DOI: 10.24143/2072-9502-2018-4-73-79
УДК 529.6

Г. А. Попов, Е. А. Попова, М. Г. Попова

СЕТЕВЫЕ МОДЕЛИ ПРОЦЕССОВ РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Цель исследования – анализ возможных путей распространения вредоносных программ (ВП) на основе взвешенных графов, где граф описывает взаимосвязи между различными программами, а веса отображают вероятности перехода ВП от одной программной системы (файла) к другой (к другому файлу). Решается задача выявления наиболее вероятных маршрутов распространения ВП и выявления наиболее вероятных путей их проникновения к заданному программному продукту. Для решения указанной задачи предлагается использовать метод динамического программирования. Процедура решения задачи продемонстрирована на конкретном примере. По результатам вычислений найден наиболее вероятный маршрут проникновения и оценена вероятность успешной реализации атаки ВП на программный продукт. Методы теории графов позволили также оценить ряд других числовых характеристик, связанных с процессом распространения ВП, к которым отнесены минимальное число тактов работы системы, после реализации которых возможно проникновение ВП к заданному программному продукту; количество тактов работы системы, когда вероятность проникновения ВП к конкретному файлу станет больше заданной величины. Кроме того, метод позволяет выявить циклические маршруты распространения ВП, характеризующие повторные попытки воздействия ВП на программный продукт, найти наиболее вероятные источники (файлы) распространения ВП, найти множество тех файлов, откуда возможно проникновение ВП к заданному программному продукту.

Ключевые слова: вредоносная программа, программный продукт, графы, маршрут проникновения, метод динамического программирования.

Введение

Проблема защиты вычислительных систем от компьютерных вредоносных программ (ВП), в частности компьютерных вирусов, является и еще долго будет оставаться актуальной, поскольку, во-первых, в настоящее время существует огромное количество ВП, на поиск и выявление которых затрачиваются значительные компьютерные ресурсы, что часто является неудобным и даже неприемлемым; во-вторых, интервал времени между появлением новых ВП (вирусов) и средств противодействия им обычно составляет несколько месяцев, в течение которых компьютерная среда подавляющего большинства пользователей совершенно беззащитна по отношению к этим ВП; в-третьих, активное присутствие подавляющего большинства людей в глобальной сети Интернет, которая является одним из наиболее опасных каналов проникновения компьютерных вирусов, существенно повышает вероятность заражения пользовательского компьютера вредоносными программами.

Проблеме анализа процесса распространения вирусных и иных атак на пользовательские рабочие места посвящено много работ, в частности [1–3]. Однако работ, опирающихся при анализе на методы теории графов, крайне мало [3, 4]. Близкой работой является [5]. Ниже предлагается один из возможных подходов к анализу различных характеристик, связанных с вирусными атаками, на основе методов теории графов. Среди зарубежных изданий отметим работы [6, 7].

Оценка основных характеристик процесса распространения вредоносных программ

Представим процесс распространения ВП в виде графа следующим образом. Рассмотрим процесс распространения ВП, привязанных к программным средствам либо информационным документам (назовем их объектами обработки (ОО)). В этом случае граф отображает взаимосвязи между различными ОО и, как следствие, потенциальные пути распространения ВП от одних ОО к другим. Граф является ориентированным, направление дуги (стрелка) указывает на тот ОО, в который может проникнуть ВП из ОО, примыкающего к началу дуги. Заданы также вероятности $\{ p_i^{\text{ВП}}, 1 \le i \le N\}$ (N – число всех вершин графа) того, что атака ВП на i-й узел графа окажется успешной. Тогда типовые методы анализа характеристик графов [7] позволяют оценить ряд важных характеристик распространения ВП. Перечислим эти характеристики.

