

**И. Г. Дровникова**, доктор технических наук, доцент  
**М. Л. Парин**ов, кандидат технических наук, доцент  
**Е. С. Овчинникова**, адъюнкт

**АНАЛИТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ ВЕРОЯТНОСТИ  
РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК  
В ДИНАМИКЕ КОНФЛИКТНОГО ВЗАИМОДЕЙСТВИЯ  
С СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ  
В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ  
ОРГАНОВ ВНУТРЕННИХ ДЕЛ**

**ANALYTICAL MODEL FOR ASSESSING THE PROBABILITY  
OF NETWORK ATTACKS  
IN THE DYNAMICS OF CONFLICT INTERACTION  
WITH THE INFORMATION SECURITY SYSTEM  
IN AUTOMATED SYSTEMS OF INTERNAL AFFAIRS BODIES**

*На основе применения теории конечных полумарковских процессов к динамическим моделям реализации типовых сетевых атак в автоматизированных системах органов внутренних дел и обобщенной динамической модели информационного конфликта «Сетевая атака — Система защиты», построенным на сетях Петри—Маркова, в статье представлена аналитическая модель оценки вероятности реализации сетевых атак. Разработанная модель позволяет провести точную количественную оценку вероятности и исследовать вероятностно-временные характеристики реализации атак в динамике их конфликтного взаимодействия с системой защиты информации от несанкционированного доступа с учетом изначальных и потенциальных возможностей конфликтующих сторон. Аналитическая модель может быть использована для определения наиболее опасных атак и построения частной модели актуальных атак для конкретной автоматизированной системы, эксплуатируемой в защищенном исполнении на объекте информатизации органов внутренних дел.*

*Based on the application of the theory of finite semi-Markov processes to dynamic models of the implementation of typical network attacks in automated systems of internal affairs bodies and the generalized dynamic model of the information conflict "Network attack-Protection System", built on Petri—Markov networks, the article presents an analytical model for assessing the probability of implementing network attacks. The developed model allows for an accurate quantitative assessment of the probability and to investigate the probabilistic and temporal characteristics of the implementation of attacks in the dynamics of their conflict interaction with the information protection system from unauthorized access, taking into account the initial and potential capabilities of the conflicting parties. The analytical model can be used to determine the most dangerous attacks and build a private model of actual attacks for a specific automated system operated in a protected version at the informatization facility of internal affairs bodies.*

**Введение.** Обеспечение эффективного функционирования современных автоматизированных систем (АС), эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД), приводит к необходимости учета возможной опасности реализации сетевых атак на их информационные ресурсы и элементы [1]. Это предполагает проведение точной количественной оценки опасности для сетевых атак, являющихся типовыми в АС ОВД, в соответствии с требованиями международных и отраслевых стандартов Российской Федерации, нормативных и методических документов ФСТЭК России и руководящих документов МВД России, посвященных во-

просам информационной безопасности АС [2—8]. Проведение точной количественной оценки опасности реализации сетевых атак требует, в свою очередь, научного осмысления процесса функционирования защищенных АС ОВД в условиях реализации атак и предполагает моделирование динамики их реализации в указанных системах [9, 10].

Анализ открытых литературных источников, посвященных данной проблеме, позволяет констатировать, что предлагаемые в большинстве из них формальные модели являются статическими, позволяющими проводить лишь качественную оценку опасности реализации сетевых атак, не обеспечивающую достаточную точность оценивания [11—15]. Немногочисленные научные труды, рассматривающие динамические модели злоумышленного удаленного доступа и предлагающие проводить количественную оценку опасности [16, 17], являются теоретически интересными, но недостаточно обеспечивающими практическую реализацию сетевых атак в современных АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД.

В данной статье предложена аналитическая модель, позволяющая осуществить точную количественную оценку вероятности реализации сетевой атаки и исследовать вероятностно-временные характеристики (ВВХ), описывающие динамику ее конфликтного взаимодействия с СЗИ от НСД в АС ОВД с учетом изначальных и потенциальных возможностей конфликтующих сторон. Полученные результаты могут быть использованы при оценивании опасности реализации сетевых атак в АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД.

**Теоретический анализ и его результаты.** Разработка аналитической модели и оценка вероятности реализации сетевой атаки в защищенных АС ОВД основаны на применении теории конечных полумарковских процессов (КПМП) к разработанным динамическим моделям реализации типовых сетевых атак [18] и обобщенной динамической модели информационного конфликта «Сетевая атака — СЗИ от НСД» в АС ОВД [19], построенным на сетях Петри—Маркова.

Представим модель динамики информационного конфликта «Сетевая атака — СЗИ от НСД» КПМП, в котором начало конфликтного взаимодействия соответствует входу КПМП в начальное состояние, а окончание — его входу в конечное состояние, являющееся поглощающим. Для описания динамики реализации сетевой атаки в ее конфликтном взаимодействии с СЗИ от НСД применяется подход, описанный в [20]. КПМП представим в виде ориентированного графа обобщенной модели динамики рассматриваемого информационного конфликта с мгновенными вероятностными переходами. При этом процесс мгновенных вероятностных переходов представляет собой вложенную цепь Маркова [21] (рис. 1).

