УДК 004.056

Надеждин Е.Н.
доктор технических наук, профессор
Тульский государственный педагогический университет имени Л.Н. Толстого
Шершакова Т.Л.
Филиал НОУ ВПО «Московский институт государственного управления и права» в Смоленской области

Игровой подход к определению защищённости ресурсов корпоративной информационной сети

В статье рассмотрена задача оценивания показателей защищённости информационных и программных ресурсов корпоративной информационной сети на основе игрового подхода к формализации процесса информационного противоборства. Разработана игровая модель, реализующая известный метод динамики средних. В ходе вычислительного эксперимента установлена линейная зависимость совокупного ущерба, обусловленного массированной атакой злоумышленника на сетевые ресурсы корпоративной информационной сети, от вероятностного показателя уязвимости программных модулей. Для нейтрализации существующих уязвимостей программного обеспечения и обеспечения заданного уровня защищённости сетевых ресурсов предлагается внедрение гибких механизмов интегрированной защиты информации.

Ключевые слова. *корпоративная информационная сеть, информационное противоборство, сетевые ресурсы, игровая модель, относительный совокупный ущерб.*

Инновационный характер и оригинальные результаты современных ИТ-проектов, успешно реализуемых коллективами ведущих проектно-конструкторских организаций (ПКО) России, вызывает повышенный интерес зарубежных конкурирующих фирм. Последние используют все доступные способы и средства для получения доступа к конфиденциальной информации. В этой связи существенно обострилась проблема обеспечения политики информационной безопасности (ИБ) ПКО [2, 4]. В настоящее время особенно актуальны вопросы создания гибких механизмов защиты ресурсов (МЗР) корпоративных информационных сетей (КИС) от массированных атак потенциальных злоумышленников [3, 6]. Возросший поток научных публикаций, посвящённых разработке методов интеллектуального анализа угроз и управления рисками ИБ, убедительно свидетельствует о нерешённости проблемы гарантированной защиты сетевых ресурсов ПКО.

Известные аналитические методики расчёта показателей защищённости активов КИС и оценки эффективности используемых МЗР ориентированы на идеализированные условий применения и во многих случаях не позволяют получить корректные прогностические оценки и практические рекомендации.

Целью статьи является обоснование игрового подхода к анализу влияния уровня защищённости программного обеспечения (ПО) узлов КИС на ве-

личину совокупного ущерба, обусловленного реализацией информационных атак злоумышленника на сетевые ресурсы.

Для решения указанной задачи воспользуемся методикой имитационного моделирования процесса информационного противоборства двух автоматизированных информационных систем (АИС), которая представлена в ранее опубликованных статьях [3, 5]. Опираясь на базовую вычислительную схему метода динамики средних [1], уточним на содержательном уровне задачу игрового моделирования процесса информационного противоборства АИС.

Пусть требуется оценить эффективность защиты ресурсов КИС путём исследования процесса информационного противоборства системы защиты информации (СЗИ) КИС и некоторого условного «злоумышленника».

Принципиальной особенностью используемого авторами модельного подхода является формальное представление объекта исследования как динамической системы (ДС) «*Система защиты информации – злоумыш-ленник*» («СЗИ-ЗЛ»), функционирующей на заданном интервале времени $[t_0, t_N]$. Вектор фазовых координат ДС в момент времени $t \in (t_0, t_N]$ 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 $Z(t) \quad \forall\, t \in (t_0, t_N]$ позволяет получить исчерпывающую информацию о процессах в структуре ДС. 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, $i = \overline{1,n}$, вычисляют по формуле:

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

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.

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

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

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 решение задачи оценки ущерба, нанесённого КИС в результате информационного противоборства со злоумышленником. Для определённости в качестве сетевых ресурсов, подверженных атакам злоумышленника, будем рассматривать программное обеспечение узлов КИС. На рис. 1 представлена укрупнённая операционная схема многоканального информационного взаимодействия подсистем ДС «СЗИ-ЗЛ». При этом введены следующие обозначения: ***игрок A*** - СЗИ; ***игрок B*** - злоумышленник, пытающийся преодолеть защиту и получить доступ к сетевым ресурсам.