1. Для j-го объекта графа (т. е. вершины графа) найти длину $\Pi_{\text{нач}}(j)$ цепочки минимальной длины, т. е. номер такта процесса функционирования сети и связанного с этим процесса обработки объектов, к которому хотя бы один из ОО, из которых может произойти обращение (запуск, обработка и т. п.) к j-му объекту, уже мог быть подвергнут воздействию ВП. То есть $\Pi_{\text{нач}}(j)$ есть минимальный номер такта обработки данных, на котором j-й ОО может уже быть подвергнут воздействию ВП. Ниже $a_{ij}^{(m)}$ есть вероятность того, что на m-ом такте i-й ОО обратится к j-му.

Для вычисления $\Pi_{\text{нач}}(j)$ находится наибольшее число $k \le N$ такое, что $a_{ij}^{(k-1)} > 0$ хотя бы для одного i и $a_{ij}^{(m)} = 0$ для всех текущих i и m, таких, что $m \le k$. Если $a_{ij}^{(m)} > 0$ для всех $m = \overline{1;N}$, то полагаем $k = N$. Здесь матрица $\left\| a_{ij}^{(k)} \right\| = A^k$. Полагаем $\Pi_{\text{нач}}(j) = k$. При этом вероятность $q_j^{(1)}$ того, что ВП воздействовала на j-й ОО, равна сумме (i, j)-х элементов матрицы $P^k = \left\| \pi_{ij}^{(k)} \right\|_{i,j=1}^{N}$, где $P = \left\| a_{ij} p_i \right\|_{i,j=1}^{N}$, т. е. $q_j = \sum_{i=1}^{N} \pi_{ij}^{(k)}$.

2. Для j-го ОО найти длину цепочки (номер такта движения обработки объектов) $\Pi^{\max}(j, p_{\text{доп}})$, к которому вероятность $q_j^{(2)}$ воздействия ВП на j-й объект будет больше заданного уровня $p_{\text{доп}}$, либо $q_j^{(2)}$ достигает своего наибольшего значения. То есть $\Pi(j)$ есть наименьший момент, когда заражение j-го ОО станет недопустимо большим либо максимально возможным. Данная характеристика учитывает возможность циклической взаимосвязи объектов друг с другом, при которой заражение объекта вредоносной программой может произойти на одном циклов.

Для вычисления $q_j^{(2)}$ находится наименьшее число k такое, что либо $\sum_{i=1}^{N} \pi_{ij}^{(k)} \ge P_{\text{доп}}$, либо $\pi_{ij}^{(k)} > 0$ и $\pi_{ij}^{(m)} = 0$ для всех $m = \overline{k+1;k+N}$ хотя бы для одного i, и $a_{ij}^{(m)} = 0$ для всех i и m таких, что $k \le m \le 10$. Если $a_{ij}^{(10)} > 0$, то полагаем $k = 10$. Здесь матрица $\left\| a_{ij}^{(k)} \right\| = A^k$. Полагаем $\Pi(j) = k$.

Затем находится величина $N = \max_{1 \le i \le 10} \Pi(j)$ – номер такта, к которому все ОО уже подвергнуты воздействию угроз.

3. Выяснить, есть ли циклические маршруты взаимосвязи ОО, что создает возможности для повторных атак. Для этого вычислить матрицу $\Omega = \sum_{k=1}^{10} A^k$.

Если матрица Ω имеет ненулевые элементы на диагонали, то в системе имеются циклы. Матрица A^n имеет квадратично-блочную структуру. При этом номера строк (столбцов), описывающих один квадратичный блок, указывают на номера вершин, образующих цикл.

4. Найти концевые (исходные и конечные) ОО. Исходным ОО соответствуют столбцы матрицы A, в которых все элементы нулевые. Конечным документам соответствуют строки матрицы A, в которых все элементы равны 0. Оценить степень опасности (как источника угроз) каждого исходного ОО для каждого конечного ОО. В качестве меры важности взять число путем l_{ij}, соединяющим исходную вершину под номером i с конечной вершиной под номером j, $l_{ij} = w_{ij}$, где $\left\| w_{ij} \right\| = \Omega$. Вывести для каждой конечной вершины список важностей различных исходных вершин.

5. Для каждого документа определить номер такта τ_i, к которому этот документ окажет вредоносное воздействие на другие документы: $\tau_i = \max_{1 \le i \le 10} w_{ij}$.