На рисунке 1 состояния с номерами  $2n$  характеризуют выигрыш сетевой атаки, а с номерами  $(2n + 1)$  — выигрыш СЗИ от НСД ( $n = 1 \dots 3$ ). Поглощающие состояния 4 и 6 соответствуют завершению процесса реализации сетевой атаки, в результате которого осуществляется «взлом» СЗИ от НСД; поглощающие состояния 5 и 7 — завершению процесса функционирования СЗИ от НСД, в результате которого она успешно выполнила свои функции (защита АС ОВД).

В соответствии с теорией полумарковских процессов [22, 23] КПМП, моделирующий динамику информационного конфликта «Сетевая атака — СЗИ от НСД», может быть задан начальным распределением  $p = \{p_i, i \in I\}$ , матрицей переходных вероятностей вложенной цепи Маркова  $\{\pi_{ij}\}$ ,  $i, j \in I$  и матрицей функции распределения  $\{P_{ij}\}$ ,  $i, j \in I$  времени пребывания процесса в состоянии  $i$  при условии, что далее переход осуществляется в состояние  $j$ .

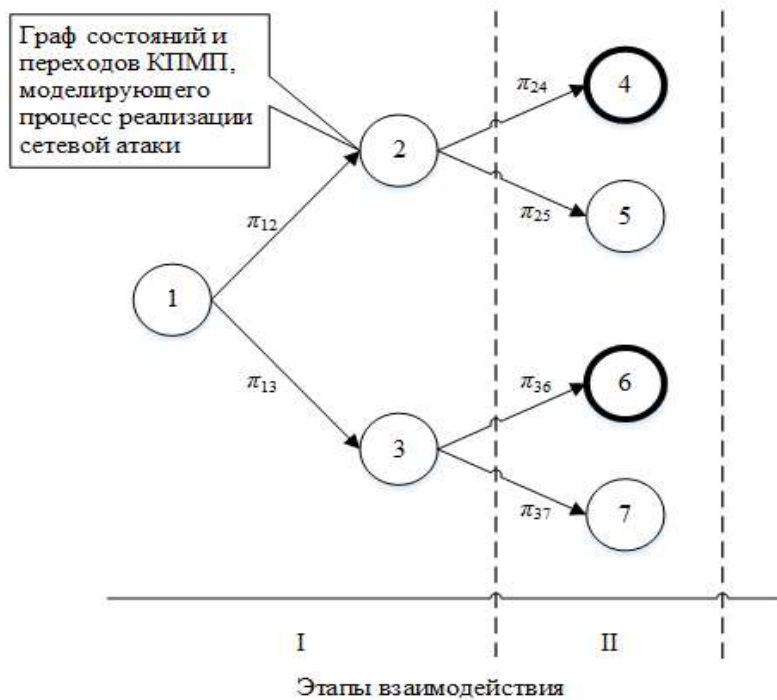


Рис. 1. Граф состояний и переходов КППП, моделирующего информационный конфликт «Сетевая атака — СЗИ от НСД»:

- 1 — производительности и объемы памяти сетевой атаки и СЗИ от НСД заданы;
- 2 — сетевая атака изначально имеет преимущество;
- 3 — СЗИ от НСД изначально имеет преимущество;
- 4, 6 — финальные состояния: «взлом» СЗИ от НСД, победа сетевой атаки;
- 5, 7 — финальные состояния: защита АС ОВД, победа СЗИ от НСД
- I этап — определение начальных условий конфликта (соотношения производительностей и объемов памяти сетевой атаки и СЗИ от НСД);
- II этап — протекание процесса конфликтного взаимодействия сетевой атаки и СЗИ от НСД

Анализ графа обобщенной модели динамики информационного конфликта «Сетевая атака — СЗИ от НСД» в АС ОВД позволил получить итоговую полумарковскую матрицу переходных вероятностей, представленную в таблице 1 [24].

Таблица 1 заполняется на основе значений, полученных в ходе решения уравнений

$$Q(\tau) = \{q_{ij}(\tau)\}, i, j \in I, \quad (1)$$

где элемент матрицы  $q_{ij}(\tau)$  определяет вероятности переходов соответствующего КППП из состояния  $i$  в состояние  $j$  за время, не превышающее среднее время  $\tau$  протекания информационного конфликта «Сетевая атака — СЗИ от НСД», и может быть рассчитан по формуле

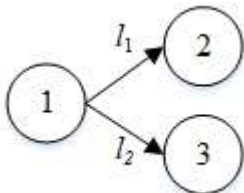
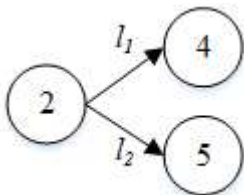
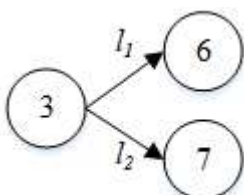
$$q_{ij}(\tau) = \pi_{ij}F_i(\tau), i, j \in I. \quad (2)$$

где:  $F_i(\tau)$  — функция распределения, равная вероятности перехода КППП из  $i$ -го состояния в другое состояние за время, не превышающее  $\tau$ ;

$\pi_{ij}$  — вероятности переходов КППП из  $i$ -го состояния в  $j$ -е состояние при условии нахождения КППП в состоянии  $i$  (данные вероятности не зависят от времени,  $\pi_{ij} \geq 0$ , для любого  $i$  выполняется условие  $\sum_{j \in J} \pi_{ij} = 1$ ).

