DOI: 10.17117/nv.2015.02.049

Поступила (Received): 08.06.2015

<http://ucom.ru/doc/nv.2015.02.049.pdf>

tgpu@tula.net

Надеждин Е.Н.**Оценка эффективности механизма защиты сетевых ресурсов на основе игровой модели информационного противоборства****Nadezhdin E.N.****Evaluation of the effectiveness of the protection mechanism of network resources based gaming model of information warfare**

На фоне общей тенденции информатизации общества расширяется спектр угроз информационной безопасности сетевым ресурсам научно-образовательных учреждений. Сформулирована задача количественной оценки эффективности механизма защиты ресурсов корпоративной вычислительной сети. В отличие от традиционного подхода, объектом исследования в статье является формальная динамическая система, структурно объединяющая противоборствующие информационные системы. Данный приём позволил исходную задачу оценки эффективности интерпретировать в терминах статистической динамики систем управления. На основе теории метода динамики средних для динамической системы «Система защиты информации – злоумышленник» разработана математическая модель в виде системы однородных дифференциальных уравнений. В предложенной модели фазовыми координатами являются параметры состояния конфликтующих подсистем. Для конкретных условий прикладной задачи методом компьютерного моделирования идентифицирована фазовая траектория динамической системы и вычислено терминальное значение показателя совокупного ущерба. Данный результат отражает эффективность функционирования механизма защиты сетевых ресурсов

Ключевые слова: вычислительная сеть, защита сетевых ресурсов

On the background of the General trend of Informatization of the society is expanding the range of information security threats network resources of scientific and educational institutions. We have formulated the problem of quantitative evaluation of effectiveness of mechanism of protection of resources of corporate computing networks. Unlike the traditional approach, the object of research in article is the formal dynamic system, structurally uniting the warring information system. This method allowed the initial problem of evaluating the effectiveness interpreted in terms of the statistical dynamics of control systems. Based on the theory of the dynamics of average method for dynamic systems "System of information protection – attacker" a mathematical model in the form of a system of homogeneous differential equations. In the proposed model of the phase coordinates are the state parameters of conflicting subsystems. For a specific applied problems by methods of computer simulations identified the phase trajectory of the dynamic system and calculated the terminal value of the loss. This result reflects the efficiency of the mechanism of protection of network resources

Key words: computer network, protection of network resources

Надеждин Евгений Николаевич*Доктор технических наук, профессор
Тульский государственный педагогический
университет имени Л.Н. Толстого
г. Тула, пр. Ленина, 125***Nadezhdin Evgeniy Nikolaevich***Doctor of Engineering Sciences, Professor
Tula state pedagogical University named
after L.N. Tolstoy
Tula, Lenin ave., 125*

Стремительное расширение сетевой инфраструктуры национальных научно-образовательных центров потребовало адекватного развития методов и аппаратно-программных средств комплексной защиты информации [1, 7]. Наиболее острой в настоящее время является проблема создания гибких механизмов защиты от массированных атак потенциальных злоумышленников на информационные и вычислительные ресурсы корпоративных вычислительных сетей (КВС). Возросший поток научных публикаций [1, 2, 5, 7], посвящённых методам и алгоритмам интеллектуального анализа угроз и управления рисками сетевой безопасности, косвенно свидетельствует о нерешённости проблемы обеспечения гарантированной защиты сетевых ресурсов.

Целью статьи является обоснование игровой модели процесса отражения массированной атаки на сетевую инфраструктуру организации и обоснование алгоритма количественной оценки эффективности механизма защиты сетевых ресурсов (МЗР) КВС.

В основу игровой модели процесса информационного противоборства положим аксиоматику и инструментарий известного метода динамики средних (МДС), который был разработан в 60-х годах XX-го века применительно к задачам численного анализа средних характеристик случайных процессов в системах управления боевыми действиями с большим числом состояний [8]. Позднее МДС получил развитие и был обобщён на класс задач игрового моделирования процессов многоканального противоборства автоматизированных информационных систем [3, 4]. Опираясь на базовую вычислительную схему МДС, изложим на содержательном уровне задачу моделирования процесса противоборства двух информационных систем (на сегменте глобальной сети).