Оценить число тактов t_i, в течение которых i-й ОО активен: $t_i = \tau_i - \Pi(i)$.

Найти время T заражения системы: $T = \max_{1 \le i \le 10} \tau_i$. Для многозвенной (многоэшелонированной) структуры системы время заражения может достигать своего максимального значения: $T = N = 10$.

Оценить оперативность L заражения системы: $L = \max_{1 \le i \le 10} t$.

6. Для каждого ОО найти множество R_i тех ОО, которые могут воздействовать на i-й ОО. R_i есть множество номеров j, таких, что $w_{ji} \neq 0$.

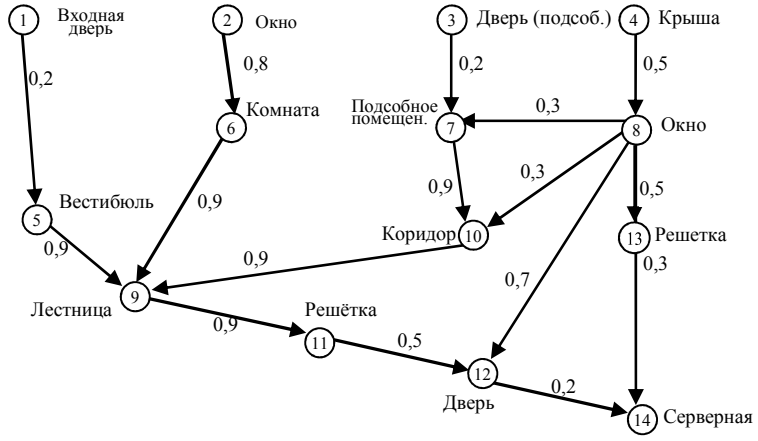
Для каждого ОО найти множество Q_i таких ОО, которые могут воздействовать (заразить вирусом) i-й ОО. Q_i есть множество номеров столбцов, таких, что $w_{ji} \neq 0$.

Сделать выводы по результатам вычислений.

Нахождение наиболее опасных путей распространения вирусных атак

Рассмотрим задачу выявления наименее защищенных маршрутов проникновения на объект защиты. Данная задача актуальна при обеспечении структурно-технологической комплексности.

Приведем постановку задачи. На основе анализа объекта защиты (в качестве объекта защиты был выбран один из фрагментов вуза) и экспертной оценки (в качестве экспертов были выбраны пять студентов группы; процедура проведения экспертизы описана выше) вероятностей движения угрозы (в частности, злоумышленника) от одной точки объекта защиты к другой, соседней (эти вероятности являются весами соответствующих ребер в графе), был сформирован граф проникновения, описывающий процесс движения угрозы (злоумышленника) по территории вуза (рис.) [8].



Граф проникновения на объект защиты

Таким образом, вершинами графа являются определенные ключевые места (точки) на плане объекта защиты – в данном случае территории здания вуза. Основное требование к выбору этих точек – они должны располагаться внутри участка территории, однородной по своим характеристикам безопасности.

Дуги графа отображают возможные направления перемещения злоумышленника по территории. Веса этих дуг (т. е. вероятности преодоления соответствующих участков территории) могут быть получены на основе экспертных методов либо путем проведения натурных экспериментов. Особое внимание следует обратить на выбор возможных точек проникновения в здание извне – это начальные точки искомого ориентированного графа. Этим точкам возможного проникновения в здание также приписываются весовые коэффициенты, описывающие относительные вероятности использования злоумышленником именно данной точки для проникновения в здание. Считаем, что все введенные вероятности описывают независимые события – это позволяет при расчетах пользоваться формулой умножения вероятностей. Конечными вершинами искомого ориентированного графа являются объекты интереса злоумышленника. В рассматриваемой задаче это серверное помещение. Тогда рассматриваемая задача может быть формализована следующим образом: выявить такой маршрут проникновения в серверное помещение, который имеет наибольшую вероятность проникновения.

