УДК 004.422 **DOI: 10.20998/2411-0558.2016.44.13**

С.Г. СЕМЕНОВ, д-р техн. наук, с.н.с., НТУ "ХПИ", Харьков,
Д.А. ЛИСИЦА, асп., НТУ "ХПИ", Харьков,
А.В. МОВЧАН, асп., НТУ "ХПИ", Харьков

GERT-МОДЕЛЬ НАЧАЛЬНОЙ ГЕНЕРАЦИИ КОДА КИБЕРАТАКИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К РЕСУРСАМ КОМПЬЮТЕРНОЙ СИСТЕМЫ ОДНОРАНГОВОЙ СЕТИ

Разработана математическая GERT-модель начальной генерации кода кибератаки несанкционированного доступа к ресурсам компьютерной системы одноранговой сети, отличающаяся от известных учетом основных этапов генерации в процессе математической формализации GERT-сети. В ходе моделирования получено аналитическое выражение для расчета времени генерации кода кибератаки несанкционированного доступа. Сделаны выводы о дальнейших практических разработках, связанных с полученными в статье результатами. Ил.: 2. Табл.: 1. Библиогр.: 13 назв.

Ключевые слова: GERT-модель, компьютерная система, несанкционированный доступ, моделирование, генерация кода кибератаки.

Постановка проблемы. В соответствии с требованиями системного подхода к защите информации, совокупность взаимосвязанных элементов, функционирование которых направлено на обеспечение безопасности, образует систему защиты информации. Такими элементами являются математические, технические и программные решения, а также человеческие ресурсы.

Сложность самой системы защиты информации определяется не только многоаспектностью ее структурно-функционального построения, но и сложностью внешних факторов, разнообразностью действий злоумышленников и просто пользователей, влияющих на процесс ее функционирования.

В последнее время все больший интерес у злоумышленников вызывают электронные информационные ресурсы. Соответственно наблюдается расширение спектра поведенческих портретов злоумышленников в рамках различного рода кибератак.

Для реализации кибератаки несанкционированного доступа (НСД) злоумышленник моделирует данное событие безопасности, приводящее к ожидаемому результату. Проведенные исследования показали, что в настоящее время существует ряд математических моделей [1 – 7] в этой области. Однако, известные модели [2, 3] кибератак НСД не используют такой компонент, как "действия злоумышленника". Это приводит к тому, что эффективность систем защиты информации [5] от НСД

снижается, и они не всегда могут выявить такой род кибератак. Поэтому разработка математической модели кибератак НСД является актуальной научной задачей.

Анализ литературы [2, 6] показал, что в настоящее время кибератаку НСД можно разбить на несколько функциональных этапов:

– генерации кода кибератаки НСД;

– активного "снифинга";

– активного анализа системы управления ресурсом;

– внедрения в компьютерную систему.

Проведенные исследования показали, что общий алгоритм кибератаки НСД имеет ряд специфических итераций, в значительной степени усложняющих общий процесс его математической формализации. Поэтому представляется целесообразным разбиение этого процесса на ряд подпроцессов. При этом для математического моделирования НСД наиболее гибкими и полезными представляются сетевые стохастические модели. Частным случаем стохастической модели является GERT-сеть (GERT: *Graphical Evaluation and Review Technique* – метод графического отображения).

Во многом это связано с доступностью математического аппарата нахождения непрерывной плотности распределения вероятностей времени прохождения GERT-сети при условии, что множество распределений, которыми могут характеризоваться отдельные дуги модели, включает в себя известные распределения: дискретное, биномиальное, пуассоновское, геометрическое, отрицательное биномиальное, равномерное, экспоненциальное, гамма и нормальное.

Кроме этого, существует возможность нахождения и использования непрерывных распределений произвольного вида. Предлагаемые методы основаны на переходе от эквивалентной передаточной функции $W_E(s)$ GERT-сети к ее характеристической функции $X_E(\zeta)$ и использовании формулы обращения [8].

Из [8] известно, что плотность распределения вероятностей времени прохождения GERT-сети определяется следующим выражением:

$$\varphi(x) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{-i\zeta x} X_E(\zeta) d\zeta \cdot \qquad (1)$$

Характеристическая функция $X_E(\zeta)$ находится на основе топологического уравнения Мейсона [9] путем замены в эквивалентной производящей функции моментов $M_E(s)$ переменной s на $i\zeta$, где ζ – действительная переменная. Если $X(\zeta)$, $M(\zeta)$ соответственно –

характеристическая функция и производящая функция моментов GERT-сети, то справедливо соотношение: $M(i\zeta) = X(\zeta)$.

Для обеспечения условий интегрирования введем в подынтегральное выражение множитель $\exp(-0{,}5\zeta^2)$ [8]. Это равносильно добавлению в GERT-сеть последовательной ветви, описываемой нормально распределенной случайной величиной ζ_2 с нулевым математическим ожиданием и дисперсией, равной единице. Фиктивную ветвь можно включить сразу после источника *s* сети. Если случайная величина ζ_1 есть время прохождения GERT-сети, то плотность распределения суммы $\zeta_1 + \zeta_2$ определяется выражением

$$\tilde{\varphi}(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-i\zeta x}\,\overline{X}_E(\zeta)\,d\zeta,$$

где $\overline{X}_E(\zeta) = X_E(\zeta)\exp(-0{,}5\zeta^2)$.

