ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНЫХ ПАРАМЕТРОВ КОНФИГУРИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ СЕТЕВОЙ РАЗВЕДКИ

Горбачев А.А.[1], Соколовский С.П.[2], Каплин М.А. [3],

Цель исследования: *повышение защищенности информационных систем от сетевой разведки.*

Используемые методы: *для достижения цели исследования в работе использованы методы математической статистики и исследования случайных процессов.*

Результат исследования: *решена задача определения оптимальной частоты конфигурирования структурно-функциональных характеристик информационной системы на каждом из этапов сетевой разведки с учетом выполнения требований по минимальному использованию ресурсных возможностей информационной системы и обеспечению заданного значения вероятности вскрытия ее характеристик. Процесс ведения сетевой разведки и противодействия ей формализован в виде марковского случайного процесса с дискретными состояниями и непрерывным временем. Исходя из соображений обеспечения устойчивости информационного обмена между узлами информационной системы и возможностей средств сетевой разведки, определены минимальные значения интервалов времени конфигурирования структурно-функциональных характеристик. Полученные значения оптимальной и предельно допустимой частоты конфигурирования позволяют оценивать время, необходимое для идентификации информационной системы и начала эксплуатации ее уязвимостей, при заданных интенсивностях сетевого сканирования средствами разведки. Полученные результаты позволяют обеспечивать заданный уровень защищенности информационной системы и устойчивость ее информационного обмена за счет оптимальной частоты конфигурирования ее структурно-функциональных характеристик.*

Научная новизна: *решение задачи скалярной оптимизации частоты конфигурирования структурно-функциональных характеристик информационной системы в условиях сетевой разведки с использованием математического аппарата полумарковских случайных процессов.*

Ключевые слова: *сетевое сканирование, случайный процесс, компьютерная атака, устойчивость информационного обмена, вероятность вскрытия, средство разведки.*

DOI:10.21681/2311-3456-2022-4-80-90

Введение

Основным этапом любой из компьютерных атак (КА) является этап сетевой разведки (СР), открывающий злоумышленнику широкие возможности по исследованию состава, структуры и алгоритмов функционирования информационных систем (ИС), что обусловлено статичностью их структурно-функциональных характеристик (СФХ). Однако появление технологии сетевой защиты *Moving Target Defense* (*MTD*), реализующей замену статических параметров ИС динамическими, позволяет оказывать злоумышленнику достаточно эффективные меры противодействия, направленные на снижение актуальности добытой средствами СР информации и вынуждающими его принимать неверные решения в условиях неопределенности [1-7]. В качестве одного из направлений *MTD* выделяют технику динамически изменяемой сети (*Dynamic network*), направленную на конфигурирование сетевых параметров, таких как используемые протоколы (включая протоколы маршрутизации), *IP*-адреса и сетевые порты взаимодействия, *MAC*-адреса, алгоритмы шиф-

1 Горбачев Александр Александрович, адъюнкт Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: infosec23.00@ mail.ru.

2 Соколовский Сергей Петрович, кандидат технических наук, доцент Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: mtd.krd@mail.ru.

3 Каплин Максим Андреевич, преподаватель Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: popi901@yandex.ru.

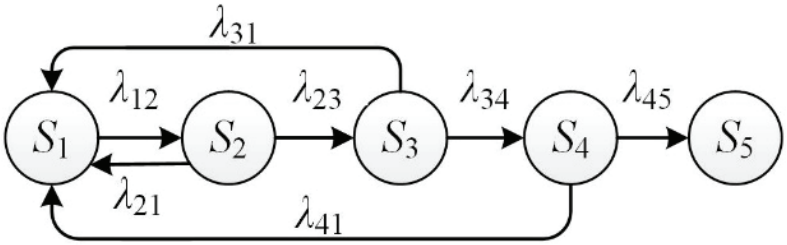

Рис. 1. Граф состояний моделируемой системы

рования, используемые для идентификации узлов источника и назначения, а также маршруты передачи трафика (информационные направления) [8-10].

В настоящее время разработан ряд научно-технических предложений по конфигурированию структурно-функциональных характеристик (СФХ) ИС [11, 12]. Однако, в этих предложениях, а также в научных работах по исследованию функционирования ИС в условиях СР в различных ситуациях а также [13-15], задача по определению оптимальных параметров конфигурирования СФХ ИС, а именно, частоты их конфигурирования, обеспечивающей минимизацию ресурсных затрат при заданном уровне защищенности ИС, не ставилась и не решалась. Вследствие чего настоящая статья будет посвящена решению данной задачи.

Качественная постановка задачи

Функционирование ИС с учетом конфигурирования ее СФХ на рассматриваемом уровне детализации связано со случайным взаимодействием элементов моделируемой системы со средствами СР, то есть с исследованием последовательностей случайных событий по поступлению в систему пакетов с определенными идентификаторами. Указанные последовательности событий инициируют переход ИС в пределах дискретного фазового пространства качественных состояний, характеризующих этапы СР.

В связи с этим, оценка оптимальных параметров конфигурирования СФХ ИС, а именно частоты конфигурирования СФХ ИС, производится на основании расчета вероятностно-временных характеристик с учетом случайного характера описываемого процесса.

Исходя из известных результатов[4], полученных относительно сходимости большинства массовых потоков независимых событий к процессу Пуассона, вводится допущение об ординарности и отсутствии последействия рассматриваемых потоков событий. В общем случае поток событий является неоднородным, что характеризуется нестационарностью случайного процесса в широком смысле (зависимость его математического ожидания и дисперсии от времени).

Вследствие того, что качественная характеристика моделируемой системы может быть представлена вектором дискретных состояний, изменяющихся под влиянием соответствующих последовательностей событий, целесообразно использование математического аппарата теории вероятностей, в частности цепей (процессов) Маркова с непрерывным временем. Так как время ожидания наступления соседних событий в последовательности распределено экспоненциально, то основной статистической характеристикой является интенсивность потока событий, численно равная математическому ожиданию количества событий в единицу времени.