Поставленная задача относится к классу задач поиска на графах. Имеется ряд алгоритмов ее решения [9]. Одним из возможных методов решения является метод динамического программирования (ДП) [10, 11]. Процесс решения задачи включает пять этапов [8]. На первом выделяются последовательные уровни достижения вершин (табл. 1).

Таблица 1

Разбиение графа на уровни иерархии

Этап просмотра графа	Вершины (в порядке просмотра)	Вершины (в порядке неубывания)	Этап решения (слой графа)
1	14	14	VIII
2	12, 13	12, 13	VII
3	11, 8	8, 11	VI
4	9, 4	**4**, 9	V
5	5, 6, 10	5, 6, 10	IV
6	1, 2, 7, 8	**1**, **2**, 7, 8	III
7	3, 8, 4	**3**, **4**, 8	II
8	4	**4**	I

На втором этапе вводится целевая функция – функция Беллмана $F_i(x_i)$, на третьем этапе записывается основное уравнение ДП – уравнение Беллмана. В рассматриваемой задаче функция Беллмана $F_i(x_i)$ есть максимальное значение вероятности проникновения злоумышленника из вершины x_i, входящей в i-й слой, в конечную (14-ю) вершину ($i = \overline{1,7}$). Для записи уравнения Беллмана необходимо ввести также переходные функции $f_i(x_i, y_i)$, описывающие успешное движение злоумышленника из вершины x_i, входящей в i-й слой, в вершину y_i, входящую в $(i + 1)$-й слой, если вершины соединены. В противном случае указанная вероятность равна нулю. Значениями функции $f_i(x_i, y_i)$ являются веса соответствующих дуг графа. В результате приходим к следующему уравнению Беллмана для рассматриваемой задачи: $F_i(x_i) = \max_{y_i}\left(f_i(x_i, y_i) \cdot F_{i+1}(y_i)\right)$, где максимум берется по всем вершинам y_i, входящим в $(I + 1)$-й слой. Полагаем по определению $F_8(x_8) \equiv 1$.

Четвертый этап, наиболее трудоемкий, заключается в построении таблиц расчета текущих вероятностей. В работе выбран метод ДП обратного хода, который лучше зарекомендовал себя при решении задач с неизменной (стационарной) структурой, каковой является и рассматриваемая задача. Поэтому вычисления выполняют, начиная с последнего этапа. Результаты вычислений приведены в табл. 2.

Таблица 2

Расчетные таблицы метода динамического программирования

№	Входная вершина	Переходная функция				Функция Беллмана	Выходная вершина
1	X_7	$f_7(x_7, y_7)$				$F_7(y_7)$	y_7
		$y_7 = 14$					
	12	0,2				0,2	14
	13	0,3				0,3	14
2	X_6	$f_6(x_6, y_6) \cdot F_7(y_6)$				$F_6(y_6)$	y_6
		$y_6 = 12$		$y_6 = 13$			
	8	0,7 · 0,2		0,5 · 0,3		0,15	13
	11	0,5 · 0,2		–		0,1	12
3	X_5	$f_5(x_5, y_5) \cdot F_6(y_5)$				$F_5(y_5)$	y_5
		$y_5 = 8$		$y_5 = 11$			
	4	0,5 · 0,15		–		**0,075**	8
	9	–		0,9 · 0,1		0,1	11
4	X_4	$f_4(x_4, y_4) \cdot F_5(y_4)$				$F_4(y_4)$	y_4
		$y_4 = 4$		$y_4 = 9$			
	5	–		0,9 · 0,1		0,09	9
	6	–		0,9 ·0,1		0,09	9
	10	–		0,9 · 0,1		0,09	9
5	X_3	$f_3(x_3, y_3)\ X_3\ F_3(y_3)$				$F_3(y_3)$	y_3
		$y_3 = 5$	$y_3 = 6$	$y_3 = 10$			
	1	0,2 · 0,09	–	–		**0,018**	5
	2	–	0,8 · 0,09	–		**0,072**	6
	7	–	–	0,9 · 0,09		0,081	10
	8	–	–	0,3 · 0,09		0,027	10
6	X_2	$f_2(x_2, y_2) \cdot F_2(y_2)$				$F_3(y_3)$	y_3
		$y_2 = 1$	$y_2 = 2$	$y_2 = 7$	$y_2 = 8$		
	3	–	–	0,2 · 0,081	–	**0,016 2**	7
	4	–	–	–	0,5 · 0,027	**0,013 5**	8
	8	–	–	0,3 · 0,081	–	0,024 3	7
7	X_1	$f_1(x_1, y_1) \cdot F_2(y_1)$				$F_1(y_1)$	y_1
		$y_1 = 3$	$y_1 = 4$	$y_1 = 8$			
	4	–	–	0,5 · 0,0243		**0,012 15**	8