После нахождения плотности $\tilde{\varphi}(x)$ должна быть найдена искомая плотность распределения $\varphi(x)$. Это достигается использованием численного метода трансформации закона распределения на основе решения системы линейных уравнений [10, 11].

Из топологического уравнения следует:

$$W_E(v,t) = \frac{\sum\limits_{\gamma_1=1}^{\Gamma_i}\prod\limits_{\delta_1=1}^{\Delta_i} \breve{W}^1_{\gamma_1\delta_1} + \ldots - (-1)^m \sum\limits_{\gamma_m=1}^{\Gamma_m}\prod\limits_{\delta_m=1}^{\Delta_m} \breve{W}^m_{\gamma_m 8_m}}{1 - \sum\limits_{a_1=1}^{A_i}\prod\limits_{\beta_1=1}^{B_i} \overline{W}^1_{a_1\beta_1} + \ldots + (-1)^l \sum\limits_{a_1=1}^{A_i}\prod\limits_{\beta_1=1}^{B_i} \overline{W}^1_{a_1\beta_1}}, \qquad (2)$$

где Γ_i – количество сетей *i*-го порядка от истока *v* к стоку *t* сети; Δ_i – число дуг *i*-го порядка на пути от истока *v* к стоку *t*; A_i – количество сетей *i*-го порядка приводящих к истоку *v* в обратном направлении; B_i – число дуг *i*-го порядка на пути, приводящего к истоку *v*;

$\prod\limits_{\delta_1=1}^{\Delta_1} \breve{W}^1_{\gamma_1\delta_1}$ – произведение *W*-функций дуг r_i-ой петли *i*-го порядка, включающей в себя сток *t*, $1 \le i \le m$;

$\prod\limits_{\beta_j=1}^{B_j} \breve{W}^j_{a_j\beta_j}$ – произведение *W*-функций дуг a_j-ой петли *j*-го порядка, не включающей в себя сток *t*, $1 \le j \le l$.

Переходя к характеристическим функциям, получаем

$$X_E(\zeta)=\frac{\dfrac{1}{P_E}\left(\sum\limits_{\gamma_i=1}^{\Gamma_i}\prod\limits_{\delta_i=1}^{\Delta_i}\breve{p}_{\gamma_i\delta_i}\breve{X}^{i}_{\gamma_i\delta_i}+\ldots+(-1)^m\sum\limits_{\gamma_m=1}^{\Gamma_m}\prod\limits_{\delta_m=1}^{\Delta_m}\breve{p}_{\gamma_m\delta_m}\breve{X}^{m}_{\gamma_m\delta_m}\right)}{1-\sum\limits_{a_i=1}^{A_i}\prod\limits_{\beta_i=1}^{B_i}\overline{p}_{\gamma_i\delta_i}\overline{X}^{i}_{a_i\beta_i}+\ldots+(-1)^l\sum\limits_{a_i=1}^{A_i}\prod\limits_{\beta_i=1}^{B_i}\overline{p}_{\gamma_m\delta_m}\overline{X}^{i}_{a_i\beta_i}}. \quad (3)$$

Здесь $\prod\limits_{\delta_i=1}^{\Delta_i}\breve{p}_{\gamma_i\delta i}\breve{X}(\zeta)^1_{\gamma_i\delta_i}$ и $\prod\limits_{\beta_j=1}^{B_j}\overline{p}_{\gamma_j\delta_j}\overline{X}(\zeta)^j_{\gamma_j\delta_j}$ находятся из произведений

$$\prod_{\delta_i=1}^{\Delta_i}\breve{W}(s)^i_{\gamma_i\delta_i}=\prod_{\delta_1=1}^{\Delta_1}\breve{p}_{\gamma_i\delta_i}\breve{M}(s)^i_{\gamma i\delta_i},\ \overline{W}(s)^j_{a_jb_j}=\prod_{\beta_j=1}^{B_j}\overline{p}_{\gamma_j\delta_j}\overline{M}(s)^j_{\gamma_j\delta_j}$$

заменой $s\to i\zeta$.

В ряде практически важных случаев распределения необходимо получать в виде математических выражений. К таким задачам можно отнести и задачу исследования алгоритмов кибератаки НСД. При этом решение задачи нахождения плотности распределения времени прохождения сформированной на основе разработанных алгоритмов GERT-сети необходимо начать с допущения, что непрерывной плотности распределения вероятностей времени прохождения GERT-сети $\varphi(x)$ определяется выражением (1).