Марковский процесс с дискретным пространством состояний и непрерывным временем однозначно определяется ориентированным графом, представленным на рис 1. Пространство фазовых состояний моделируемой системы S представленных на графе является конечным множеством несовместных событий, описывающих существенные свойства системы и изменяющихся скачкообразно: S_1 – состояние, в котором система функционирует в штатном режиме, активность средств СР и эксплуатация уязвимостей отсутствует; S_2 – состояние, в котором злоумышленник с использованием средств СР идентифицировал *IP*-адреса и маски подсетей целевой системы, определил путь к целевым узлам системы; S_3 – состояние, в котором злоумышленник с использованием средств СР вскрыл наличие средств сетевой защиты и идентифицировал открытые сетевые порты; S_4 – состояние, в котором злоумышленник с использованием средств СР идентифицировал типы и версии ОС, сервисов и служб, используемого ПО; S_5 – состояние, в котором

4 Гнеденко Б. В., Коваленко И. Н. Введение в теорию массового обслуживания. – М.: Наука, 1966. С. 152.

злоумышленник осуществляет эксплуатацию уязвимостей.

Эволюция процесса функционирования системы происходит под воздействием потоков случайных событий, которые характеризуются интенсивностями λ_{ij} и трактуются следующим образом: λ_{12} – интенсивность потока *ICMP*- и *DNS*-запросов (определение пути к узлу и его активности); λ_{23} – интенсивность потока *TCP*- и *UDP*-запросов (определение открытых сетевых портов); λ_{34} – интенсивность потока *TCP*-, *UDP*- и *ICMP*-запросов (определение типа и версии ОС, сервисов и служб); λ_{45} – интенсивность потока событий по эксплуатации уязвимостей ИС.

Значения интенсивностей потоков случайных событий, характеризующих действия злоумышленника при переходе моделируемой системы из состояния в состояние, определяются из следующих соображений. В рассматриваемом случае, в соответствии с особенностями функционирования сетевого сканера *NMap* [18], для *TCP* и *UDP* сканирования средство СР направляет в среднем два пакета на каждый сетевой порт, всего портов 65535 (*TCP*)+65535(*UDP*). Обычно сканируется только первые 1024 стандартных порта, итого 2048 (*TCP+UDP*). Для трассировки пути к узлу и для проверки его доступности *NMap* направляет каждому узлу два пакета *ICMP*. Для распознавания типа и версии операционной системы (*OS fingerprinting*), программного обеспечения, а также сетевых сервисов и служб *NMap* отправляет до 16 *TCP*, *UDP* и *ICMP* запросов на известные открытые и закрытые порты целевого узла. Эти запросы специально применяются для исключения различных неоднозначностей в стандартных протоколах.

В качестве средства противодействия СР применяется разработанное техническое решение, основанное на конфигурировании СФХ ИС, таких как *IP*-адреса, время их аренды, маска подсети, номера сетевых портов взаимодействия и доменные имена [19]. Основу технического решения составляет совокупность динамических *DHCP* и *DNS* серверов, управляемых специализированным контроллером, взаимодействующим с применяемыми в ИС средствами сетевой защиты. Потоки случайных событий, описывающие противодействие средствам СР со стороны системы защиты, характеризуются следующими параметрами: λ_{21} – интенсивность потока событий по конфигурированию *IP*-адресов узлов, изменяемых в рамках нескольких подсетей; λ_{31} – интенсивность потоков событий по конфигурированию *IP*-адресов узлов и номеров сетевых портов, изменяемых в рамках нескольких подсетей и пространства динамических портов, соответственно; λ_{41} – интенсивность потоков событий по конфигурированию *IP*-адресов узлов, номеров сетевых портов взаимодействия и доменных имен. Потоки событий средств защиты представляют собой команды между контроллером, *DHCP* сервером и клиентами на прекращение аренды действующих СФХ ИС и назначение новых.

С целью проверки гипотезы о стационарности (однородности) марковского процесса, рассмотрим

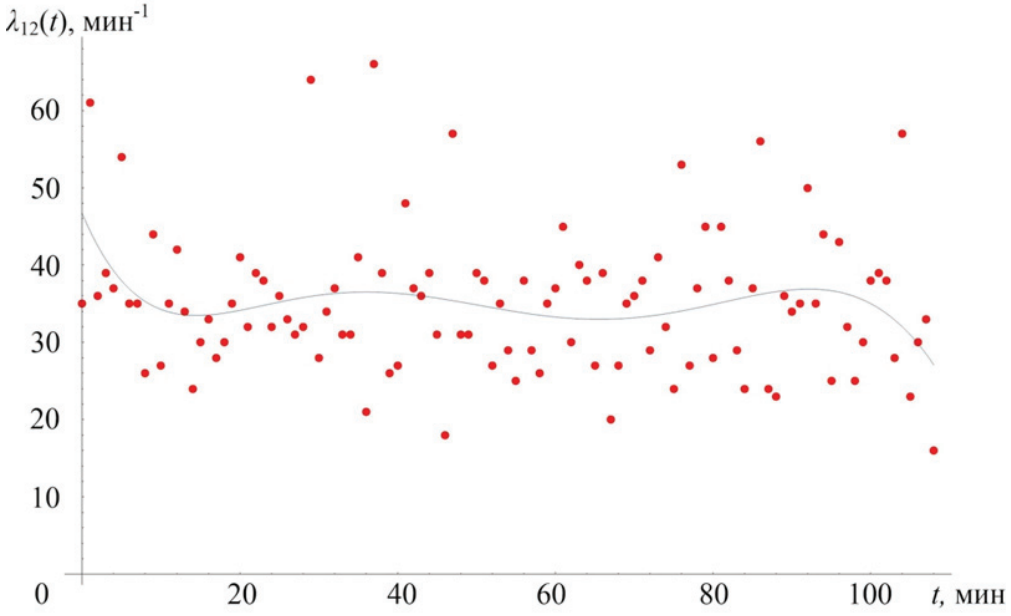

Рис. 2. Оценка зависимости интенсивности $\lambda_{12}(t)$

реализацию потока пакетов (*ICMP*- и *DNS*-запросов), посредством которых осуществляется сканирование адресного пространства *IP*-адресов узлов ИС. Оценка параметров потока пакетов осуществлялась с использованием анализатора сетевого трафика *WireShark*, выборка проводилась на внешнем интерфейсе маршрутизатора, отделяющего локальный сегмент моделируемой ИС, за интервал времени равный 2 часам. Применяя методы регрессионного анализа для оценки уравнения регрессии интенсивности λ_{12} от времени, с определенной степенью точности, можно сделать вывод о стационарности потока случайных событий на рассматриваемых временных интервалах (рис. 2).