В структуре СЗИ (*игрок A*) выделены следующие элементы: специальное программное обеспечение (СПО), общее программное обеспечение (ОПО), средства пассивной защиты (СПЗ) и средства активной защиты (САЗ). В модели злоумышленника (*игрок B*) выделены: средства активного нападения первого и второго типов ($САН_1$ и $САН_2$) и система координации и управления (СКУ) ими. Будем полагать, что СПЗ используются для обнаружения, локализации и восстановления повреждённых программных модулей ОПО и СПО.

Для формализованного представления ДС «КВС-ЗЛ» введены переменные $z_i, i = 1,...,6$, под которыми будем понимают численности состояний соответственно следующих элементов: ОПО, СПО и средств активной защиты подсистемы **A**, а также средств активного нападения первого типа, СКУ и средств активного нападения второго типа подсистемы **B.** Состояние ДС «КВС-ЗЛ» в каждый момент времени $t \in (t_0, t_N]$ характеризуется системой обыкновенных дифференциальных уравнений, в которой в качестве переменных рассматриваются численности состояний $z_i, i = 1,...,6$:

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

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:

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

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

$$A_1 = -\lambda_4 \cdot p_{14} \cdot v_1; \qquad A_2 = -\lambda_6 \cdot p_{16} \cdot v_3;$$
$$A_4 = -\lambda_6 \cdot p_{36} \cdot v_4; \qquad A_3 = -\lambda_4 \cdot p_{24} \cdot v_2;$$
$$A_6 = -\lambda_3 \cdot p_{53} \cdot u_2; \qquad A_5 = -\lambda_3 \cdot p_{43} \cdot u_1; \qquad A_7 = -\lambda_3 \cdot p_{63} u_3.$$

(4)

Здесь $\lambda_i, i = 1,...,6$ - интенсивности атак (контратак), выполняемых средствами $z_i, i = 1,...,6,$ 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 **А**, участвующих в подавлении средств z_4, z_5 и z_6 стороны **В** соответственно; v_1 и v_2 - доли средств z_4 стороны **В**, участвующих в подавлении соответственно средств z_1 и z_2 стороны **А**; v_3 и v_4 - доли средств z_6 стороны **В**, участвующих в подавлении соответственно средств z_1 и z_3 стороны **А**.

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

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

(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 $\Delta t_{среза} = t_{к.вв} - t_{н.вв}$. 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: $u_1 + u_2 + u_3 \le 1$.

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: $v_1 + v_2 \le 1$; 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: $v_3+v_4 \le 1$; $p_{ij}, i, j = \overline{1,6}$ - 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: $z_1(t) \le 80\ \% \cdot z_1(t_0)$; резерв для пополнения элементов в состоянии z_2 используется при выполнении условия: $z_2(t) \le 80\ \% \cdot z_2(t_0)$.

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:

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

$\lambda_3 = 0{,}12$ мин$^{-1}$; $\lambda_4 = 0{,}15$ мин$^{-1}$; $\lambda_6 = 0{,}06$ мин$^{-1}$; $\delta z_1 = 0{,}18$ мин$^{-1}$; $\delta z_2 = 0{,}12$ мин$^{-1}$.

4. С учётом анализа информационных угроз и имеющегося опыта исследования СЗИ приняты фиксированные стратегии $\{u\}$ и $\{v\}$ игроков A и B:

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

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

Таблица 1. Вероятности поражения элементов

Игрок A				***Игрок B***		
p_{14}	p_{16}	p_{24}	p_{36}	p_{43}	p_{53}	p_{63}
0,004	0,004	0,004	0,005	0,012	0,009	0,017

5. 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.

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

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

Используя данные об изменении численностей состояний ДС 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 КИС.

Таблица 2. Показатели относительного ущерба (%) для средств игроков в контрольной точке $t^* = T = 180\,(мин.)$

Средства игрока **А**			Средства игрока **В**		
$\Delta Z_1(t^*)$	$\Delta Z_2(t^*)$	$\Delta Z_3(t^*)$	$\Delta Z_4(t^*)$	$\Delta Z_5(t^*)$	$\Delta Z_6(t^*)$
7,28	2,59	2,09	7,69	3,85	6,41

Для количественной оценки влияния уязвимости ПО на относительный совокупный ущерб КИС проведена серия вычислительных экспериментов, в результате которых построены графики (рис. 3). Зависимость относительного совокупного ущерба $W_A = W1$ от вероятности поражения программного модуля $P_{ПО}$ (рис.3) аппроксимирована с помощью функции линейной регрессии вида $W1 = a + b \cdot P_{ПО}$, где коэффициенты регрессии $a = 2{,}632$ и $b = 2322$.