Из литературы [8] известно, что в уравнении (1) можно выполнить замену переменных: $z = -i\zeta$. Функцию, получающуюся в результате замены переменных, обозначим через $\Phi_E(z)$. Функция $\Phi_E(z)$ может быть представлена через комбинации функций $\Phi(z)$ петель первого и более высоких порядков в зависимости от того, принадлежит ли данной петле или нет источник и сток GERT-сети:

$$\Phi_E(z)=\frac{\sum\limits_{\gamma_i=1}^{\Gamma_i}\prod\limits_{\delta_i=1}^{\Delta_i}\breve{\Phi}^{i}_{\gamma_i\delta_i}(z)+\ldots+(-1)^{m+1}\sum\limits_{\gamma_m=1}^{\Gamma_m}\prod\limits_{\delta_m=1}^{\Delta_m}\breve{\Phi}^{m}_{\gamma_m\delta_m}(z)}{1-\sum\limits_{a_i=1}^{A_i}\prod\limits_{\beta_i=1}^{B_i}\overline{\Phi}^{i}_{\gamma_i\delta_i}(z)+\ldots+(-1)^l\sum\limits_{a_i=1}^{A_i}\prod\limits_{\beta_i=1}^{B_i}\Phi^{l}_{\gamma_l\delta_l}}, \quad (4)$$

где $\prod\limits_{\delta_i=1}^{\Delta i}\breve{\Phi}^{i}_{\gamma_i\delta_i}(z)$ – произведение $\Phi(z)$-функций ветвей петли i-го порядка, включающей в себя сток t, $1\le i\le m$, $\gamma_1\le\gamma_i\le\gamma_m$;

$\prod_{\delta_j=1}^{Bj} \overline{\Phi}^{\,j}_{a_j\beta_j}$ – произведение Φ(*z*)-функций ветвей петли *j*-го порядка, не включающей в себя сток *t*, $1 \le j \le l$,

$a_1 \le a_j \le a_l$; $\Gamma_1, ..., \Gamma_m$ – число петель порядков 1, ... , *m*, включающих в себя сток сети; A_1 , … , A_l – число петель порядков 1, ..., *l*, не включающих в себя сток сети.

Если функция $\Phi_E(z)$ в полуплоскости $\mathrm{Re}\, z < 0$ удовлетворяет условиям леммы Жордана, то интеграл, взятый вдоль контура Бромвича, равен сумме вычетов функции $\Phi_E(z)$ относительно всех ее особенностей [12, 13]:

$$\varphi(x) = \frac{1}{2\pi i} \int_{-i\infty}^{i\infty} e^{zx}\Phi_E(z)dz = \sum_{k=1}^{n} \mathrm{Res}_{z=z_k}\left[e^{zx}\Phi_E(z)\right].$$

Для выполнения условия леммы Жордана необходимо, чтобы в левой полуплоскости функция $\Phi_E(z)$ была аналитической за исключением конечного числа полюсов, и равномерно относительно *arg z* стремилась к нулю при $|z| \to \infty$.

Функция $\Phi_i(z) = \lambda/(\lambda + z)$ экспоненциального распределения равномерно сходится к нулю относительно arg *z* при $|z| \to \infty$. Имеется простой полюс в точке $z = -\lambda$. Функция $\Phi_i(z) = \lambda^a/(\lambda + z)^a$ распределения Эрланга равномерно сходится к нулю относительно arg *z* при $|z| \to \infty$. Имеется полюс кратности *a* в точке $z = -\lambda$.

При преобразовании структуры GERT-сети к ациклическому виду последняя представляется в виде эквивалентной совокупности последовательных и параллельных ветвей. Если ациклическая GERT-сеть имеет *M* параллельных ветвей с вероятностями выбора q_1, и каждая из них состоит из *N* последовательных ветвей с вероятностями выбора p_{ij}, то при использовании в качестве характеристик ветвей распределений Эрланга имеем $\Phi_E(z) = \sum_{i=1}^{M} q_1 \prod_{j=1}^{N_i} p_{ij}\left[\lambda_{ij}^{k_{ij}}/(\lambda_{ij} + z)^{k_{ij}}\right]$.

Функция $\Phi_E(z)$ является аналитической и все ее особые точки лежат в левой полуплоскости. Таким образом, задача нахождения плотности распределения времени прохождения такой GERT-сети может быть решена путем нахождения предела последовательности распределений.

Целью данной статьи является разработка GERT-модели начальной генерации кода кибератаки несанкционированного доступа к ресурсам компьютерной системы одноранговой сети.

Основная часть. При моделировании кибератаки НСД возникает большое число задач, которые могут быть решены с использованием моделей такого рода. Они могут использоваться как независимо друг от друга, так и в комбинированных системах. В распоряжение пользователя могут быть предоставлены несколько новых разновидностей моделей GERT (однородные сети большой размерности, неоднородные сети, сети со старением заявок, случайные GERT-сети и т.д.).

Проведен анализ и разработана GERT-модель начального этапа рассматриваемого злоумышленного воздействия – начальной генерации кода кибератаки НСД к ресурсам компьютерной системы одноранговой сети.

1. Разработка GERT-сети этапа начальной генерации кода.

Структурная схема алгоритма этого этапа представлена на рис. 1. Структурная схема показывает пошаговый алгоритм действий, которые должен выполнить злоумышленник для НСД к ресурсам компьютерной системы.

Данный алгоритм можно представить в виде стохастической GERT-сети (рис. 2), в которой переход системы из состояния в состояние связывается с выполнением операции алгоритма (рис. 1), описываемой случайной величиной с известным законом распределения.

На рис. 2 и табл. 1 переход (1, 2) характеризует операции выбора оборудования – жертвы для взлома, при этом заранее известно, что атака производится в пределах одноранговой сети (P_1 – вероятность перехода из 1 в 2, λ_1 – соответствующая интенсивность перехода).

Переходы (2, 3) (2, 4) описывают процесс выбора метода атаки с учетом определения операционной системы на узле – жертве, *Windows* или *Linux* соответственно (P_2 – вероятность перехода из 2 в 3, λ_2 – соответствующая интенсивность; $1 – P_2 – P_3$ – вероятность перехода из 2 в 4, λ_4 – соответствующая интенсивность перехода).