Пусть требуется оценить эффективность МЗР путём систематического изучения игровой модели информационного противоборства системы защиты информации КВС и некоторого условного «злоумышленника». Для определённости примем, что под «злоумышленником» (ЗЛ) понимается группа профессионально подготовленных и мотивированных сотрудников фирмы-конкурента, стремящихся взломать систему защиты активов, получить доступ к конфиденциальной информации, нарушить управление и, в целом, ухудшить имидж учреждения на рынке инновационных НБИК-технологий.

Основываясь на опыте создания автоматизированных систем, оснащённых комплексной системой защиты информации (СЗИ), введём ряд определений. При этом отметим, что комплексная СЗИ, обладая значительным информационно-аналитическим потенциалом, должна не только обнаруживать факты нарушения целостности информации, определять степень ущерба и оперативно восстанавливать информацию, но и целенаправленно выявлять и оценивать новые угрозы и применять активные способы и средства защиты. Здесь на основе

использования современных интеллектуальных технологий открываются новые возможности для прерывания информационных атак злоумышленника на элементы инфраструктуры КВС и снижения возможного ущерба.

Как показал анализ известных работ в области ИБ, в настоящее время отсутствуют общепринятые унифицированные методики расчёта эффективности защиты ресурсов и оценки рисков автоматизированных систем. Это объясняется, прежде всего, уникальностью сетевой инфраструктуры учреждения и сложностью аналитического описания функционала КВС с учётом специфики динамично изменяющейся информационной среды. В этой связи основным методом количественной оценки и прогнозирования показателей СЗИ остаётся метод имитационного моделирования [5].

Принципиальной особенностью развиваемого в статье модельного подхода является формальное представление объекта исследования как динамической системы «Система защиты информации – злоумышленник» («СЗИ-ЗЛ»), функционирующей на заданном интервале времени $[t_0, t_N]$. Вектор фазовых координат динамической системы (ДС) в момент времени $t \in (t_0, t_N]$ имеет вид: $Z = (z_1, z_2, \dots, z_k, \dots, z_n)^T$, 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 ДС позволит получить исчерпывающую информацию о подпроцессах, протекающих в подсистемах (элементах) этой динамической системе. Предлагаемая методика исследования эффективности комплексной защиты информации в КВС на основе компьютерной реализации игровой модели включает следующие этапы [4].

Шаг 1. Анализ характеристик (состава, направленности, интенсивности возникновения и механизмов реализации) информационных угроз. Содержательная постановка задачи исследования.

Шаг 2. Разработка операционной схемы для исследования динамической системы «СЗИ-ЗЛ» на полуинтервале времени $t \in (t_0, t_N]$. Формулировка дисциплинирующих условий и основных ограничений.

Шаг 3. Составление уравнений для численностей состояний в дифференциальной форме в соответствии с методом динамики средних.

Шаг 4. Задание исходных данных, базовых и дополнительных ограничений для решения задачи исследования. Определение условий преждевременного завершения процесса информационного противоборства и выхода из цикла операционного моделирования.

Шаг 5. Формализация модели и решение задачи анализа с использованием унифицированных процедур численного интегрирования. Фиксация и аппроксимация результатов моделирования.

Шаг 6. Вычисление значений частных показателей эффективности, отражающих относительное состояние каждого типа элементов (средств) динамической системы на момент времени $t^* \in (t_0, t_N]$ выхода из цикла моделирования по заданному условию.

Шаг 7. Оценка ущерба W_A и W_B для участвующих в информационном взаимодействии подсистем.

Текущее состояние средств всех типов предлагается оценивать с помощью показателя потерь ΔZ_i , под которым понимают величину относительного ущерба, нанесенного средству z_i в результате целенаправленного информационного воздействия со стороны других средств ДС. Фактически потери – это результат информационных атак средств, относящихся к противодействующей стороне (подсистеме). Показатель относительного ущерба ΔZ_i , $i = \overline{1, n}$, может быть вычислен по формуле:

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

где t^* – текущий момент времени (момент выхода из цикла 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 .

Шаг 8. Обобщение результатов моделирования и обоснование рекомендаций по выбору характеристик СЗИ и стратегии её использования в КВС.

Изложенная выше схема оценки эффективности механизма защиты КВС реализована в виде компьютерной программы, которая составлена в интегрированной вычислительной среде MathCad (v. 15) и даёт возможность для заданных условий возникновения и развития информационного конфликта оценить частные показатели, отражающие снижение ресурса средств каждого типа и совокупный риск (ущерб) каждой стороны (подсистемы).