Формализованная постановка задачи

Исходя из качественной интерпретации случайного процесса, задачу по определению оптимальной частоты конфигурирования СФХ ИС можно сформулировать следующим образом: с учетом заданной математической модели ведения СР в условиях конфигурирования СФХ, начальных условий и ограничений на матрицу входных, управляющих и выходных характеристик модели, необходимо найти такой вектор управления (минимальных частот конфигурирования СФХ ИС), при которых обеспечивается определенная вероятность вскрытия (идентификации) ИС. Иными словами, решается задача определения оптимальных параметров конфигурирования СФХ, минимально использующих ресурсные возможности ИС при обеспечении заданного уровня ее защищенности (вероятности вскрытия ИС средствами СР).

Вектор $x(t)$ фазовых переменных (выходных характеристик модели) системы – функции распределения $F_{ij}(t)$ времени, необходимого для достижения состояния j из состояния i впервые. То есть функция распределения $F_{ij}(t)$ в момент времени t численно равна вероятности того, что система за интервал времени $(0; t)$ впервые достигнет состояния j, если в начальный момент времени, система достоверно находилась в состоянии i:

$$x(t) = \{F_{11}(t), F_{12}(t), \cdots, F_{15}(t)\}. \quad (1)$$

Входные характеристики модели можно представить в виде квадратной матрицы интенсивностей потоков событий и/или плотностей вероятности случайных величин ζ_{ij} времени по переходу системы из состояния S_i в состояние S_j.

$$\lambda = \begin{vmatrix} \lambda_{11} & \dots & \lambda_{15} \\ \dots & \dots & \dots \\ \lambda_{51} & \dots & \lambda_{55} \end{vmatrix}, f(t) = \begin{vmatrix} f_{11}(t) & \dots & f_{15}(t) \\ \dots & \dots & \dots \\ f_{51}(t) & \dots & f_{55}(t) \end{vmatrix}. \quad (2)$$

Так как, рассматриваемый случайный процесс является марковским, то времена ожидания смены состояний распределены по экспоненциальному закону с плотностями вероятностей:

$$f_{\zeta_{ij}}(t) = \lambda_{ij} e^{-\lambda_{ij} t}, t \geq 0, \quad (3)$$

Вектор управления $u(t)$ представляет собой набор средних интервалов времени ΔT_i, по истечении которых происходит конфигурирование (смена) СФХ ИС с целью воздействия на элементы вектора фазовых переменных системы. Указанные интервалы времени ΔT_i обратно пропорциональны интенсивностям (частотам) потоков событий конфигурирования СФХ ИС:

$$u = \{u_1, u_2, u_3\}, \quad (4)$$

$$u_1 = \Delta T_1 = \frac{1}{\lambda_{21}}; u_2 = \Delta T_2 = \frac{1}{\lambda_{31}}; u_3 = \Delta T_3 = \frac{1}{\lambda_{41}}. \quad (5)$$

Начальное условие: система в начальный момент времени t=0 достоверно находится в состоянии S_1, то есть:

$$x(0) = \{F_{11}(0), F_{12}(0), \cdots, F_{15}(0)\} = \{1, 0, 0, 0, 0\}. \quad (6)$$

Допустимые значения элементов вектора выходных характеристик $x(t)$ модели определяются, исходя из определения функции распределения непрерывной случайной величины:

$$0 \leq F_{ij}(t) \leq 1. \quad (7)$$

Допустимые значения элементов вектора управления могут принимать следующие значения:

$$u_{1\text{кр.}} \leq u_1 \leq \infty, u_{2\text{кр.}} \leq u_2 \leq \infty, u_{3\text{кр.}} \leq u_3 \leq \infty, \quad (8)$$

Причем, минимальные значения интервалов времени $u_{i\text{кр.}}$ конфигурирования СФХ ИС устанавливаются, исходя из соображений обеспечения устойчивости информационного обмена между узлами ИС. Так, предельные частоты конфигурирования СФХ узла ИС задаются следующими: частота конфигурирования *IP*-адресов $u_{1\text{кр.}}$ принимает значение от 30 мс, частота совместного конфигурирования *IP*-адресов и сетевых портов $u_{2\text{кр.}}$ принимает значение от 60 мс, а конфигурирование *IP*-адресов, сетевых портов и *DNS*-имен может производиться не чаще, чем через $u_{3\text{кр.}}$=5 сек. Выбор значений предельных частот конфигурирования каждого из СФХ ИС обусловлен наличием необходимого времени на завершение аренды ранее задан-

ных *IP*-адресов и других сетевых параметров, а также активных сетевых соединений и других процессов без нарушения информационного обмена в ИС [20].

Уравнение объекта управления (математическая модель процесса) представляет собой выражение по определению функций распределения времени, необходимого для достижения впервые состояний случайного процесса:

а) при условии, что марковский процесс представляет собой однонаправленную последовательность невозвратных состояний (без задействования механизмов конфигурирования СФХ ИС), то плотность вероятности суммы независимых случайных величин ζ_{ij} времени по переходу системы из состояния S_i в состояние S_j, рассчитывается, исходя из формулы свертки [18]:

$$f_{\zeta_{12}+\ldots+\zeta_{45}}(t) = f_{15}(t) = f_{\zeta_{12}} * \ldots * f_{\zeta_{45}}(t), \quad (9)$$

а функция распределения рассчитывается соответственно:

$$F_{\zeta_{12}+\ldots+\zeta_{45}}(t) = F_{15}(t) = \int_0^t f_{\zeta_{12}} * \ldots * f_{\zeta_{45}}(t)dt, \quad (10)$$