В предпоследнем столбце (функция Беллмана) табл. 2 выделяются те значения, которые начинаются из какой-либо входной вершины X. Именно среди этих значений и следует выбирать наибольшее значение целевой функции. В рассматриваемой задаче это наибольшее значение равно 0,075 – это и есть наибольшее значение целевой функции.

На пятом этапе формируется непосредственно маршрут, на котором достигается указанное значение целевой функции. Из последней табл. 2 получаем, что максимальное значение достигается из входной вершины 4, из которой попадаем в вершину 8. Просматривая таблицы в обратном порядке, в результате получаем: из вершины 8 происходит переход в вершину 13, а из 13 – в конечную (14-ю). Таким образом, наиболее уязвимым маршрутом злоумышленного проникновения в защищаемое помещение (серверную) является следующий: 4 → 8 → 13→ 14, вероятность успешного проникновения по этому маршруту равна 0,075 (т. е. 7,5 %).

Можно также найти следующие, наиболее вероятные по опасности, маршруты проникновения. Для этого необходимо последовательно по убыванию значений выбирать вероятности из последних столбцов таблиц, полученных на четвертом этапе. В рассматриваемой задаче следующим по величине значением является 0,072 (или 7,2 %) от входной вершины X_3. Тогда аналогично предыдущему находим соответствующий маршрут: 2 → 6 → 9 → 11 → 12 → 14.

Другие возможные маршруты не рассматриваются ввиду незначительности соответствующих вероятностей.

Решение рассматриваемой задачи представляет особый интерес применительно к большим объектам. В этом случае граф проникновения может содержать очень много вершин и ребер, поэтому метод ДП может оказаться неэффективным. Таким образом, выбор метода решения поставленной задачи применительно к большим системам остается открытым. Отметим, что для больших систем граф проникновения может быть сформирован на основе автоматизированных процедур путем выделения однородных зон на плане объекта защиты.

Заключение

В работе рассматривается задача анализа возможных путей распространения вредоносных программ (ВП) на основе взвешенных графов, где граф описывает взаимосвязи между различными программами, а веса отображают вероятности перехода ВП от одной программной системы (файла) к другой (к другому файлу). Ставится задача выявления наиболее вероятных маршрутов распространения ВП и выявления наиболее вероятных путей их проникновения к заданному программному продукту. Предлагается для решения указанной задачи использовать метод динамического программирования. Процедура решения задачи продемонстрирована на конкретном примере. По результатам вычислений найден наиболее уязвимый маршрут проникновения и оценена вероятность успешной реализации атаки ВП на искомый программный продукт.

Методы теории графов позволили также оценить ряд других числовых характеристик, связанных с процессом распространения ВП, в частности минимальное число тактов работы системы, после реализации которых возможно проникновение ВП к заданному программному продукту; количество тактов работы системы, когда вероятность проникновения ВП к конкретному файлу станет больше заданной величины; выявить циклические маршруты распространения ВП, что характеризует повторные попытки воздействия ВП на программный продукт; найти наиболее вероятные источники (файлы), откуда началось распространение ВП; найти множество тех файлов, откуда возможно проникновение ВП к заданному программному продукту.