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

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

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**.

В качестве примера приложения авторской методики ниже представлено решение задачи количественной оценки эффективности МЗР. При этом к сетевым ресурсам будем относить информационное и программное обеспечение КВС. Учитывая специфику комплексных СЗИ [1], в составе её модели выделим средства пассивной защиты (СПЗ) и средства активной защиты (САЗ).

На рис. 1 представлена укрупнённая операционная схема многоканального информационного взаимодействия подсистем исследуемой динамической

системы «СЗИ-ЗЛ». При этом введены следующие обозначения: *сторона А* (игрок **А**) – СЗИ; *сторона В* (игрок **В**) – злоумышленник, пытающийся преодолеть защиту и получить доступ к сетевым ресурсам. В структуре СЗИ (*подсистема А*) выделены следующие элементы: средства программного обеспечения (СПО), база данных (БД), средства пассивной защиты /средства восстановления/ (СПЗ) и средства активной защиты (САЗ). В модели злоумышленника (*подсистема В*) выделены: средства активного нападения первого и второго типов (САН₁ и САН₂) и система управления ими. Будем полагать, что СПЗ используются для обнаружения, локализации и восстановления повреждённых информационных элементов и программных модулей. В интересах упрощения процесса алгоритмизации задачи исследования специальные ограничения на характеристики СПЗ подсистемы **А** не вводились.

Для формализованного представления ДС «КВС-ЗЛ» введём переменные $z_i, i = 1, \dots, 6$, под которыми будем понимать численности состояний соответственно следующих элементов: базы данных, средств программного обеспечения и средств активной защиты подсистемы **А**, а также средств активного нападения первого типа, системы управления и средств активного нападения второго типа подсистемы **В**.

Состояние динамической системы «КВС-ЗЛ» в целом в каждый момент времени $t \in (t_0, t_N]$ характеризуется системой обыкновенных линейных дифференциальных уравнений, в которой в качестве переменных рассматриваются численности состояний $z_i, i = 1, \dots, 6$:

$$\left\{ \begin{array}{l} \frac{dz_1}{dt} = \dot{z}_1(t) = -\lambda_4 \cdot p_{14} \cdot v_1 \cdot z_4 - \lambda_6 \cdot p_{16} \cdot v_2 \cdot z_6 + \delta z_1 \cdot \gamma(z_1, Z_1^*) \\ \frac{dz_2}{dt} = \dot{z}_2(t) = -\lambda_4 \cdot p_{24} \cdot v_2 \cdot z_4 + \delta z_2 \cdot \gamma(z_2, Z_2^*); \\ \frac{dz_3}{dt} = \dot{z}_3(t) = -\lambda_6 \cdot p_{36} \cdot v_4 \cdot z_6; \\ \frac{dz_4}{dt} = \dot{z}_4(t) = -\lambda_3 \cdot p_{43} \cdot u_1 \cdot z_3; \\ \frac{dz_5}{dt} = \dot{z}_5(t) = -\lambda_3 \cdot p_{53} \cdot u_2 \cdot z_3; \\ \frac{dz_6}{dt} = \dot{z}_6(t) = -\lambda_3 \cdot p_{63} \cdot u_3 \cdot z_3. \end{array} \right. \quad (3)$$

Здесь $\delta z_1 \cdot \gamma_1(z_1, Z_1^*)$ – модель введения резерва для восстановления (пополнения) численности состояний z_1 ; $\delta z_2 \cdot \gamma_2(z_2, Z_2^*)$ – модель введения резерва для восстановления (пополнения) численности состояний z_2 ; Z_1^* и Z_2^* – пороговые значения численностей состояний z_1 и z_2 , при достижении которых в действие вводится резерв из состава СПЗ; δz_1 и δz_2 – интенсивности введения резервных z_1 и z_2 ; $\gamma_1(z_1, Z_1^*)$ и $\gamma_2(z_2, Z_2^*)$ – сигнальные функции, определяемые по формулам:

$$\gamma_1(z_1, Z_1^*) = \begin{cases} 1, & \text{если } z_1(t) \leq Z_1^*; \\ 0, & \text{если } z_1(t) > Z_1^*. \end{cases} \quad \gamma_2(z_2, Z_2^*) = \begin{cases} 1, & \text{если } z_2(t) \leq Z_2^*; \\ 0, & \text{если } z_2(t) > Z_2^*. \end{cases}$$