и свертка (10) для экспоненциальных распределений случайных величин ζ_{ij} имеет следующий аналитический вид:

$$f_{\zeta_{12}+\ldots+\zeta_{45}}(t) = \begin{cases} \dfrac{\prod_{i,j=1}^{5}\lambda_{ij}}{\prod_{i,j=1,ij\neq 12}^{5}(\lambda_{12}-\lambda_{ij})}\sum_{i,j=1}^{5}e^{-\lambda_{ij}t}, \forall\lambda_{12}\neq\lambda_{23}\neq\lambda_{34}\neq\lambda_{45}, \\ \dfrac{\lambda^n}{(n-1)!}t^{(n-1)}e^{-\lambda t} = \dfrac{\lambda^4}{6}t^3e^{-\lambda t}, \lambda_{12}=\lambda_{23}=\lambda_{34}=\lambda_{45}=\lambda. \end{cases} \quad (11)$$

где n=3 – количество переходов системы из начального состояния (S_1) в финальное (S_5);

б) в противном случае (при λ_{21}, λ_{31}, $\lambda_{41}>0$), существует возможность использования результатов теории полумарковских процессов [22], тогда искомая функция распределения в матричном виде будет иметь вид:

$$F(t) = \lim_{x\to\infty}\frac{1}{2\pi j}\int_{x-j\omega}^{x+j\omega}e^{ts}\left(\frac{1}{s}f(s)\left(I-f(s)\right)^{-1}\left[I\times\left(I-f(s)\right)^{-1}\right]^{-1}\right)ds \quad (12)$$

$$f(s) = L[f(t)] = \int_0^{\infty}e^{-st}f(t)dt, \quad (13)$$

где $f(s)$ – преобразование Лапласа от матрицы плотностей вероятностей $f(t)$; I – единичная матрица, размерность которой совпадает с мощностью пространства фазовых состояний марковского процесса; оператор «×» обозначает бинарную операцию поэлементного произведения элементов матриц.

Функционал качества (целевая функция) представляет собой следующее выражение:

$$J[x(t),u,\lambda] = \begin{cases} u_1(\lambda\,|F_{12}(u_1) \le F_{12}^{кр.}) \to \max, \\ u_2(\lambda\,|F_{13}(u_2) \le F_{13}^{кр.}) \to \max, \\ u_3(\lambda\,|F_{14}(u_3) \le F_{14}^{кр.}) \to \max. \end{cases} \quad (14)$$

где $F_{12}^{кр.}$ – критическое значение вероятности того, что средство сетевой разведки достигнет состояния S_2 за интервал времени ΔT_1; $F_{13}^{кр.}$ – критическое значение вероятности того, что средство СР достигнет состояния S_3 за интервал времени ΔT_2; $F_{14}^{кр.}$ – критическое значение вероятности того, что средство СР достигнет состояния S_4 за интервал времени ΔT_3.

Пусть $F_{12}^{кр.} = F_{13}^{кр.} = F_{14}^{кр.} = 0,2$. Определим функцию распределения $F_{12}(t)$ для ориентированного графа (рис.1) без конфигурирования СФХ ИС и определим значение среднего интервала времени ΔT_1 реконфигурации значений *IP*-адресов узлов ИС:

$$F_{12}(t) = \int_0^t f_{12}dt = 1 - e^{-\frac{3}{4}t}. \quad (15)$$

Как видно из рис. 3, получившееся значение $\Delta T_1 = 0,2975$ с на порядок выше предельно допустимого значения $u_{1кр.}$=30 мс, что говорит о наличии адаптационного ресурса для повышения частоты конфигурирования *IP*-адресов при повышении интенсивности сканирования защищаемой ИС средством СР.

Аналогично (рис. 3), определим функцию распределения $F_{13}(t)$ с учетом интенсивности $\lambda_{21} = \Delta T_1^{-1} = 0,2975$ с конфигурирования *IP*-адресов и определим значение среднего интервала времени ΔT_2 совместного изменения *IP*-адресов и сетевых портов на узлах ИС:

$$F_{13}(t) = 1 + 0,000578\cdot e^{-4,03035t} + 0,18786\cdot e^{-0,5t} - 1,18843\cdot e^{-0,08099t}, \quad (16)$$

$$\Delta T_2 = 4,59899A$$

Значение $\Delta T_2 = 4,59899$ с более, чем на порядок выше предельно допустимого значения $u_{2кр.}$=60 мс, что также указывает на существование адаптационного ресурса для повышения частоты конфигурирования *IP*-адресов и сетевых портов узлов ИС.

Далее, с учетом значений *IP*-адресов и сетевых портов узлов определим функцию распределения

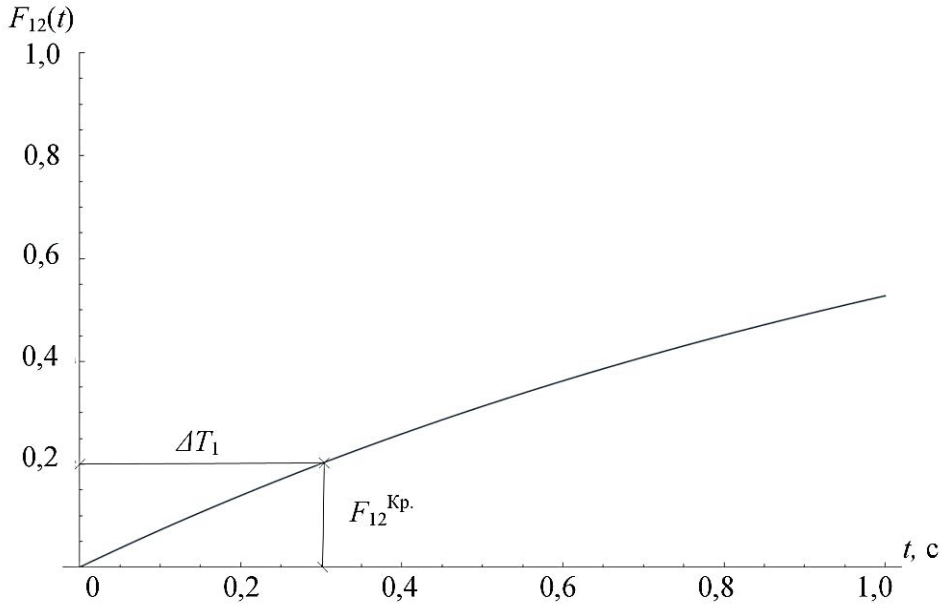

Рис. 3. Определение значения интервала времени реконфигурации IP-адресов узлов ИС