Таблица 1

Расчет вероятностей переходов КППП, моделирующего динамику информационного конфликта «Сетевая атака — СЗИ от НСД» в АС ОВД

Графическое представление	Описание переходов	Расчет вероятностей
	$l_1$ — получение сетевой атакой изначального преимущества по производительности и объему памяти; $l_2$ — получение СЗИ от НСД изначального преимущества по производительности и объему памяти	$P(s_2) = P(s_1) \times P(s_2 s_1);$ $P(s_3) = P(s_1) \times P(s_3 s_1);$ $P(s_1) = P(s_2) + P(s_3)$
	$l_1$ — усиление сетевой атакой изначального имеющегося преимущества; финальное состояние: «взлом» СЗИ от НСД, победа сетевой атаки; $l_2$ — потеря сетевой атакой изначального имеющегося преимущества; финальное состояние: защита АС ОВД, победа СЗИ от НСД	$P(s_4) = P(s_2) \times P(s_4 s_2);$ $P(s_5) = P(s_2) \times P(s_5 s_2);$ $P(s_2) = P(s_4) + P(s_5)$
	$l_1$ — потеря СЗИ от НСД изначального имеющегося преимущества; финальное состояние: «взлом» СЗИ от НСД, победа сетевой атаки; $l_2$ — усиление СЗИ от НСД изначального имеющегося преимущества; финальное состояние: защита АС ОВД, победа СЗИ от НСД	$P(s_6) = P(s_3) \times P(s_6 s_3);$ $P(s_7) = P(s_3) \times P(s_7 s_3);$ $P(s_3) = P(s_6) + P(s_7)$
$P(s_1), P(s_2), P(s_3) = 1;$ $P(s_4) = P(s_2) \times P(s_4 s_2);$ $P(s_5) = P(s_2) \times P(s_5 s_2);$ $P(s_6) = P(s_3) \times P(s_6 s_3);$ $P(s_7) = P(s_3) \times P(s_7 s_3)$		

Функция распределения  $F_i(t)$  ( $i \in I$ ) определяется процедурой, характеризующей временные задержки переходов КППП, формализующего динамику реализации сетевой атаки в ее конфликтном взаимодействии с СЗИ от НСД, а вероятности переходов  $\pi_{ij}$  ( $i, j \in I$ ) характеризуются соответствующими разрешающими процедурами. При оценивании вероятности реализации сетевой атаки в защищенной АС ОВД законы распределения времени для функции  $F_i(t)$  полагаются нормальным (для описания действий по переходам, необходимым для определения преимущества одной из конфликтующих сторон) и экспоненциальным (для описания действий по оставшимся переходам КППП, в том числе характеризующим этапы реализации сетевой атаки) [25]. Однако ее параметры и переходные вероятности  $\pi_{ij}$  определяются предварительными показателями. Дальнейшее изменение их значений основывается на статистике, связанной с обработкой данных,

которые характеризуют вредоносные функции сетевой атаки и защитные функции СЗИ от НСД в процессе реализации атаки в защищенной АС ОВД.

Для определения вероятности реализации сетевой атаки и исследования ВВХ, характеризующих динамику ее конфликтного взаимодействия с СЗИ от НСД в АС ОВД, разрабатывается система интегро-дифференциальных уравнений (3, 4), которая далее сводится к системе линейных алгебраических уравнений, описывающих представленные в нижней части таблицы 1 полные вероятности переходов КППП из всех возможных состояний в конечное поглощающее состояние за время, не превышающее  $\tau$  [26, 27]:

$$P_{ij}(t) = \sum_{k \in I} \int_0^t q'_{ik}(t - \tau) \cdot P_{kj}(\tau) \cdot d\tau, \quad k, i, j \in I, t > 0, \quad (3)$$

где:  $P_{ij}(t)$  — вероятность достижения находящимся в  $i$ -м состоянии КППП состояния  $j$  за время, не превышающее  $\tau$ ;  $q'_{ik}(t - \tau)$  — производная от функции — элемента полумарковской матрицы, характеризующей временные задержки переходов КППП.

