из перспективных направлений обеспечения гарантированной защищённости сетевых ресурсов КИС можно указать совместное применение рекомендаций и структурных решений теории обманных систем и алгоритмов интеллектуального управления МЗР [2].

Список литературы

1. Малюк А.А. Теория защиты информации / А.А. Малюк. – М.: Горячая линия – Телеком, 2012. – 184 с.

2. Надеждин Е.Н. Кибернетические аспекты управления рисками информационной безопасности в компьютерных сетях образовательных организаций / Е.Н. Надеждин, Е.В. Сурков // Современные наукоёмкие технологии. – 2016. – № 10–2. – С. 279–285.

3. Гаврилов В.М. Оптимальные процессы в конфликтных ситуациях / В.М. Гаврилов. – М.: Советское радио, 1969. – 160 с.

4. Чуев Ю.В. Исследование операций в военном деле / Ю.В. Чуев. – М.: Воениздат Министерства обороны, 1970. – 256 с.

5. Остапенко Г.А. Формализация описания сетевого конфликта / Г.А. Остапенко, Д.Г. Плотников, Ю.Н. Гузев // Информация и безопасность. – 2016. – Т. 19, № 2. – С. 232–237.

6. Макаренко С.И. Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса / С.И. Макаренко // Системы управления, связи и безопасности. – 2017. – № 1. – С. 60–97. URL: http://sccs.intelgr.com/archive/2017-01/06-Makarenko.pdf.

7. Белый А.Ф. Метод анализа двусторонних процессов информационного противодействия в критически важной информационной системе на основе моделей динамики средних / А.Ф. Белый // Безопасность информационных технологий. – 2011. – № 3. – С. 5–9.

8. Надеждин Е.Н. Модели информационного противоборства в задачах оценки безопасности вычислительных сетей / Е.Н. Надеждин, Е.Е. Смирнова, А.О. Козлов // Информатизация образования и науки. – 2009. – № 2. – С. 45–50.

9. Надеждин Е.Н. Оценка эффективности механизма защиты сетевых ресурсов на основе игровой модели информационного противоборства/ Е.Н. Надеждин // Научный вестник. 2015. – № 2(4). – С. 49–58.

10. Усынин Ю.С. Теория автоматического управления: учебное пособие для вузов / Ю.С. Усынин. – Челябинск: Издательский центр ЮУрГУ, 2010. – 176 с.

11. Эконометрика: учебник / под ред. В.С. Мхитаряна. – М.: Проспект, 2010. – 384 с.