На основе вычислительного эксперимента установлено, что прямой путь повышения эффективности МЗР через снижение уязвимости средств z_1, z_2 и z_3 является весьма ресурсозатратным. Для существенного приращения эффективности МЗР можно рекомендовать одновременное применение нескольких способов пассивной и активной защиты ПО узлов КИС. Закономерным итогом комплексирования способов защиты в составе интегрированных МЗР будет

«закрытие» уязвимостей программного обеспечения и существенное снижение результативности информационных атак со стороны средств z_4 и z_6.

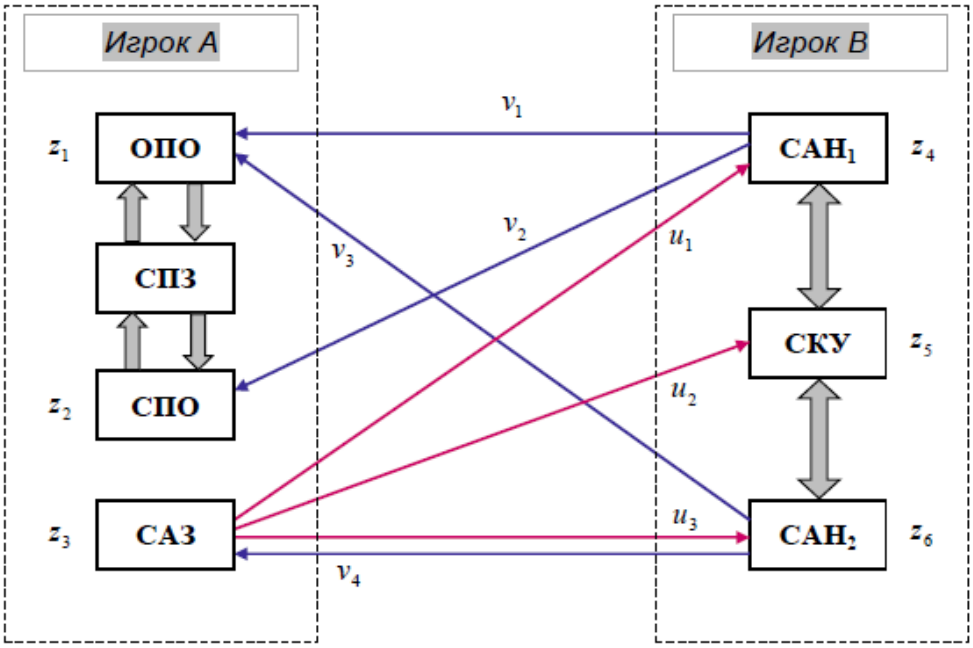

Рис. 1. Операционная схема информационного противоборства

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

$$W_A = \sum_{i=1}^{3} \alpha_i \cdot \Delta Z_i = 30{,}25\,\% \quad \text{и} \quad W_B = \sum_{i=4}^{6} \beta_i \cdot \Delta Z_i = 16{,}98\,\%.$$