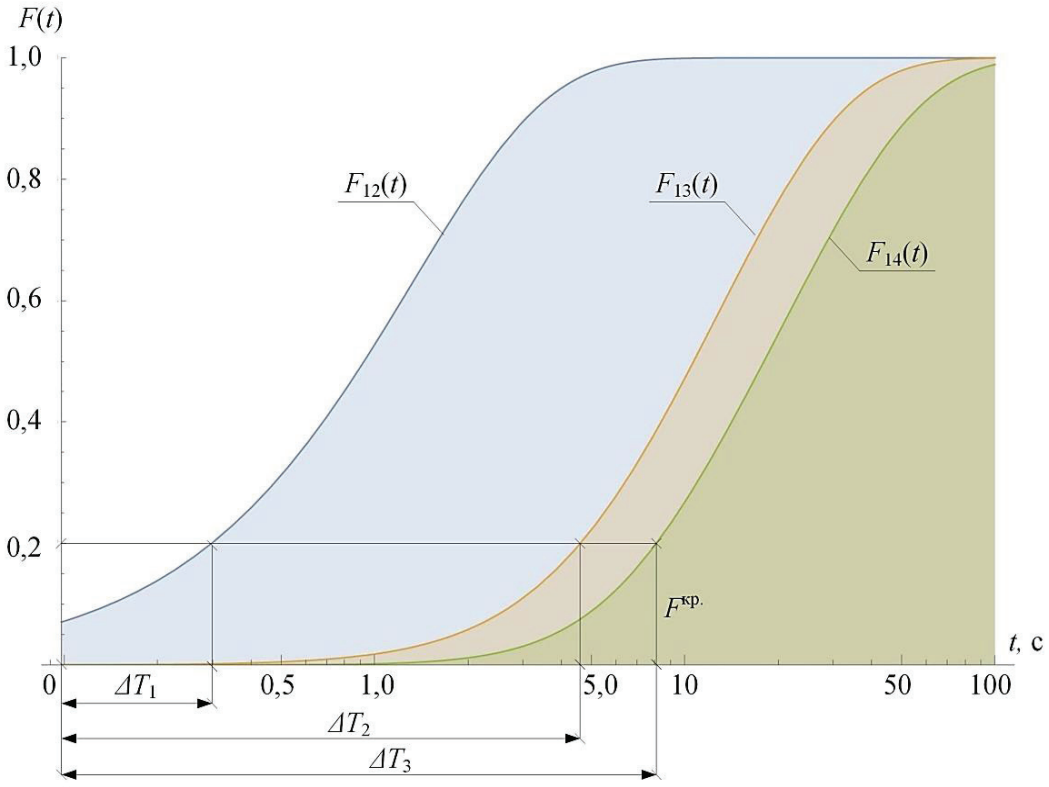

Рис. 4. Определение значений интервалов времени конфигурирования СФХ (IP-адресов, IP-адресов и сетевых портов, IP-адресов и сетевых портов и DNS-имен) узлов ИС

$F_{14}(t)$ и интервал времени совместного изменения *IP*-адресов, сетевых портов и *DNS*-адресов (ΔT_3):

$$F_{13}(t) = 1{,}0 + 3{,}7517 \cdot 10^{-6} \cdot e^{-4{,}03031t} + \\ + 0{,}6040 \cdot e^{-0{,}5409t} - 4{,}6507 \cdot e^{-0{,}4034t} + \\ + 9{,}8670 \cdot e^{-0{,}3333t} - 5{,}5766 \cdot e^{-0{,}3034t} - \\ - 0{,}1049 \cdot e^{-0{,}1459t} - 1{,}1388 \cdot e^{-0{,}0287t}), \quad (17)$$

$$\Delta T_3 = 8{,}08A$$

Достигаемый положительный эффект за счет конфигурирования СФХ ИС демонстрируется графической интерпретацией функции распределения времени, необходимого для достижения финального состояния S_5, характеризующего эксплуатацию уязвимостей злоумышленником, без учета конфигурирования СФХ (рис. 5, кривая 1), с учетом оптимальных параметров конфигурации СФХ (рис. 5, кривая 2), и с учетом предельно допустимых параметров конфигурации СФХ (рис. 5, кривая 3).

Как видно из рис. 5, использование оптимальных параметров конфигурирования СФХ ИС, минимально использующих ее ресурсы, обеспечивает увеличение времени, необходимого для начала эксплуатации уязвимостей злоумышленником, при заданных интенсивностях сканирования, с вероятностью 0,2 более чем в два раза с $\Delta T' = 4{,}68$ с до $\Delta T'' = 13{,}11$ с, а конфигурирование СФХ ИС с предельными значениями параметров, увеличивают продолжительность этого интервала времени более чем на два порядка до $\Delta T''' = 1982$ с.

Также, решением системы дифференциальных уравнений Колмогорова с учетом варьирования одного из дополнительных параметров, можно оценить характер переходного процесса и длительность времени, необходимого для начала эксплуатации уязвимостей злоумышленником, при фиксированных значениях параметров конфигурирования СФХ и изменении интенсивности сканирования.

Решение данной системы дифференциальных уравнений может быть получено в аналитической форме с использованием метода Эйлера и поиском собственных чисел и векторов матрицы интенсивностей потоков событий либо с использованием численных методов (явные, неявные методы Рунге-Кутта, Эйлера, многошаговый метод Адамса, метод Гира и т.д.).