Обозначив через  $\pi_{in}\delta(t)$  вероятность того, что КППП останется в состоянии  $i$  до момента  $t$ , а затем за малый промежуток времени  $(t, t + \delta(t))$  перейдет в состояние  $j$  и с учетом (2) выражение (3) примет вид [24]

$$P_{ij}(t) = \pi_{in}\delta(t) + \sum_{k=1}^n \int_0^t \pi_{ik} \varphi_{ik}(t - \tau) \cdot P_{kj}(\tau) \cdot d\tau, \quad i = 1..n - 1; j = 2..n, \quad (4)$$

где:  $\varphi_{ik}(t - \tau) = F'_i(t - \tau)$  — плотность распределения вероятности (ПРВ) для случайной величины  $t$  (времени пребывания КППП в  $i$ -м состоянии при условии его последующего перехода в  $k$ -е состояние за время, не превышающее  $\tau$ );  $\delta(t) = 1$  при  $i = j$ ,  $\delta(t) = 0$  при  $i \neq j$ .

Для переходов, описывающихся экспоненциальным законом распределения времени, сведение системы интегро-дифференциальных уравнений к системе линейных алгебраических уравнений осуществляется путем применения к обеим частям уравнений (4) преобразования Лапласа по переменной  $t$  так, что функции-изображения будут зависеть от переменной  $s$ :

$$P_{ij}(s) = \pi_{in}\delta(s) + \sum_{k=1}^n \pi_{ik} \varphi_{ik}(s) \cdot P_{kj}(s), \quad i = 1..n - 1; j = 2..n. \quad (5)$$

Решение системы уравнений (5) относительно  $P_{ij}(s)$  с последующим получением  $P_{ij}(t)$  путем выполнения обратного преобразования Лапласа позволяет определить ВВХ реализации сетевой атаки:

$$P_{ij}(t) = L_{\tau}^{-1}[P_{ij}(s)]. \quad (6)$$

Для переходов, описывающихся нормальным законом распределения времени, решение системы интегро-дифференциальных уравнений (4) с применением преобразования Лапласа становится невозможным, поэтому для нахождения вероятностей соответствующих переходов целесообразно воспользоваться фильтрующим свойством  $\delta$ -функции Дирака [28]:

$$x(t) = \int_0^{+\infty} x(\tau) \delta(t - \tau) d\tau. \quad (7)$$

Считаем, что все переходы, необходимые для определения преимущества одной из конфликтующих сторон, описывающиеся нормальным законом распределения времени, имеют ПРВ вида

$$\varphi_{mk}(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(t-M)^2}{2\sigma^2}}, \quad (8)$$

где:  $M$ ,  $\sigma$  — математическое ожидание и среднее квадратичное отклонение случайной величины  $t$  (времени реализации сетевой атаки (функционирования СЗИ от НСД)), зависящей от производительностей, объемов памяти сетевой атаки и СЗИ от НСД ( $m = 1; k = 2, 3$ ).

Полагаем, что все действия по оставшимся переходам КППП, описывающиеся

экспоненциальным законом распределения, имеют ПРВ вида

$$\varphi_{ij}(t) = \lambda_{ij} e^{-\lambda_{ij} t}, \quad (9)$$

где:  $\lambda_{ij} = \frac{1}{\tau_{ij}}$ ,  $\tau_{ij}$  — средние времена соответствующих переходов ( $i = 2, 3; j = 4 \dots 7$ ).

С учетом вышеизложенного разрабатывается система интегро-дифференциальных уравнений для всех состояний КППП, моделирующего информационный конфликт «Сетевая атака — СЗИ от НСД» (рис. 1):

$$\begin{aligned} P_1(t) &= \pi_{1H} \delta(t); \\ P_2(t) &= \pi_{2H} \delta(t) + \int_0^t P_1(\tau) \varphi_{12}(t - \tau) \cdot \pi_{12} d\tau; \\ P_3(t) &= \pi_{3H} \delta(t) + \int_0^t P_1(\tau) \varphi_{13}(t - \tau) \cdot \pi_{13} d\tau; \\ P_4(t) &= \pi_{4H} \delta(t) + \int_0^t P_2(\tau) \varphi_{24}(t - \tau) \cdot \pi_{24} d\tau; \\ P_5(t) &= \pi_{5H} \delta(t) + \int_0^t P_2(\tau) \varphi_{25}(t - \tau) \cdot \pi_{25} d\tau; \\ P_6(t) &= \pi_{6H} \delta(t) + \int_0^t P_3(\tau) \varphi_{36}(t - \tau) \cdot \pi_{36} d\tau; \\ P_7(t) &= \pi_{7H} \delta(t) + \int_0^t P_3(\tau) \varphi_{37}(t - \tau) \cdot \pi_{37} d\tau. \end{aligned} \quad (10)$$

Для нахождения ПРВ  $\varphi_{ij}(t)$ , необходимых для решения системы уравнений (10) относительно  $P_j(t)$ , рассмотрим два выделенных этапа конфликтного взаимодействия сетевой атаки и СЗИ от НСД в соответствии с представленным графом (рис. 1).