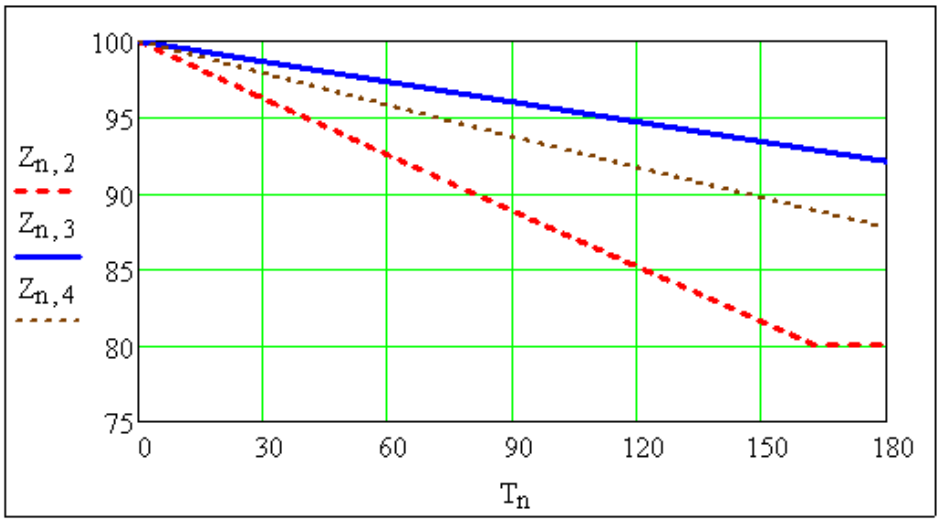

Рис. 2. Изменение численности состояний z_1, z_2, z_3 от времени информационного контакта T (мин.) игроков **A** и **B**

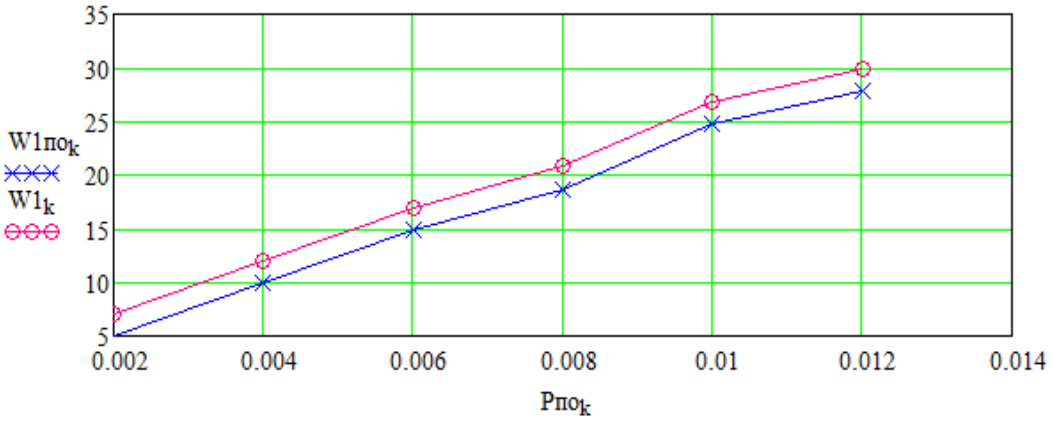

Рис. 3. Зависимость относительного совокупного ущерба от уязвимости ограммных модулей КИС (для случая: $P_{ПО} = p_{1,4} = p_{1,6} = p_{2,4}$; $p_{3,6} = 0{,}005$)

Таким образом, результаты игрового моделирования процесса информационного противоборства дают основание для детального критического анализа функционирования и оценки показателей эффективности используемых МЗР. Унификация и гибкость вычислительной схемы игровой модели позволяют получить обоснованные прогностические оценки для всего набора ожидаемых вариантов развития информационного противоборства СЗИ КИС со злоумышленником.

ЛИТЕРАТУРА

1. Абчук В.А. Справочник по исследованию операций / В.А Абчук., Ф.А. Матвейчук, Л.П. Томашевский; Под общ. ред. Ф.А.Матвейчука. – М.: Воениздат, 1979. 368 с.
2. Михайлов Ю.Б. Научно-методические основы обеспечения безопасности защищаемых объектов. - М.: Горячая линия – Телеком, 2015. 322 с.
3. Надеждин Е.Н. Оценка эффективности механизма защиты сетевых ресурсов на основе игровой модели информационного противоборства // Научный вестник. 2015. № 2(4). С. 49-58.
4. Надеждин Е.Н., Новикова Т.Л. Информационно-аналитическая поддержка деятельности аудитора информационной безопасности // Фундаментальные исследования. 2016. № 10 (часть 1). С. 67-72.
5. Надеждин Е.Н. Оценка эффективности механизма защиты сетевых ресурсов на основе игровой модели информационного противоборства // Научный вестник. 2015. № 2(4). С. 49-58.
6. Сердюк В.А. Организация и технология защиты информации: обнаружение и предотвращение 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.