Введём вспомогательные переменные $A_k, k=1, \dots, 7$ для обозначения для коэффициентов дифференциальных уравнений:

$$\begin{aligned} A_1 &= -\lambda_4 \cdot p_{14} \cdot v_1; & A_2 &= -\lambda_6 \cdot p_{16} \cdot v_3; \\ A_3 &= -\lambda_4 \cdot p_{24} \cdot v_2; & & \\ A_4 &= -\lambda_6 \cdot p_{36} \cdot v_4; & A_5 &= -\lambda_3 \cdot p_{43} \cdot u_1; \\ A_6 &= -\lambda_3 \cdot p_{53} \cdot u_2; & A_7 &= -\lambda_3 \cdot p_{63} \cdot u_3. \end{aligned} \quad (4)$$

Здесь $\lambda_i, i=1, \dots, 6$ – интенсивности атак (контратак), выполняемых средствами $z_i, i=1, \dots, 6$, соответственно; p_{ij} – вероятность поражения единицы средства z_i в результате атаки со стороны средства z_j ; u_1, u_2 и u_3 – доли средств z_3 стороны **A**, участвующих в подавлении средств z_4, z_5 и z_6 стороны **B** соответственно; v_1 и v_2 – доли средств z_4 стороны **B**, участвующих в подавлении соответственно средств z_1 и z_2 стороны **A**; v_3 и v_4 – доли средств z_6 стороны **B**, участвующих в подавлении соответственно средств z_1 и z_3 стороны **A**.

После преобразований системы дифференциальных уравнений (3) с учётом введённых обозначений (4) получим:

$$\begin{cases} \dot{z}_1(t) = A_1 \cdot z_4 + A_2 \cdot z_6 + \delta z_1 \cdot \gamma_1(z_1, Z_1^*); \\ \dot{z}_2(t) = A_3 \cdot z_4 + \delta z_1 \cdot \gamma_2(z_2, Z_2^*); \\ \dot{z}_3(t) = A_4 \cdot z_6; \\ \dot{z}_4(t) = A_5 \cdot z_3; \\ \dot{z}_5(t) = A_6 \cdot z_3; \\ \dot{z}_6(t) = A_7 \cdot z_3. \end{cases} \quad (5)$$

Здесь δz_1 – интенсивность ввода резерва, единиц/час; $\gamma(t)$ – сигнальная функция (окно на оси времени), которая позволяет выбрать интервал ввода резерва в средства $z_1(t)$; время среза $\Delta t_{\text{среза}} = t_{\text{к.вв}} - t_{\text{н.вв}}$. u_1, u_2 и u_3 – относительные доли (в %) средств z_3 стороны **A**, участвующих в информационном подавлении средств z_4, z_5 и z_6 соответственно; при этом должно выполняться дисциплинирующее условие: $u_1 + u_2 + u_3 \leq 1$.

Соотношения $u_1/u_2/u_3 = a/b/c$ определяют стратегию игрока **A** в отражении информационных атак игрока **B**. Соотношения $v_1/v_2/v_3 = w/d/r$ определяют стратегию игрока **B** в организации информационных атак на средства игрока **A**; v_1 и v_2 – доли (%) потенциала средства z_4 стороны **B**, участвующего в информационном подавлении средства z_1 и z_2 стороны **A**, причем должно выполняться условие: $v_1 + v_2 \leq 1$; v_3 и v_4 – доли (в %) потенциала средства z_6 стороны **B**, участвующего в информационном подавлении средств z_1 и z_3 стороны **A** соответственно; при этом должно выполняться условие: $v_3 + v_4 \leq 1$; $p_{ij}, i, j = \overline{1, 6}$ – вероятность информационного подавления средства i -го типа средством j -го типа.

В интересах удобства алгоритмизации введём **дополнительные условия**:

1. Резерв для пополнения элементов в состоянии z_1 используется при выполнении условия: $z_1(t) \leq 80 \% \cdot z_1(t_0)$; резерв для пополнения элементов в состоянии z_2 используется при выполнении условия: $z_2(t) \leq 80 \% \cdot z_2(t_0)$.

2. Каждое из средств z_i , $i = \overline{1,6}$, имеет только два состояния: рабочее и нерабочее (без возможности восстановления).