Переходы (2, 1) и (3, 1) представляю ситуации, когда злоумышленник в силу ряда причин не смог осуществить выбор метода атаки в пределах заданного времени или характеристики найденного злоумышленного программного обеспечения (ПО) не соответствуют условиям и целям кибератаки НСД. Так как данная ситуация может рассматриваться как идентичная для состояний 2 и 3, то вероятности перехода из 2 в 1 и из 3 в 1 одинаковы и равны P_3 при соответствующей интенсивности перехода λ_3.

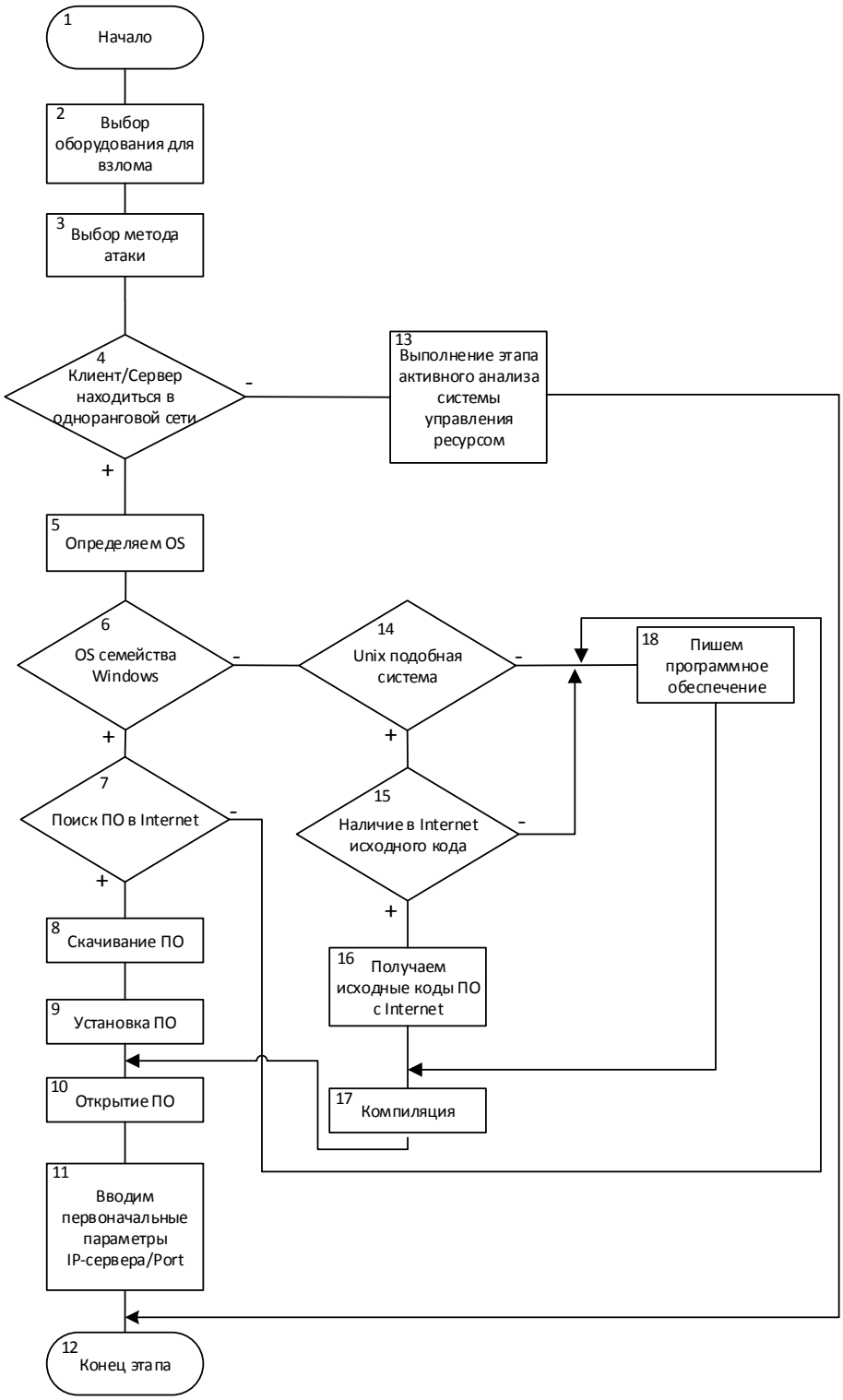

Рис. 1. Структурная схема алгоритма этапа генерации кода кибератаки НСД

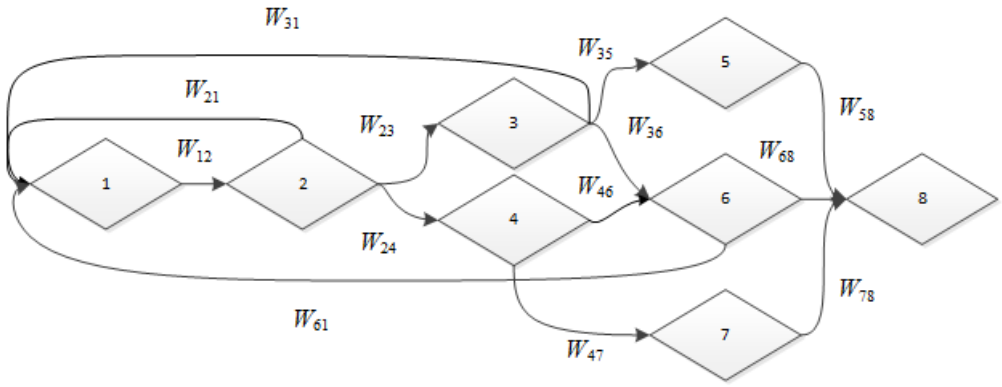

Рис. 2. GERT-сеть алгоритма генерации кода кибератаки НСД

Переход (3, 5) характеризует процесс поиска программного обеспечения (ПО) в глобальной сети Интернет, скачивания и установки функционирующего под *OS Windows* (P_4 – вероятность перехода из 3 в 5, λ_2 – соответствующая интенсивность).

Соответственно переход (4, 7) описывает процесс получения исходного кода в глобальной сети Интернет и компиляции ПО под *OS Linux* ($1 - P_5$ – вероятность перехода из 4 в 7, λ_2 – соответствующая интенсивность перехода).

Переходы (3, 6) и (4, 6) представляют процедуры кодирования и отладки ПО под *OS Windows* и *Linux* соответственно, в случае отсутствия такового в глобальной сети Интернет ($1 - P_3 - P_4$ – вероятность перехода из 3 в 6, λ_4 – соответствующая интенсивность; P_5 – вероятность перехода из 4 в 6, λ_4 – соответствующая интенсивность перехода).

Переход (6, 1) характеризует ситуацию, когда злоумышленник не смог выполнить операции кодирования и отладки злоумышленного ПО в заданное для атаки время ($1 - P_6$ – вероятность перехода из 6 в 1, λ_6 – соответствующая интенсивность перехода).