REFERENCES (TRANSLITERATED)

1. Abchuk V.A. Spravochnik po issledovaniju operacij / V.A Abchuk., F.A. Matvejchuk, L.P. Tomashevskij; Pod obshh. red. F.A.Matvejchuka. – M.: Voenizdat, 1979. 368 s.
2. Mihajlov Ju.B. Nauchno-metodicheskie osnovy obespechenija bezopasnosti zashhishhaemyh ob#ektov.- M.: Gorjachaja linija – Telekom, 2015. 322 s.

3. Nadezhdin E.N. Ocenka jeffektivnosti mehanizma zashhity setevyh resursov na osnove igrovoj modeli informacionnogo protivoborstva // Nauchnyj vest-nik. 2015. № 2(4). S. 49-58.

4. Nadezhdin E.N., Novikova T.L. Informacionno-analiticheskaja podderzhka dejatel'nosti auditora informacionnoj bezopasnosti // Fundamental'nye issledovanija. 2016. № 10 (chast' 1). S. 67-72.

5. Nadezhdin E.N. Ocenka jeffektivnosti mehanizma zashhity setevyh resursov na osnove igrovoj modeli informacionnogo protivoborstva // Nauchnyj vestnik. 2015. № 2(4). S. 49-58.

6. Serdjuk V.A. Organizacija i tehnologija zashhity informacii: obnaruzhenie i predotvrashhenie atak v avtomatizirovannyh sistemah predprijatij: uchebnoe posobie; Gos. un-t – Vysshaja shkola jekonomiki. – M.: Izd. dom Gos. un-ta – Vysshej shkoly jekonomiki, 2011. 572 s.

Nadezhdin E. N.
Doctor of technical Sciences, Professor, Tula state pedagogical University named after L. N. Tolstoy
Sharshakova T. L.
Branch NOU VPO "Moscow Institute of state management and law" in the Smolensk region

GAME APPROACH TO DEFINITION OF PROTECTION RESOURCES OF THE CORPORATE INFORMATION NETWORK

The article considers the task of evaluating the protection of informational and program resources of the corporate information network based on the game approach to the formalization of the information confrontation process. A game model has been developed that implements the known method of the dynamics of averages. On the basis of the computational experiment, a linear dependence of the cumulative damage caused by a massive attack of the attacker on the network resources of the corporate information network is established on the probabilistic index of the vulnerability of program modules. To neutralize existing software vulnerabilities and provide a given level of protection of network resources, it is proposed to implement flexible mechanisms for integrated information protection.

Keywords: *corporate information network, information confrontation, network resources, game model, relative cumulative damage.*

Сведения об авторах:

*Надеждин Евгений Николаевич***,** доктор технических наук, профессор, ФГБОУ ВО «Тульский государственный педагогический университет имени Л.Н. Толстого», 300026, г. Тула, проспект Ленина, 125, E-mail: en-hope@yandex.ru

Шершакова Татьяна Леонидовна, начальник отдела контроля качества обучения, Филиал НОУ ВПО «Московский институт государственного управления и права» в Смоленской области, 214012, г. Смоленск, ул. Ново-Московская, д. 2/8; E-mail: tshershakova@mail.ru

Nadezhdin Evgeny Nikolaevich, Doctor of technical Sciences, Professor, Federal state budgetary educational institution of higher professional education "Tula state pedagogical University named after L. N. Tolstoy", Tula, Prospekt Lenina, 125; E-mail: en-hope@yandex.ru

Tshershakova Tatjana Leonidovna, Head of the Quality Control Department, Smolensk Branch of the Moscow Institute of Public Administration and Law , 214012, Smolensk, ul. Novo-Moscow, d. 2/8; E-mail: tshershakova@mail.ru

Ссылка для цитирования:

Надеждин Е.Н. , Шершакова Т.Л. Игровой подход к определению защищённости ресурсов корпоративной информационной сети // Наукосфера. 2017. №7. С. 19-28. URL: http://nmsjour.ru/doc/ns-2017-№7-Nadezhdin.pdf