I этап — определение начальных условий конфликта (соотношения производительностей и объемов памяти сетевой атаки и СЗИ от НСД).

Считаем, что моделируемый процесс из состояния 1 попадет в состояние 2 в случае наличия преимуществ сетевой атаки одновременно по двум исходным характеристикам (производительности и объему памяти) или при большем значении разности между соответствующими исходными характеристиками сетевой атаки и СЗИ от НСД. В противном случае моделируемый процесс окажется в состоянии 3.

Для переходов КППП из состояния 1 в состояния 2 и 3 ПРВ для конфликтующих сторон согласно формуле (8) определяются соотношениями:

$$\varphi_{tCA}(t) = \frac{1}{\sigma_{tCA} \sqrt{2\pi}} e^{-\frac{(t-M_{tCA})^2}{2\sigma_{tCA}^2}}; \quad (11)$$

$$\varphi_{tCЗИ}(t) = \frac{1}{\sigma_{tCЗИ} \sqrt{2\pi}} e^{-\frac{(t-M_{tCЗИ})^2}{2\sigma_{tCЗИ}^2}}. \quad (12)$$

Для каждой из представленных ПРВ вычисляется нормирующий множитель и рассчитываются нормированные ПРВ по формулам [29, 30]:

$$P_H^{CA} = \int_0^\infty \varphi_{tCA}(t) dt; \quad P_H^{CЗИ} = \int_0^\infty \varphi_{tCЗИ}(t) dt; \quad (13)$$

$$\varphi_{CA}^H(t) = \frac{\varphi_{tCA}(t)}{P_H^{CA}}; \quad \varphi_{CЗИ}^H(t) = \frac{\varphi_{tCЗИ}(t)}{P_H^{CЗИ}}. \quad (14)$$

Определяются условные нормированные ПРВ  $\varphi_{12}^*(t)$ ,  $\varphi_{13}^*(t)$  и переходные вероятности  $\pi_{12}$ ,  $\pi_{13}$ :

$$\varphi_{12}^*(t) = \varphi_{CA}^H(t) \left[ 1 - \int_0^t \varphi_{CЗИ}^H(\tau) d\tau \right]; \quad \varphi_{13}^*(t) = \varphi_{CЗИ}^H(t) \left[ 1 - \int_0^t \varphi_{CA}^H(\tau) d\tau \right]; \quad (15)$$

$$\pi_{12} = \int_0^\infty \varphi_{12}^*(t) dt; \quad \pi_{13} = \int_0^\infty \varphi_{13}^*(t) dt. \quad (16)$$

Тогда ПРВ  $\varphi_{12}(t)$  и  $\varphi_{13}(t)$  рассчитываются по формулам

$$\varphi_{12}(t) = \frac{\varphi_{12}^*(t)}{\pi_{12}}; \quad \varphi_{13}(t) = \frac{\varphi_{13}^*(t)}{\pi_{13}}. \quad (17)$$

Для нахождения вероятностей  $P_1(t)$ ,  $P_2(t)$  и  $P_3(t)$  воспользуемся фильтрующим свойством  $\delta$ -функции Дирака (7). В результате получим:

$$\begin{aligned} P_1(t) &= \delta(t); \\ P_2(t) &= \int_0^t \delta(\tau) \varphi_{12}^*(t - \tau) d\tau = \varphi_{12}^*(t); \\ P_3(t) &= \int_0^t \delta(\tau) \varphi_{13}^*(t - \tau) d\tau = \varphi_{13}^*(t). \end{aligned} \quad (18)$$

II этап — протекание процесса конфликтного взаимодействия сетевой атаки и СЗИ от НСД.

Для исследования ВВХ второго этапа информационного конфликта «Сетевая атака — СЗИ от НСД» необходимо воспользоваться результатами моделирования механизма реализации типовых сетевых атак, воздействующих на информационные ресурсы и элементы АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД [18]. С целью проведения данного моделирования рассмотренный выше математический аппарат (формулы (4) и (5)) применяется к процессу реализации каждой из восьми типовых сетевых атак. Для решения полученной системы линейных алгебраических уравнений (5) и нахождения преобразования Лапласа вероятности достижения конечного состояния  $P_{ij}(s)$  для каждой модели сетевой атаки строится ее динамическая структура в виде передаточных функций  $F_{ij}(s) = \pi_{ij} \varphi_{ij}(s) = L_s\{\pi_{ij} \varphi_{ij}(t)\}$ . При этом  $P_{ij}(s)$  характеризуется суммой произведений передаточных функций всех ветвей от исходных до ветви, содержащей искомое конечное состояние  $j$ .

Рассчитаем  $P_{ij}(s)$  на примере атаки «Сканирование сети» (рис. 2).