Переходы (5, 8), (6, 8) и (7, 8) описывают процедуры открытия злоумышленного ПО и ввода первоначальных параметров *IP*-сервера узла–жертвы (P_4 – вероятность перехода из 5 в 8, λ_2 – соответствующая интенсивность; P_6 – вероятность перехода из 6 в 8, λ_5 – соответствующая интенсивность; $1 - P_5$ – вероятность перехода из 7 в 8, λ_2 – соответствующая интенсивность перехода).

Анализ работ [2, 3, 6], а также проведенные исследования процедур компиляции, отладки, скачивания, установки и др., входящих в процесс первоначальной генерации кода кибератаки НСД, позволили сформировать характеристики рассмотренных в GERT-модели ветвей и параметров распределения и представить их в табл. 1.

Таблица 1

Характеристики ветвей модели

№ п/п	Ветвь	*W*–функция	Вероятность перехода	Производящая функция моментов
1.	(1, 2)	W_{12}	P_1	$\lambda_1/(\lambda_1 - s)$
2.	(2, 3)	W_{23}	P_2	$\lambda_2/(\lambda_2 - s)$
3.	(2, 1)	W_{21}	P_3	$\lambda_3/(\lambda_3 - s)$
4.	(2, 4)	W_{24}	$1 - P_2 - P_3$	$\lambda_4/(\lambda_4 - s)$
5.	(3, 5)	W_{35}	P_4	$\lambda_2/(\lambda_2 - s)$
6.	(3, 1)	W_{31}	P_3	$\lambda_3/(\lambda_3 - s)$
7.	(3, 6)	W_{36}	$1 - P_3 - P_4$	$\lambda_4/(\lambda_4 - s)$
8.	(4, 6)	W_{46}	P_5	$\lambda_4/(\lambda_4 - s)$
9.	(4, 7)	W_{47}	$1 - P_5$	$\lambda_2/(\lambda_2 - s)$
10.	(5, 8)	W_{58}	P_4	$\lambda_2/(\lambda_2 - s)$
11.	(6, 8)	W_{68}	P_6	$\lambda_5/(\lambda_5 - s)$
12.	(6, 1)	W_{61}	$1 - P_6$	$\lambda_6/(\lambda_6 - s)$
13.	(7, 8)	W_{78}	$1 - P_5$	$\lambda_2/(\lambda_2 - s)$

В соответствии с характеристиками ветвей GERT-сети эквивалентную передаточную *W*-функцию времени начальной генерации кода кибератаки НСД к ресурсам компьютерной системы одноранговой сети можно представить, как [10, 11]:

$$W_E(s) = \frac{\left(W_{12}W_{23}W_{35}W_{58} + W_{12}W_{23}W_{36}W_{68} + W_{12}W_{24}W_{46}W_{68} + W_{12}W_{24}W_{47}W_{78}\right)}{1 - W_{12}W_{21} - W_{12}W_{23}W_{31} - W_{12}W_{23}W_{36}W_{61} - W_{12}W_{24}W_{46}W_{61}}.$$