Графическая форма численного решения вышеуказанного уравнения неявным методом Рунге-Кутта

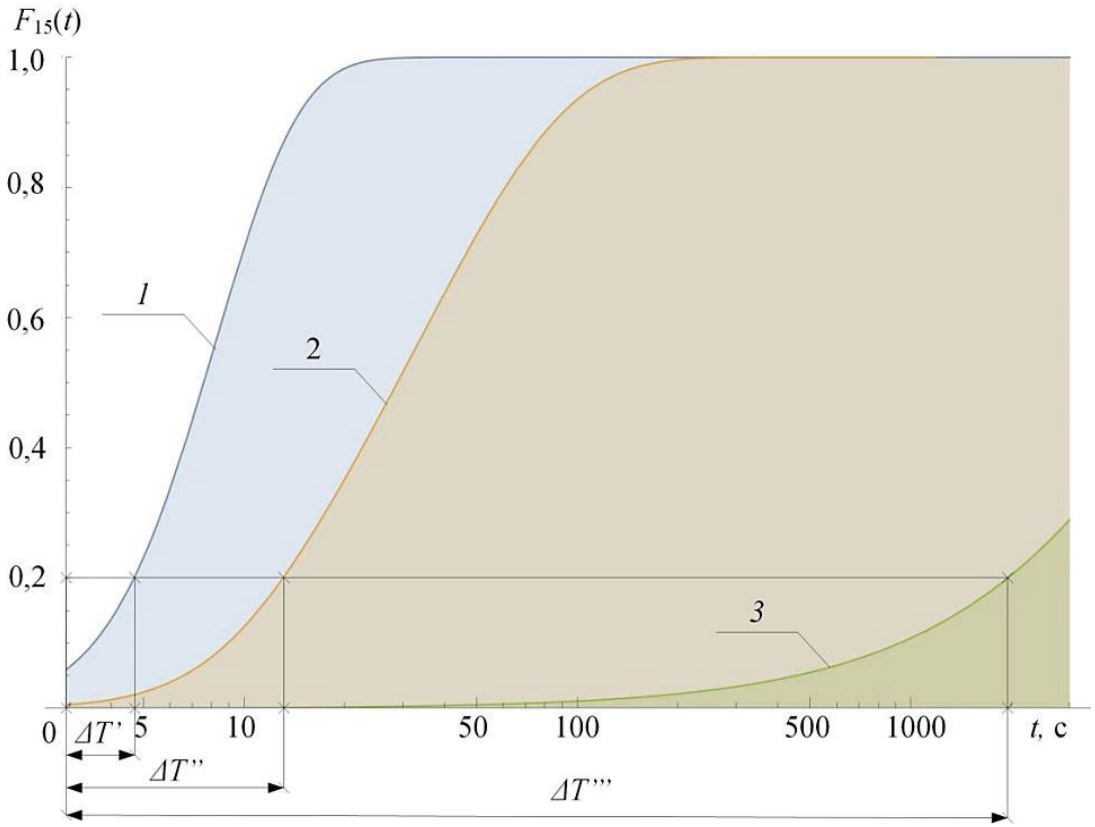

Рис. 5. Оценка эффекта от конфигурирования СФХ ИС в условиях сетевой разведки

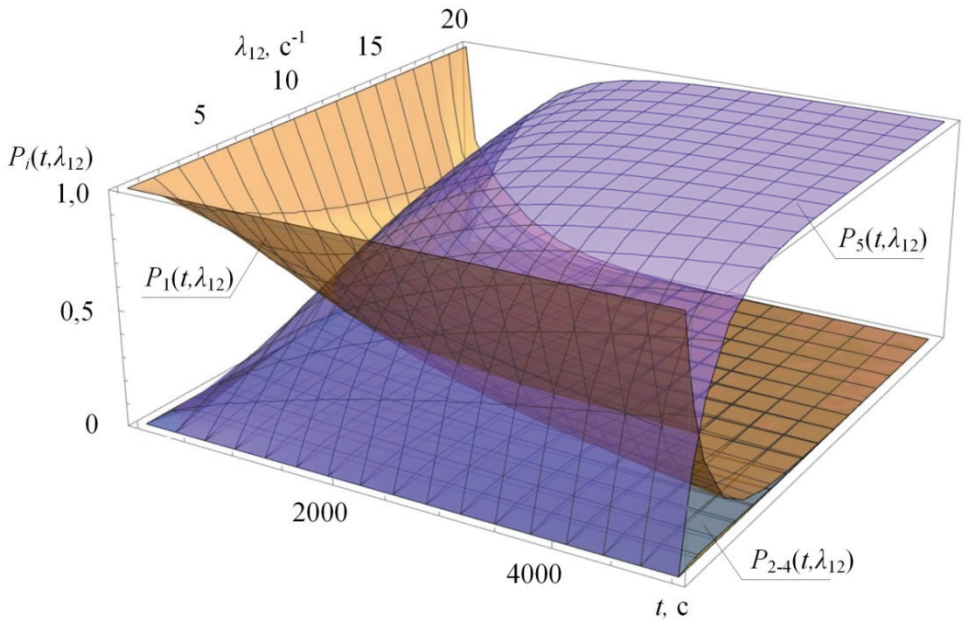

Рис. 6. Зависимость вероятностей пребывания системы от времени и интенсивности сканирования IP-адресов средствами СР

8 порядка (рис. 6) позволяет оценить характер зависимости вероятности пребывания системы в состоянии S_5 при увеличении интенсивности сканирования *IP*-адресов.

Как видно из рис. 6, при заданных предельных значениях параметров конфигурирования СФХ ИС, при интенсивности сканирования $\lambda_{12} = 5\text{c}^{-1}$ злоумышленником будет достоверно осуществлена идентификация ИС и проведена эксплуатация ее уязвимостей за интервал времени равный 2000 с.

Таким образом, в зависимости от интенсивностей сканирования существует возможность конфигурирования СФХ ИС с целью снижения результативности ведения СР и возможности эксплуатации уязвимостей ИС, при заданном уровне защищенности ИС и обеспечения устойчивости информационного обмена.

Выводы

В статье рассмотрена задача поиска оптимальной частоты конфигурирования СФХ ИС на каждом из этапов СР с учетом выполнения требований по минимальному использованию ресурсных возможностей ИС и обеспечению заданного значения вероятности ее вскрытия. С использованием методологии теории вероятностей и математической статистики выполнена качественная и формализованная постановка задачи, сформулированы критерии оптимизации параметров конфигурирования СФХ ИС.