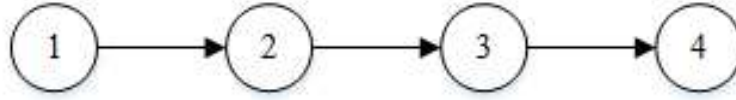


Рис. 2. Граф КППП, описывающий механизм реализации атаки «Сканирование сети»

Для каждого этапа реализации рассматриваемой сетевой атаки записываются выражения для определения вероятностей перехода КППП в соответствующие состояния согласно формуле (4):

$$\begin{aligned} P_1(t) &= -\pi_{1H} \delta(t); 0 \\ P_2(t) &= \pi_{2H} \delta(t) + \int_0^t P_1(\tau) \varphi_{12}(t - \tau) \cdot \pi_{12} d\tau; \\ P_3(t) &= \pi_{3H} \delta(t) + \int_0^t P_2(\tau) \varphi_{23}(t - \tau) \cdot \pi_{23} d\tau; \\ P_4(t) &= \pi_{4H} \delta(t) + \int_0^t P_3(\tau) \varphi_{34}(t - \tau) \cdot \pi_{34} d\tau. \end{aligned}$$

После применения преобразования Лапласа по формуле (5) получаем:

$$\begin{aligned} P_1(s) &= \pi_{1H}; \\ P_2(s) &= P_1(s) \varphi_{12}(s) \pi_{12}; \\ P_3(s) &= P_2(s) \varphi_{23}(s) \pi_{23}; \end{aligned}$$

$$P_4(s) = P_3(s)\varphi_{34}(s) \pi_{34};$$

$$\pi_{12} = \pi_{23} = \pi_{34} = 1.$$

Динамическая структура рассматриваемой атаки в виде передаточных функций имеет вид

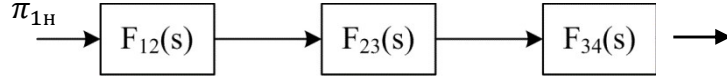


Рис. 3. Динамическая структура атаки «Сканирование сети»

Преобразование Лапласа вероятности достижения КППП конечного состояния  $P_4(s)$  определится из соотношения

$$P_4(s) = \pi_{1n}F_{12}(s) \cdot F_{23}(s) \cdot F_{34}(s).$$

Ниже представлены результаты расчета  $P_{ij}(s)$  для остальных семи типовых сетевых атак.

– «Анализ сетевого трафика» (сниффинг пакетов):

$$P_4(s) = F_{34}(s)(\pi_{1n}F_{13}(s) + \pi_{2n}F_{23}(s));$$

– «Парольная»:

$$P_5(s) = \pi_{1n}[F_{12}(s)\pi_{12} \cdot F_{25}(s) + F_{13}(s)\pi_{13} \cdot F_{34}(s) \cdot F_{45}(s)\pi_{45}];$$

$$P_6(s) = \pi_{1n}F_{13}(s)\pi_{13} \cdot F_{34}(s) \cdot F_{46}(s)\pi_{46};$$

– «Подмена доверенного объекта сети» (IP-spoofing):

$$P_{10}(s) = F_{910}(s)[F_{34}(s) \cdot F_{45}(s) \cdot F_{56}(s) \cdot F_{69}(s) \cdot (\pi_{1n}F_{13}(s) + \pi_{2n}F_{23}(s)) + \\ + \pi_{7n}F_{78}(s) \cdot F_{89}(s)];$$

– «Навязывание ложного маршрута»:

$$P_6(s) = F_{45}(s) \cdot F_{56}(s)[\pi_{1n}F_{14}(s) + \pi_{2n}F_{23}(s) \cdot F_{34}(s)];$$

– «Внедрение ложного объекта сети» (ARP-spoofing):

$$P_6(s) = F_{45}(s) \cdot F_{56}(s)[\pi_{1n}F_{14}(s) + \pi_{2n}F_{23}(s) \cdot F_{34}(s)];$$

– «Отказ в обслуживании» (SYN-flood):

$$P_5(s) = F_{45}(s)[\pi_{1n}F_{13}(s) \cdot F_{34}(s) + \pi_{2n} \cdot F_{24}(s)];$$

– «Удаленный запуск приложений» (IP-hijacking):

$$P_8(s) = F_{34}(s) \cdot F_{45}(s) \cdot F_{56}(s) \cdot F_{67}(s) \cdot F_{78}(s)[\pi_{1n}F_{13}(s) + \pi_{2n} \cdot F_{23}(s)].$$

Поскольку вероятность распределения времени реализации сетевой атаки определяется ПРВ времени нахождения моделирующего ее КППП в конечном (поглощающем) состоянии, то соответствующие ПРВ для каждой из рассмотренных типовых сетевых атак можно определить по формуле (6):

$$\varphi_{\text{сз}}^m(t) = L_{\tau}^{-1}[P_n^m(s)], \quad (19)$$

где:  $m$  — тип сетевой атаки;  $n$  — номер поглощающего состояния  $n$ -й сетевой атаки.

ПРВ времени функционирования СЗИ от НСД, рассчитываемая по формуле (9), имеет вид

$$\varphi_{\text{сзи}}(t) = \lambda e^{-\lambda t}, \quad (20)$$



где:  $\lambda = \frac{1}{\tau_{\text{сзи}}}$ ,  $\tau_{\text{сзи}}$  — среднее время функционирования СЗИ от НСД.