Учитывая составляющие GERT-сеть алгоритма генерации кода кибератаки НСД и используя соответствующие данные табл. 1 получим основную формулу для расчета *W*-функции времени начальной генерации кода кибератаки НСД к ресурсам компьютерной системы одноранговой сети [10, 11]:

$$W_E(s)=\frac{\left(\begin{array}{l} p_1(\lambda_1/\lambda_1-s)\left(\begin{array}{l} p_2p_4^2\lambda_2^3(\lambda_1-s)(\lambda_4-s)^2(\lambda_5-s)+\\ +p_1p_2p_6q_2\lambda_1\lambda_2\lambda_4\lambda_5(\lambda_2-s)^2(\lambda_4-s)+\\ +p_1p_5p_6q_1\lambda_1\lambda_4^2\lambda_5(\lambda_2-s)^3+\\ +p_1q_1q_3^2\lambda_1\lambda_2^2\lambda_4(\lambda_2-s)(\lambda_5-s)\end{array}\right)\end{array}\right)}{\left(\begin{array}{l}(\lambda_1-s\lambda)(\lambda_2-s)(\lambda_3-s)(\lambda_4-s)^2(\lambda_6-s)-\\ -p_1p_2\lambda_1\lambda_3(\lambda_2-s)(\lambda_4-s)^2(\lambda_6-s)-\\ -p_1p_2p_3\lambda_1\lambda_2\lambda_3(\lambda_4-s)^2(\lambda_6-s)-\\ -p_1p_2q_1q_2p_3\lambda_1\lambda_2\lambda_4\lambda_6(\lambda_4-s)(\lambda_3-s)-\\ -p_1p_5q_1q_4p_3\lambda_1\lambda_4^2\lambda_6(\lambda_2-s)(\lambda_3-s)\end{array}\right)}{(\lambda_1-s)(\lambda_2-s)(\lambda_3-s)(\lambda_4-s)^2(\lambda_6-s)}, \quad (5)$$

где $q_1=1-p_2-p_3$; $q_2=1-p_3-p_4$; $q_3=1-p_5$; $q_4=1-p_6$.

Проведенные исследования показали, что в сложных GERT-сетях с возможными циклами отсутствуют простые методы нахождения особых точек функции $\Phi_E(z)$ (выражение (4)) путем замены действительных переменных $(z=-i\varsigma)$, где ς – действительная переменная [10 – 12]. Связано это с тем, что для нахождения особых точек необходимо решать нелинейные уравнения, и чем сложнее структура GERT-сети, тем сложнее и исходное уравнение [2, 7, 8]. Поэтому в ходе моделирования, выполняя комплексное преобразование [10 – 12] и используя выражения (4) и (5), получим:

$$\Phi_E(z)=\frac{-yz^6+bz^5-tz^4+uz^3-kz^2+wz-h}{\left(-z^6+jz^5-dz^4+gz^3-vz^2+rz-c\right)(\lambda_1+z)(\lambda_2+z)(\lambda_5+z)}, \quad (6)$$

где $y=p_1p_2p_4\lambda_1\lambda_2^3$;

$$b=-p_1\lambda_1\left(\begin{array}{l}(p_2(p_4\lambda_2^3(1+\lambda_1+\lambda_5+2\lambda_4)+p_1p_6q_2\lambda_1\lambda_2\lambda_4\lambda_5))+\\ +p_1p_5p_6q_1\lambda_1\lambda_4^2\lambda_5\end{array}\right);$$

$$t = p_1\lambda_1\left(\begin{array}{l} p_2\left(\begin{array}{l} p_4\lambda_2^3 + p_4\lambda_2^3(\lambda_1+\lambda_5+2\lambda_4)(\lambda_6+\lambda_3)+ \\ + p_1p_6q_2\lambda_1\lambda_2\lambda_4\lambda_5 + \\ + p_4\lambda_2^3\left(\begin{array}{l} \lambda_1\lambda_5 + 2\lambda_4\lambda_5 + 2\lambda_1\lambda_4 + \lambda_4^2 + \\ + p_1p_6q_2\lambda_1\lambda_2\lambda_4\lambda_5(\lambda_4+2\lambda_2) \end{array}\right) \end{array}\right) + \\ + 3p_1p_5p_6q_1\lambda_1\lambda_2\lambda_4^2\lambda_5 \end{array}\right);$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$c = \left(\begin{array}{l} \lambda_1\lambda_2\lambda_3\lambda_4^2\lambda_6 + p_1p_3\lambda_1\lambda_2\lambda_3\lambda_4^2\lambda_6 + p_1p_2p_3\lambda_1\lambda_2\lambda_4^3\lambda_6 + \\ + p_1p_2q_1q_2\lambda_1\lambda_2\lambda_3\lambda_4^2\lambda_6 + p_1p_5q_1q_4\lambda_1\lambda_2 + \lambda_3\lambda_4^2\lambda_6 \end{array}\right).$$

Тогда плотность распределения вероятностей времени генерации кода кибератаки НСД:

$$\varphi(x) = \frac{1}{2\pi i}\int\limits_{-i\infty}^{i\infty} e^{zx}\frac{-yz^6 + bz^5 - tz^4 + uz^3 - kz^2 + wz - h}{\left(\begin{array}{l}(-z^6 + jz^5 - dz^4 + gz^3 - vz^2 + rz - c)\times \\ \times(\lambda_1+z)(\lambda_2+z)(\lambda_5+z)\end{array}\right)}, \qquad (7)$$

где интегрирование выполняется по контуру Бромвича [7].