Получены значения оптимальных параметров конфигурирования СФХ ИС, позволяющие обеспечивать заданный уровень защищенности ИС и устойчивости ее информационного обмена. Из полученных результатов видно, что конфигурирование СФХ ИС с оптимальными параметрами обеспечивает увеличение времени идентификации ИС средствами СР с последующей эксплуатацией ее уязвимостей злоумышленником, при заданных интенсивностях сканирования, более чем в два раза, а конфигурирование СФХ ИС с предельными значениями параметров, увеличивает длительность идентификации с последующей эксплуатацией уязвимостей ИС более чем на два порядка.

Научная новизна предложенного метода заключается в решении задачи скалярной оптимизации частоты конфигурирования структурно-функциональных характеристик информационной системы в условиях сетевой разведки с использованием математического аппарата полумарковских случайных процессов.

Рецензент: *Максимов Роман Викторович, доктор технических наук, профессор, профессор Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: rvmaxim@yandex.ru*

Литература

1. Kanellopoulos, A., Vamvoudakis, K.G. A Moving Target Defense Control Framework for Cyber-Physical Systems. IEEE Trans. Autom. Control 2020, 65, 1029-1043.
2. Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., Kambhampati, S. A Survey of Moving Target Defenses for Network Security. IEEE Commun. Surv. Tutor. 2020, 22, 1909-1941.
3. Giraldo, J. and Cardenas, A. A. Moving target defense for attack mitigation in multi-vehicle systems. In Proactive and Dynamic Network Defense, Cham, Switzerland:Springer, 2019, 163-190.
4. Vadlamudi, S. G., Sengupta, S., Taguinod, M., Zhao, Z., Doup´e, A., Ahn, G.-J. and Kambhampati, S. Moving target defense for web applications using bayesian stackelberg games. In Proceedings of AAMAS, 2016, 1377–1378.
5. Иванов И.И., Максимов Р.В. Спецификация функциональной модели для расширения пространства демаскирующих признаков в виртуальных частных сетях / И.И. Иванов, Р.В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации: сб. тр. участников всеармейской научно-практической конференции. – Санкт-Петербург, 2017. С. 138-147.
6. Иванов И.И., Максимов Р.В. Этюды технологии маскирования функционально-логической структуры информационных систем / И.И. Иванов, Р.В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации: сб. тр. участников всеармейской научно-практической конференции. – Санкт-Петербург, 2017. С. 147-154.
7. Maximov R.V., Ivanov I.I., Sharifullin S.R. Network Topology Masking in Distributed Information Systems // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 83-87.
8. Yan S., Huang X., Ma M., Zhang P., Ma Y. A novel efficient address mutation scheme for IPv6 networks // IEEE Access, vol. 5, 2017. P. 7724–7736.
9. Cho, J., Sharma, D.P. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. IEEE Commun. Surv. Tutor. 2020, 22, 709-745.
10. Sokolovsky, S.P., Telenga, A.P., Voronchikhin, I.S. Moving target defense for securing Distributed Information Systems // Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-методической конференции / под редакцией Д.Н. Борисова. – Воронеж.: ВГУ, 2019. С. 639-643.
11. Способ защиты вычислительных сетей. Пат. 2716220 Рос. Федерация, МПК G06F 21/606 / Максимов Р.В., Соколовский С.П., Ворончихин И.С.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2019123718; заявл. 22.07.2019; опубл. 06.03.20. Бюл. № 7. 33 с.
12. Способ защиты вычислительных сетей. Пат. 2726900 Рос. Федерация, МПК G06F 21/554 / Максимов Р.В., Соколовский С.П., Ворончихин И.С., Гритчин А.Д. и др.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2019140769; заявл. 19.12.2019; опубл. 16.07.20. Бюл. № 20. 45 с.
13. Максимов Р.В., Соколовский С.П., Ворончихин И.С. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей // Информатика и автоматизация. 2020. № 5. С. 1018-1049.
14. Соколовский С.П. Модель защиты информационной системы от сетевой разведки динамическим управлением ее структурно-функциональными характеристиками // Вопросы оборонной техники. Серия 16 противодействие терроризму. 2020. № 7-8. С. 62-73.
15. Wang K., Chen X., Zhu Y. Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks // PLoS ONE 12 (5): e01771112017, 2017. P. 22.
16. 16. Соколовский С.П., Максимов Р.В., Ворончихин И.С. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей // Информатика и автоматизация, 2020. Т. 19. № 5. С. 1090–1121.
17. Iskolnyy B.B., Maximov R.V., Sharifullin S.R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 59-65.
18. Glen D. Learn Kali Linux 2019: Perform powerful penetration testing using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark. Birmingham: Packt Publishing, 2019. 550 p.
19. Мультисервисный маршрутизатор с управлением параметрами сетевых соединений и маскированием вычислительной сети. Пат. 205636 Рос. Федерация, МПК H04L 12/00 / Максимов Р.В., Соколовский С.П., Ворончихин И.С., Гугин А.Ю.; заявитель и патентообладатель Общество с ограниченной ответственностью «Питер Софт» (RU). – № 2020128357; заявл. 24.08.2020; опубл. 23.07.2021. Бюл. № 21. 21 с.
20. Wang, K., Chen, X., Zhu, Y. Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks. PLoS ONE 12 (5): e01771112017, 2017, 22 p. https://doi.org/10.1371/journal.pone.0177111.

DETERMINATION OF OPTIMAL PARAMETERS FOR CONFIGURING INFORMATION SYSTEMS IN THE CONDITIONS OF NETWORK INTELLIGENCE

Gorbachev A.A.[5], Sokolovsky S.P.[6], Kaplin M.A.[7]

Research objective: *to improve the information systems security against network reconnaissance.*

Methods used: *in order to achieve the goal of the research, the methods of mathematical statistics and random processes study were used.*

Research result: *the task of determining the optimal frequency of dynamic configuration of the information system's structural and functional characteristics at each stage of network reconnaissance, taking into account the requirements for the minimum use of resource capabilities and ensuring a given value of the probability of disclosure of true values of the characteristics of the protected object was solved. The process of network reconnaissance and counteraction is formalized in the form of a Markov random process with discrete states and continuous time. Based on considerations of stability of information exchange between nodes of information system and capabilities of network reconnaissance, the maximum values of time intervals of dynamic configuration of structural and functional characteristics are determined. The obtained values of the optimal and maximum allowable frequency of dynamic configuration allow to estimate the time of disclosure of information system at given intensities of network scanning by reconnaissance tools. The results allow to provide a given level of protection of information system and the stability of its information exchange at the expense of the optimal frequency of dynamic configuration of its structural and functional characteristics.*