Полагаем, что условная нормированная ПРВ времени функционирования СЗИ от НСД не зависит от того, в каком из состояний графовой модели (2 или 3) находится моделируемый процесс. Тогда условные ПРВ  $\varphi_{24}^*(t)$ ,  $\varphi_{25}^*(t)$ ,  $\varphi_{36}^*(t)$ ,  $\varphi_{37}^*(t)$  и переходные вероятности  $\pi_{24}$ ,  $\pi_{25}$ ,  $\pi_{36}$ ,  $\pi_{37}$  определяются из соотношений

$$\begin{aligned}\varphi_{24}^*(t) &= \varphi_{\text{сзи}}^m(t) \left[ 1 - \int_0^t \varphi_{\text{сзи}}(\tau) d\tau \right]; \quad \varphi_{25}^*(t) = \varphi_{\text{сзи}}(t) \left[ 1 - \int_0^t \varphi_{\text{сзи}}^m(\tau) d\tau \right]; \\ \varphi_{36}^*(t) &= \varphi_{\text{сзи}}^m(t) \left[ 1 - \int_0^t \varphi_{\text{сзи}}(\tau) d\tau \right]; \quad \varphi_{37}^*(t) = \varphi_{\text{сзи}}(t) \left[ 1 - \int_0^t \varphi_{\text{сзи}}^m(\tau) d\tau \right]; \\ \pi_{24} &= \int_0^\infty \varphi_{24}^*(t) dt; \quad \pi_{25} = \int_0^\infty \varphi_{25}^*(t) dt; \quad \pi_{36} = \int_0^\infty \varphi_{36}^*(t) dt; \quad \pi_{37} = \int_0^\infty \varphi_{37}^*(t) dt.\end{aligned}\quad (21)$$

В результате входящие в систему уравнений (10) ПРВ  $\varphi_{24}(t)$ ,  $\varphi_{25}(t)$ ,  $\varphi_{36}(t)$ ,  $\varphi_{37}(t)$  рассчитываются по формулам

$$\varphi_{24}(t) = \frac{\varphi_{24}^*(t)}{\pi_{24}}; \quad \varphi_{25}(t) = \frac{\varphi_{25}^*(t)}{\pi_{25}}; \quad \varphi_{36}(t) = \frac{\varphi_{36}^*(t)}{\pi_{36}}; \quad \varphi_{37}(t) = \frac{\varphi_{37}^*(t)}{\pi_{37}}. \quad (22)$$

Учитывая, что в системе уравнений (10)  $\delta(t) = 1$  при вычислении  $P_1(t)$  и  $\delta(t) = 0$  при расчете остальных вероятностей  $P_2(t) \dots P_7(t)$ , вероятность полной реализации сетевой атаки («взлома» СЗИ от НСД, победы сетевой атаки) и вероятность полного выполнения защитных функций СЗИ от НСД (защиты АС ОВД, победы СЗИ от НСД) определяются в виде сумм вероятностей нахождения КППП в соответствующих поглощающих состояниях:

$$P_{\text{сзи}}(t) = P_4(t) + P_6(t) = \int_0^t P_2(\tau) \varphi_{24}(t - \tau) \cdot \pi_{24} d\tau + \int_0^t P_3(\tau) \varphi_{36}(t - \tau) \cdot \pi_{36} d\tau; \quad (23)$$

$$P_{\text{сзи}}(t) = P_5(t) + P_7(t) = \int_0^t P_2(\tau) \varphi_{25}(t - \tau) \cdot \pi_{25} d\tau + \int_0^t P_3(\tau) \varphi_{37}(t - \tau) \cdot \pi_{37} d\tau. \quad (24)$$

**Заключение.** Таким образом, в статье разработана аналитическая модель, позволяющая провести точную количественную оценку вероятности реализации сетевых атак и исследовать их ВВХ, характеризующие динамику взаимодействия с системой защиты в информационном конфликте «Сетевая атака — СЗИ от НСД» в процессе эксплуатации защищенных АС на объектах информатизации ОВД. Точность оценки обеспечивается учетом изначальных и потенциальных возможностей конфликтующих сторон, а также всех возможных переходов между состояниями рассматриваемого информационного конфликта в интегро-дифференциальных уравнениях (10). Адекватность полученных результатов обеспечивается проведением расчетов для конкретных сетевых атак, являющихся типовыми в АС ОВД. Использование предложенной модели совместно с аналитической моделью расчета размеров ущерба от реализации атак в течение времени их действия в системе позволит количественно оценить опасность реализации сетевых атак в защищенных АС ОВД, обеспечивая точность и адекватность оценки. Перспективы использования полученных результатов связаны с выявлением наиболее опасных сетевых атак и разработкой частной модели актуальных атак для конкретной АС ОВД.