СПИСОК ЛИТЕРАТУРЫ

1. *Рудниченко А. К., Кошелек С. О.* Использование OLE-объектов в документах Vicrosoft Word как средство распространения вредоносных программ. Методы защиты от них // Молодой ученый. 2016. № 29 (135). С. 36–39.

2. *Зайцев О.* Технологии вредоносных программ и угрозы информационной безопасности. URL: https://compress.ru/Article.aspx?id=17361 (дата обращения: 17.06.18).

3. *Зикратов И. А., Василенко Р. С.* Поиск вредоносных программ на основе анализа процесса распространения. URL: https://cyberleninka.ru/article/n/poisk-vredonosnyh-programm-na-osnove-analiza-protsessa-rasprostraneniya-publikuetsya-v-poryadke-diskussii (дата обращения: 17.06.18).

4. *Курилов Ф. М.* Моделирование систем защиты информации. Приложение теории графов // Технические науки: теория и практика: материалы III Междунар. науч. конф. (Чита, апрель 2016 г.). Чита: Молодой ученый, 2016. С. 6–9.

5. *Shawn A.* List of Types of Malware May 24, 2017. URL: https://www.malwarefox.com/malware-types/ (дата обращения: 17.06.18).

6. *Wanping Liu, Shouming Zhong.* Web malware spread modelling and optimal control strategies // Scientific RepoRts. 10 February 2017. URL: www.nature.com/scientificreports (accessed: 17.06.18).

7. *Денисов А. А., Колесников Д. Н.* Теория больших систем управления. Л.: Энергоиздат, 1982. 288 с.

8. *Попов Г. А., Попова Е. А.* Методическое пособие по проведению практических занятий по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем». Ч. 2. Астрахань, 2013. 24 с.

9. *Белов С. В., Мельников А. В.* Процедура оценки показателей злоумышленного проникновения в составе автоматизированной системы контроля физической безопасности объекта защиты // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2014. № 2. С. 28–37.

10. *Беллман Р.* Динамическое программирование. М.: Изд-во иностр. лит., 1960. 400 с.

11. *Акулич И. Л.* Задачи динамического программирования // Математическое программирование в примерах и задачах. Гл. 4. М.: Высш. шк., 1986. 288 с.

Статья поступила в редакцию 24.09.2018

ИНФОРМАЦИЯ ОБ АВТОРАХ

Попов Георгий Александрович – Россия, 414056, Астрахань; Астраханский государственный технический университет; д-р техн. наук, профессор; зав. кафедрой информационной безопасности; popov@astu.org.

Попова Екатерина Александровна – Россия, 414056, Астрахань; Астраханский государственный технический университет; старший преподаватель кафедры информационной безопасности; e.popova@astu.org.

Попова Марина Георгиевна – Россия, 414056, Астрахань; Астраханский государственный технический университет; магистрант, специальность «Прикладная информатика в экономике»; popov@astu.org.

G. A. Popov, E. A. Popova, M. G. Popova

NETWORK MODELS OF MALWEAR PROLIFERATION PROCESSES

Abstract. The paper deals with the analysis of possible ways of spreading malware on the basis of weighted graphs, where the graph describes the relationship between different programs, and the weight shows the probability of transition malware from one software system to another. The task is to identify the most likely routes of malicious programs distribution and to find the most likely ways of their penetration into a given software product. The method of dynamic programming is proposed to solve the problem. The procedure of solving the problem has been demonstrated on a particular example. The results of calculations helped to determine the most probable route of penetration and to estimate the probability of successful attack of malicious programs on the required software product. Graph theory methods also allowed to estimate a number of other numerical characteristics related to the process of the malicious programs distribution, which include the minimum number of clock cycles of the system (after the implementation of this characteristic it becomes possible for a malicious program to penetrate the specified software product); the number of clock cycles of the system (when probability of penetration of the malware into a specific file will be greater than the specified value). Besides, the method helps identify cyclical routes of malware distribution, which characterizes repeated attempts of malware to impact on the software product, find the most likely sources of distribution, detect the files, through which penetration into given software product is possible.