Функция $\Phi(z)$ кроме простых полюсов, определяемых корнями уравнения $-z^6 + jz^5 - dz^4 + gz^3 - vz^2 + rz - c = 0$, может иметь и полюсы второго – четвертого порядка. Это возможно в тех случаях, когда значения λ_1, λ_2, λ_5 или совпадают между собой, или равны значениям корней z_3, z_4, z_5, z_6 В этих случаях плотность распределения времени тестирования программного обеспечения $\varphi(x)$ находится по формуле нахождения вычетов γ_{-1} от полюсов z_n порядка m

$$\gamma_{-1} = \frac{1}{(m-1)!}\lim_{z\to z_n}\frac{d^{m-1}[(z-z_n)^m e^{zx}\Phi(z)]}{dz^{m-1}}.$$

Выражение (6), в соответствии с работами [1, 7, 8], можно представить как дробнорациональную функцию относительно z со степенью знаменателя большей, чем степень числителя, поэтому для него выполняются условия леммы Жордана. Функция $\Phi(z)$ имеет полюсы в точках $z_1 = -\lambda_1$, $z_2 = -\lambda_2$, $z_3 = -\lambda_5$. Многочлен

$-z^6 + jz^5 - dz^4 + gz^3 - vz^2 + rz - c$ порождает еще шесть полюсов. Решение уравнения

$$-z^6 + jz^5 - dz^4 + gz^3 - vz^2 + rz - c = 0 \qquad (8)$$

может быть найдено любым численным методом. Тогда получим еще шесть особых точек z_4, z_5, z_6, z_7, z_8.

Выводы. Таким образом, предложена математическая GERT-модель процесса генерации кода кибератаки НСД. Предложенная математическая модель отличается от известных учетом основных этапов генерации в процессе математической формализации GERT-сети. Модель может быть использована для исследования основных этапов генерации кода кибератаки НСД с целью выработки практических рекомендаций противодействия процессу НСД к ресурсам компьютерной системы одноранговой сети, а также при разработке новых методов, алгоритмов и способов управления компьютерными системами.

Применение GERT-сетей в ходе математического моделирования даст возможность использовать результаты, полученные в аналитическом виде (функции, плотности распределения) для проведения сравнительного анализа и исследований, более сложных комплексных этапов кибератаки НСД.

Список литературы: 1. *Гмурман В.Е.* Теория вероятностей и математическая статистика / *В.Е. Гмурман*. – М.: Высшая школа, 2003. – С. 479. **2.** *Семенов С.Г.* Методика математического моделирования защищенной ИТС на основе многослойной GERT-сети / *С.Г. Семенов* // Вестник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков, 2012. – Вып. 62 (968). – С. 173–181. **3.** *Семенов С.Г.* Моделирование защищенного канала связи с использованием экспоненциальной GERT-сети / *С.Г. Семенов, А.А. Можаев* // Информатика, математическое моделирование, экономика: Сборник научных статей. – Смоленск.: Смоленский филиал АНО ВПО ЦС РФ "Российский университет кооперации". – 2012. – Том. 1. – С. 152-160. **4.** *Тихомиров В.М.* Десять доказательств основной теоремы алгебры / *В.М. Тихомиров, В.В. Успенский* // Математическое просвещение. – МЦНМО, 1997. – № 1. – С. 50-70. **5.** *Шорошев В.* Перспективный метод защиты информационных ресурсов сетей Интранет / *В. Шорошев* // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К.: НТУ "КПІ". – 2003. – Вип. 7. – С. 62–76. **6.** *Semenov S.G.* Protection Data in computerized Governors systems / *S.G. Semenov, V.V. Davydov, C.Yu. Gavrylenko* // LAP Lambert Academic Publishing GmbH & Co. KG. – Germany, 2014. – 236 p. **7.** *Cohen F.* Computational aspects of computer viruses Computers & Security / *F. Cohen.* – 1989. – Vol. 8. – P. 325-344. **8.** *Феллер В.* Введение в теорию вероятностей и ее приложения / *В. Феллер.* – М.: Мир. – 1984. – 738 с. **9.** *Филлипс Д.* Методы анализа сетей / *Д. Филлипс, А. Гарсиа-Диас.* – М.: Мир. – 1984. – 496 с. **10.** *Бахвалов Н.С.* Численные методы / *Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков.* – М.: Наука. – 1987. – 627 с.. **11.** *Крайников А.В.* Вероятностные методы в вычислительной технике / *А.В. Крайников, Б.А. Курдиков,*

А.Н. Лебедев и др. – М.: Высш. шк. – 1986. – 312 с. **12.** *Лаврентьев М. А.* Методы теории функций комплексного переменного / *М.А. Лаврентьев, Б. В. Шабат*. – М.: Наука. – 1987. – С. 688. **13.** *Привалов И.И.* Введение в теорию функций комплексного переменного / *И.И. Привалов*. – М.: Наука. – 1984. – 432 с.

References:

1. Gmurman, V.E. (2003), *Probability theory and mathematical statistics*, Moscow Higher School, 479 p.

2. Semenov, S.G. (2012), "Methods of mathematical modeling based on ITS protected multilayer GERT-networks", *Journal of the National Technical University "Kharkiv Polytechnic Institute". Collection of scientific papers. Special Issue: Information and Modeling*, 173-181 p.