3. Начальные условия приняты следующими:

$$z_1(t_0) = z_2(t_0) = 100; \quad z_3(t_0) = z_5(t_0) = 100; \quad z_4(t_0) = z_6(t_0) = 100.$$

$$\lambda_3 = 0,12 \text{ мин}^{-1}; \lambda_4 = 0,15 \text{ мин}^{-1}; \lambda_6 = 0,06 \text{ мин}^{-1};$$

$$\delta z_1 = 0,18 \text{ мин}^{-1}; \delta z_2 = 0,12 \text{ мин}^{-1}.$$

С учётом анализа информационных угроз и имеющегося опыта исследования СЗИ приняты фиксированные стратегии $\{u\}$ и $\{v\}$ игроков А и В:

$$u_1 = u_2 = 0,2; \quad u_3 = 0,3; \quad v_1 = 0,5; \quad v_2 = 0,25; \quad v_4 = 0,4; \quad v_3 = 0,35.$$

Значения вероятностей поражения одной единицы средств игроков А и В примем в соответствии с данными таблицы 1.

Таблица 1. Вероятности поражения элементов

Игрок А				Игрок В		
p14	p16	p24	p36	p43	p53	p63
0,014	0,010	0,012	0,03	0,012	0,009	0,017

Моделирование (численное решение) системы дифференциальных уравнений выполнено в цикле на интервале времени $[t_0, t_N]$: $t_0 = 0$ мин., $t_N = 180$ мин. с шагом $\Delta t = 0,1$ мин.

Выход из цикла моделирования (решения) осуществлялся в одном из следующих случаев: $\{z_1 \leq 10; z_2 \leq 10; z_3 \leq 10; z_4 \leq 5; z_5 \leq 10; z_6 \leq 5\}$.

В качестве выходных данных при моделировании фиксируются: время решения задачи $t_{\text{реш}}$, тождественно равное времени информационного взаимодействия t^* : $t_{\text{реш}} = t^*$; численные значения переменных $z_i(t^*)$, $i = \overline{1,6}$; строятся графики $z_i = f_i(t)$, $i = \overline{1,6}$; $t \in [t_0, t^*]$ в двух системах координат (рис. 2 и рис. 3).

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 , $i = \overline{1,6}$, игроков А и В. Результаты расчёта показателей относительного ущерба $\Delta Z_i(t^*)$ для фиксированных исходных данных приведены в табл.2.

Результаты цифрового моделирования фазовой траектории в виде таблиц или графиков изменения во времени фазовых координат z_i , $i = \overline{1,6}$, позволяют проследить динамику взаимодействия СЗИ со злоумышленником и косвенно оценить результативность используемых механизмов комплексной защиты ресурсов КВС.

Таблица 2. Показатели относительного ущерба (%) для средств игроков в контрольной точке $t^* = T = 120$ (мин.)

Средства игрока А			Средства игрока В		
$\Delta Z_1(t^*)$	$\Delta Z_2(t^*)$	$\Delta Z_3(t^*)$	$\Delta Z_4(t^*)$	$\Delta Z_5(t^*)$	$\Delta Z_6(t^*)$
14,81	5,30	8,33	3,31	2,48	7,03

Рис. 1. Операционная схема информационного конфликта

Рис. 2. Изменение численности состояний z_1, z_2, z_3 от времени информационного контакта T (мин.) игроков А и В

Рис. 3. Изменение численности состояний z_4, z_5, z_6 от времени информационного противоборства T (мин.) игроков А и В

Для рассмотренной задачи совокупный ущерб противоборствующих сторон А и В, вычисленный по формулам (2) при учёте данных табл.2 для случая равных весовых коэффициентов $\alpha_i = \text{const} = 1$ и $\beta_i = \text{const} = 1$, составил (y.e.):

$$W_A = \sum_{i=1}^3 \alpha_i \cdot \Delta Z_i = 28,436 \% \text{ и } W_B = \sum_{i=4}^6 \beta_i \cdot \Delta Z_i = 12,817 \%.$$

Результаты операционного моделирования дают основание для аналитического анализа результативности используемых механизмов защиты ресурсов КВС при возможных вариантах и сценариях информационного взаимодействия игроков **А** и **В**. На основе вычислительного эксперимента, в частности, установлено, что прямой способ повышения эффективности МЗР через снижение уязвимости средств z_1 , z_2 и z_3 не является продуктивным. Так, за счёт уменьшения вероятностей поражения единиц средства z_1 в два раза совокупный ущерб W_A игрока **А** может снизиться всего на 8,6 %. Этот результат не окупает тех материальных затрат, которые требуются для разработки и внедрения в состав СЗИ соответствующих аппаратно-программных средств. Вопреки ожиданиям, незначительный эффект (всего 3,7 %) даёт и смещение акцентов информационных контратак средства z_3 в направлении средства z_6 .