Key words: malicious program, software product, graphs, penetration route, dynamic programming method.

REFERENSES

1. Rudnichenko A. K., Koshelek S. O. Ispol'zovanie OLE-ob"ektov v dokumentakh Vicrosoft Word kak sredstvo rasprostraneniia vredonosnykh programm. Metody zashchity ot nikh [Using OLE-objects in documents Microsoft Word as means of distributing malware. Preventive measures against them]. *Molodoi uchenyi*, 2016, no. 29 (135), pp. 36-39.

2. Zaitsev O. *Tekhnologii vredonosnykh programm i ugrozy informatsionnoi bezopasnosti* [Technology of malicious software and threats to information security]. Available at: https:// compress.ru/ Article.aspx?id=17361 (accessed: 17.06.18).

3. Zikratov I. A., Vasilenko R. S. *Poisk vredonosnykh programm na osnove analiza protsessa rasprostraneniia* [Search of malware through5 the analysis of their distribution]. Available at: https://cyberleninka.ru/article/n/poisk-vredonosnyh-programm-na-osnove-analiza-protsessa-rasprostraneniya-publikuetsya-v-poryadke-diskussii (accessed: 17.06.18).

4. Kurilov F. M. Modelirovanie sistem zashchity informatsii. Prilozhenie teorii grafov [Modeling information protection systems. Graph theory application]. *Tekhnicheskie nauki: teoriia i praktika: materialy III Mezhdunarodnoi nauchnoi konferentsii (Chita, aprel' 2016 g.)*. Chita, Molodoi uchenyi Publ., 2016. Pp. 6-9.

5. Shawn A. *List of Types of Malware May 24, 2017*. Available at: https://www.malwarefox.com/malware-types/ (accessed: 17.06.18).

6. Wanping Liu, Shouming Zhong. *Web malware spread modelling and optimal control strategies.* Scientific RepoRts, 10 February 2017. Available at: www.nature.com/scientificreports (accessed: 17.06.18).

7. Denisov A. A., Kolesnikov D. N. *Teoriia bol'shikh sistem upravleniia* [Theory of big management systems]. Leningrad, Energoizdat, 1982. 288 p.

8. Popov G. A., Popova E. A. *Metodicheskoe posobie po provedeniiu prakticheskikh zaniatii po distsipline "Kompleksnoe obespechenie informatsionnoi bezopasnosti avtomatizirovannykh system". Chast' 2* [Methodological instructions on conducting practical classes on discipline "Complex providing information security of automated systems. Part 2"]. Astrakhan', Izd-vo AGTU, 2013. 24 p.

9. Belov S. V., Mel'nikov A. V. Protsedura otsenki pokazatelei zloumyshlennogo proniknoveniia v sostave avtomatizirovannoi sistemy kontrolia fizicheskoi bezopasnosti ob"ekta zashchity [Procedure of evaluating parameters of malicious penetration in terms of automated system of control of physical security of the protective entity]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2014, no. 2, pp. 28-37.

10. Bellman R. *Dinamicheskoe programmirovanie* [Dynamic programming]. Moscow, Izd-vo inostrannoi literatury, 1960. 400 p.

11. Akulich I. L. Zadachi dinamicheskogo programmirovaniia [Problems of dynamic programming]. *Matematicheskoe programmirovanie v primerakh i zadachakh. Chapt. 4*. Moscow, Vysshaia shkola Publ., 1986. 288 p.

The article submitted to the editors 24.09.2018

INFORMATION ABOUT THE AUTHORS

Popov Georgiy Aleksandrovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Doctor of Technical Sciences, Professor; Head of the Department of Information Security; popov@astu.org.

Popova Ekaterina Aleksandrovna – Russia, 414056, Astrakhan; Astrakhan State Technical University; Senior Lecturer of the Department of Information Security; e.popova@astu.org.

Popova Marina Georgievna – Russia, 414056, Astrakhan; Astrakhan State Technical University; Master's Course Student, specialty "Applied Informatics in Economics"; popov@astu.org.