Scientific novelty: *solving the problem of scalar optimization of the frequency of configuration of the structural and functional characteristics of the information system under conditions of network reconnaissance using the mathematical apparatus of semi-Markov random processes.*

Keywords: *network scanning, random process, computer attack, stability of information exchange, probability of disclosure, reconnaissance tool.*

References

1. Kanellopoulos, A., Vamvoudakis, K.G. A Moving Target Defense Control Framework for Cyber-Physical Systems. IEEE Trans. Autom. Control 2020, 65, 1029-1043.
2. Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., Kambhampati, S. A Survey of Moving Target Defenses for Network Security. IEEE Commun. Surv. Tutor. 2020, 22, 1909-1941.
3. Giraldo, J. and Cardenas, A. A. Moving target defense for attack mitigation in multi-vehicle systems. In Proactive and Dynamic Network Defense, Cham, Switzerland:Springer, 2019, 163-190.
4. Vadlamudi, S. G., Sengupta, S., Taguinod, M., Zhao, Z., Doup´e, A., Ahn, G.-J. and Kambhampati, S. Moving target defense for web applications using bayesian stackelberg games. In Proceedings of AAMAS, 2016, 1377–1378.
5. Ivanov I.I., Maksimov R.V. Specifikacija funkcional'noj modeli dlja rasshirenija prostranstva demaskirujushhih priznakov v virtual'nyh chastnyh setjah / I.I. Ivanov, R.V. Maksimov // Innovacionnaja dejatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii: sb. tr. uchastnikov vsearmejskoj nauchno-prakticheskoj konferencii. – Sankt-Peterburg, 2017. S. 138-147.
6. Ivanov I.I., Maksimov R.V. Jetjudy tehnologii maskirovanija funkcional'no-logicheskoj struktury informacionnyh sistem / I.I. Ivanov, R.V. Maksimov // Innovacionnaja dejatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii: sb. tr. uchastnikov vsearmejskoj nauchno-prakticheskoj konferencii. – Sankt-Peterburg, 2017. S. 147-154.
7. Maximov R.V., Ivanov I.I., Sharifullin S.R. Network Topology Masking in Distributed Information Systems // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 83-87.

5 Alexander A. Gorbachev, Applicant for academic degree of Ph.D., Krasnodar, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: infosec23.00@mail.ru

6 Sergey P. Sokolovsky, Ph.D., Associate Professor, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: mtd.krd@mail.ru

7 Maxim A. Kaplin, Lecturer, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: popi901@yandex.ru

8. Yan S., Huang X., Ma M., Zhang P., Ma Y. A novel efficient address mutation scheme for IPv6 networks // IEEE Access, vol. 5, 2017. R. 7724–7736.
9. Cho, J., Sharma, D.P. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. IEEE Commun. Surv. Tutor. 2020, 22, 709-745.
10. Sokolovsky, S.P., Telenga, A.P., Voronchikhin, I.S. Moving target defense for securing Distributed Information Systems // Informatika: problemy, metodologija, tehnologii. Sbornik materialov XIX mezhdunarodnoj nauchno-metodicheskoj konferencii / pod redakciej D.N. Borisova. – Voronezh.: VGU, 2019. S. 639-643.
11. Sposob zashhity vychislitel'nyh setej. Pat. 2716220 Ros. Federacija, MPK G06F 21/606 / Maksimov R.V., Sokolovskij S.P., Voronchihin I.S.; zajavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishhe (RU). – № 2019123718; zajavl. 22.07.2019; opubl. 06.03.20. Bjul. № 7. 33 s.
12. Sposob zashhity vychislitel'nyh setej. Pat. 2726900 Ros. Federacija, MPK G06F 21/554 / Maksimov R.V., Sokolovskij S.P., Voronchihin I.S., Gritchin A.D. i dr.; zajavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishhe (RU). – № 2019140769; zajavl. 19.12.2019; opubl. 16.07.20. Bjul. № 20. 45 s.
13. Maksimov R.V., Sokolovskij S.P., Voronchihin I.S. Algoritm i tehnicheskie reshenija dinamicheskogo konfigurirovanija klient-servernyh vychislitel'nyh setej // Informatika i avtomatizacija. 2020. № 5. S. 1018-1049.
14. Sokolovskij S.P. Model' zashhity informacionnoj sistemy ot setevoj razvedki dinamicheskim upravleniem ee strukturno-funkcional'nymi harakteristikami // Voprosy oboronnoj tehniki. Serija 16 protivodejstvie terrorizmu. 2020. № 7-8. S. 62-73.
15. Wang K., Chen X., Zhu Y. Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks // PLoS ONE 12 (5): e01771112017, 2017. R. 22.
16. Sokolovskij S.P., Maksimov R.V., Voronchihin I.S. Algoritm i tehnicheskie reshenija dinamicheskogo konfigurirovanija klient-servernyh vychislitel'nyh setej // Informatika i avtomatizacija, 2020. T. 19. № 5. S. 1090–1121.
17. Iskolnyy B.B., Maximov R.V., Sharifullin S.R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 59-65.
18. Glen D. Learn Kali Linux 2019: Perform powerful penetration testing using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark. Birmingham: Packt Publishing, 2019. 550 p.
19. Mul'tiservisnyj marshrutizator s upravleniem parametrami setevyh soedinenij i maskirovaniem vychislitel'noj seti. Pat. 205636 Ros. Federacija, MPK H04L 12/00 / Maksimov R.V., Sokolovskij S.P., Voronchihin I.S., Gugin A.Ju.; zajavitel' i patentoobladatel' Obshhestvo s ogranichennoj otvetstvennost'ju «Piter Soft» (RU). – № 2020128357; zajavl. 24.08.2020; opubl. 23.07.2021. Bjul. № 21. 21 s.
20. Wang, K., Chen, X., Zhu, Y. Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks. PLoS ONE 12 (5): e01771112017, 2017, 22 r. https://doi.org/10.1371/journal.pone.0177111.