В результате исследования определено, что более значительного приращения эффективности МЗР следует ожидать в случае комплексного (согласованного по целям, задачам и времени) применения нескольких способов пассивной и активной защиты сетевых ресурсов КВС [5]. Закономерным итогом комплексирования способов защиты будет существенное снижение интенсивности информационных атак со стороны средств z_4 и z_6 и ослабление уязвимости средств игрока **А**. В качестве перспективного направления обеспечения заданного уровня защищённости сетевых ресурсов КВС можно указать совместное применение рекомендаций и структурных решений теории обманных систем и алгоритмов интеллектуального управления МЗР [2].

Таким образом, изложенный игровой подход к операционному моделированию информационного противоборства СЗИ со злоумышленником в условиях отсутствия доступных для инженерной практики аналитических методик анализа рисков ИБ является удобным способом приближённой оценки эффективности механизма защиты сетевых ресурсов.

Список используемых источников:

1. Малюк А.А. Теория защиты информации. М.: Горячая линия-Телеком. 2012. 184 с.
2. Надеждин Е.Н. Проблемные вопросы управления рисками информационной безопасности в сфере образования // Научный поиск. 2012. №2.6. С.50-56.
3. Надеждин Е.Н., Смирнова Е.Е. Игровой подход к оценке защищённости информации в корпоративной вычислительной сети. Тула: Тульский артиллерийский инженерный институт, 2006.
4. Надеждин Е.Н. Игровой подход к задачам моделирования информационного противоборства и оценки рисков автоматизированных информационных систем. Тула, 2014.
5. Надеждин Е.Н., Смирнова Е.Е., Шершакова Т.Л. Математические основы моделирования и анализа интегрированных систем защиты информации: учебное пособие. Тула: Московский институт комплексной безопасности, 2013. 206 с.
6. Надеждин Е.Н., Смирнова Е.Е. Методы моделирования и оптимизации интегрированных систем управления организационно-технологическими процессами в образовании: монография. Тула: Изд-во ТулГУ, 2013. 250 с.

7. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие; Гос. ун-т – Высшая школа экономики. М.: Изд. дом гос. ун-та – Высшей школы экономики, 2011. 572 с.
8. Чуев Ю.В. Исследование операций в военном деле. М.: Воениздат МО, 1970. 256 с.

References:

1. Malyuk A.A. *The Theory of information security*. M.: Hot line-Telecom. 2012. 184 p.
2. Nadezhdin E.N. *Issues of risk management of information security in education* // *Scientific search*. 2012. No. 2.6. P. 50-56.
3. Nadezhdin E.N., Smirnova E.E. *The game approach to the assessment of information security in corporate computer networks*. Tula: Tula artillery engineering Institute, 2006.
4. Nadezhdin E.N. *The game approach to the modeling of information warfare and risk assessment of automated information systems*. Tula: Tula state pedagogical University named after L.N. Tolstoy, 2014.
5. Nadezhdin E.N., Smirnova E.E., Shershakova T.L. *Mathematical foundations of modeling and analysis of integrated systems of information protection: a training manual*. Tula: Moscow Institute of complex security, 2013. 206 p.
6. Nadezhdin E.N., Smirnova E.E. *Methods of modeling and optimization of integrated management systems, technological-organizational processes in education: monograph*. Tula: Publishing house of TSU, 2013. 250 p.
7. Serdyuk V.A. *Organization and technology of information protection: the detection and prevention of information attacks in auto-specialized systems of enterprises: textbook*; State. University – Higher school of Economics. M.: Izd. house state University – Higher school of Economics, 2011. 572 p.
8. Chuev Yu.V. *Operations Research in military Affairs*. M.: Voenizdat MO, 1970. 256 p.

© 2015, Надеждин Е.Н.

Оценка эффективности механизма защиты сетевых ресурсов на основе игровой модели информационного противоборства

© 2015, Nadezhdin E.N.

Evaluation of the effectiveness of the protection mechanism of network resources based gaming model of information warfare