3. Semenov, S.G. and Mozhaev, A.A. (2012), "Simulation of a secure communication channel with exponential GERT-network", *Information technology, mathematical modeling, economics: Collected articles*. – Smolensk Smolensk branch.: ANO VPO RF CC "Russian University of Cooperation", Vol. 1, pp. 152-160

4. Tikhomirov, V.M. (1997), "Ten proof of the fundamental theorem of algebra", *Mathematical education*, MTsNMO, No 1, 50-70 p.

5. Shoroshim, V. (2003), "Promising methods of protection of information resources networking", *Intranet, legal, regulatory she metrological support of the Defense Information Systems in Ukraine*, Kiev NTU "KPI", No 7, 62-76 pp.

6. Semenov, S.G., Davydov, V.V. and Gavrylenko, C.Yu. (2014), *Protection Data in computerized Governors systems*. LAP Lambert Academic Publishing GmbH & Co. KG, Saarbrücken, Germany, 236 p.

7. Cohen, F. (1989), "Computational aspects of computer viruses", *Computers & Security*, Vol. 8, No 4, 325 – 344 pp.

8. Feller, W. (1984), *An Introduction to Probability Theory and its Applications*, Moscow, Mir, 738 p.

9. Phillips, D., Garcia-Diaz, A. (1984), *Network analysis methods*, Moscow, Mir, 496 p.

10. Bahvalov, N.S., Zhidkov, N.P. and Kobelkov, G.M. (1987), *Numerical methods*, Moscow, Nauka, 627 p.

11. Krainik, A.V., Kurdikov, B.A. and Lebedev, A. (1986), *Probabilistic Methods in Computer Science*, Moscow, Higher School, 312 p.

12. Lavrent'ev, M.A. and Shabat, B.V. (1987), *Methods of theory of functions of complex variables*, Moscow, Nauka, 688 p.

13. Privalov, I.I. (1984), *Introduction to the theory of functions of a complex variable*, Moscow, Nauka, 432 p.

Статью представил д-р техн. наук, профессор НТУ "ХПИ" Можаев А.А.

Поступила (received) 05.06.2016

Semenov Sergey, Dr.Sci.Tech, Senior Researcher
National Technical University "Kharkiv Polytechnic Institute"
Str. Frunze, 21, Kharkov, Ukraine, 61002
Tel: (050) 300-76-47, e-mail: s_semenov@ukr.net
ORCID ID: 0000-0003-4472-9234

Lysytsia Dmytro, postgraduate
National Technical University "Kharkiv Polytechnic Institute"
Str. Frunze, 21, Kharkov, Ukraine, 61002
Tel: (066) 584-20-09, e-mail: L.Dimon.O@mail.ru
ORCID ID: 0000-0003-1778-4676

Movchan Aleksandr, postgraduate
National Technical University "Kharkiv Polytechnic Institute"
Str. Frunze, 21, Kharkov, Ukraine, 61002
Tel: (066) 584-20-09, e-mail: L.Dimon.O@mail.ru

УДК 004.422

GERT-модель початкової генерації коду кібератаки несанкціонованого доступу до ресурсів комп'ютерної системи одноранговой мережі / Семенов С.Г., Лисиця Д.О., Мовчан А.В. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2016. – № 44 (1216). – С. 147 – 161.

Розроблено математичну GERT-модель початкової генерації коду кібератаки несанкціонованого доступу до ресурсів комп'ютерної системи одноранговой мережі, що відрізняється від відомих урахуванням основних етапів генерації в процесі математичної формалізації GERT-мережі. В ході моделювання отримано аналітичний вираз для розрахунку часу генерації коду кібератаки несанкціонованого доступу. Іл .: 2. Табл.: 1. Бібліогр .: 13 назв.

Ключові слова: GERT-модель, комп'ютерна система, несанкціонований доступ, моделювання, генерація коду кібератаки.

УДК 004.422

GERT–модель начальной генерации кода кибератаки несанкционированного доступа к ресурсам компьютерной системы одноранговой сети / Семенов С.Г., Лисица Д.А., Мовчан А.В. // Вестник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2016. – № 44 (1216). – С. 147 – 161.

Разработана математическая GERT-модель начальной генерации кода кибератаки несанкционированного доступа к ресурсам компьютерной системы одноранговой сети, отличающаяся от известных учетом основных этапов генерации в процессе математической формализации GERT-сети. В ходе моделирования получено аналитическое выражение для расчета времени генерации кода кибератаки несанкционированного доступа. Сделаны выводы о дальнейших практических разработках, связанных с полученными в статье результатами. Ил.: 2. Табл.: 1. Библиогр.: 13 назв.

Ключевые слова: GERT-модель, компьютерная система, несанкционированный доступ, моделирование, генерация кода кибератаки.

UDC 004.422

GERT-model of the initial code generation cyber-attack unauthorized access to computer system resources Peer Network / Semenov S.G., Lysytsia D.O., Movchan A.V. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2016. – № 44 (1216) – P. 147 – 161

A mathematical model of the initial GERT-model generation cyber-attack unauthorized access to a computer system-peer network resources, characterized by the famous view of the main stages in the process of generating a mathematical formalization of GERT-network. During the simulation, an analytical expression for the calculation of the time code generation cyber-attacks unauthorized access. Figs.: 2. Tabl.: 1. Refs.: 13 titles.

Keywords: GERT-model, computer system, unauthorized access, simulation, code generation cyber-attacks.