## ЛИТЕРАТУРА

1. Concept for increasing security of national information technology infrastructure and private clouds / D. A. Melnikov, A. P. Durakovsky, S. V. Dvoryankin, V. S. Gorbatov // Proceedings — 2017 IEEE 5th International Conference on Future Internet of Things and

Cloud, FiCloud 2017 : 5. — Prague, 2017. — P. 155—160. DOI 10.1109/FiCloud.2017.11. doi: 10.1109/FiCloud.2017.11

2. ГОСТР ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2 : Функциональные компоненты безопасности [Электронный ресурс]. — URL: <http://docs.cntd.ru/document/1200105710> (дата обращения: 18.10.2019).

3. ГОСТ 34.003-90. Автоматизированные системы. Термины и определения [Электронный ресурс]. — URL: <http://docs.cntd.ru/document/1200006979> — (дата обращения: 10.10.2019).

4. ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении [Электронный ресурс]. — URL: <http://docs.cntd.ru/document/1200108858> (дата обращения: 11.10.2019).

5. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsdatelya-gostekhkommisii-rossii-ot-30-marta-1992-g> (дата обращения: 14.10.2019).

6. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [Электронный ресурс]. — URL: <http://fstec.ru/component/attachments/download/299> (дата обращения: 18.10.2019).

7. ФСТЭК России. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 5 февраля 2021 г.) [Электронный ресурс]. — URL: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhdzen-fstek-rossii-5-fevralya-2021> (дата обращения: 27.02.2021).

8. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года : приказ МВД России от 14.03.2012 № 169 [Электронный ресурс]. — URL: <http://policemagazine.ru/forum/showthread.php?t=3663> (дата обращения: 21.10.2019).

9. Butusov I. V., Romanov A. A. Methodology of Security Assessment Automated Systems as Objects Critical Information Infrastructure [Электронный ресурс]. — URL: [http://fcyberrus.com/wp-content/uploads/2018/05/02-10-125-18\\_1.-Butusov.pdf](http://fcyberrus.com/wp-content/uploads/2018/05/02-10-125-18_1.-Butusov.pdf) (дата обращения: 27.05.2021).

10. Kalashnikov A., Sakrutina E. Towards risk potential of significant plants of critical information infrastructure // International Russian Automation Conference, RusAutoCon 2018. — Sochi, 2018. — P. 8501644. — DOI 10.1109/RUSAUTOCON.2018.8501644.

11. Дровникова И. Г., Овчинникова Е. С., Рогозин Е. А. Анализ существующих способов и процедур оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел и аспекты их совершенствования // Вестник Воронежского института МВД России. — 2019. — № 4. — С. 51—63.

12. Sher A. Simulation of Attacks in a Wireless Sensor Network using NS2 // The School of Engineering & Computing Sciences. — Texas : A&M University-Corpus Christi, 2015. — 49 p.

13. Yao Y. Automated Crowdturfing Attacks and Defenses in Online Review Systems / Eds. B. Viswanath, J. Cruan, H. Zheng, B. Y. Zhao // arXiv:1708.08151v2 [cs.CR]. 8 Sep., 2017. 16 p. [Электронный ресурс]. — URL: <https://docviewer.yandex.ru/view/0/> — (дата обращения: 27.05.2021).

14. Kresimir S., Hrvoje O., Marin G. The information systems' security level assessment model based on an ontology and evidential reasoning approach // *Computers & Security*. — 2015. — P. 100—112.
15. Lan Y. Effectiveness Evaluation on Cyberspace Security Defense System / Eds. S-P. Liu, L. Lin, Y-Y. Ma // *International Conference on Network and Information Systems for Computers (IEEE Conference Publications)*. — 2015. — P. 576—579.
16. Радько Н. М., Скобелев И. О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. — М. : РадиоСофт, 2010. — 232 с.
17. Радько Н. М., Язов Ю. К., Корнеева Н. Н. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа. — Воронеж : Воронеж. госуд. технич. ун-т, 2013. — 265 с.
18. Innovative technology in the research of implementation dynamics of network attacks on the digital educational resources / O. I. Bokova, I. G. Drovnikova, E. S. Ovchinnikova, S. V. Rodin // *ASEDU-2020: 1st International Conference on Advances in Science, Engineering and Digital Education [Электронный ресурс]*. — IOP Conf. Series: Journal of Physics: Conf. Series 1691 (2020) 012063 IOP Publishing doi:10.1088/1742-6596/1691/1/012063
19. Моделирование динамики информационного конфликта в защищенных автоматизированных системах органов внутренних дел на основе сети Петри—Маркова / И. Г. Дровникова, Е. С. Овчинникова, Е. А. Рогозин, А. В. Калач // *Вестник Воронежского института ФСИН России*. — 2020. — № 4. — С. 37—44.
20. Соломатин М. С., Рогозин Е. А., Дровникова И. Г. Создание модели информационного конфликта «нарушитель — система защиты» на основе сети Петри—Маркова // *Вестник Воронежского института МВД России*. — 2019. — № 2. — С. 93—100.
21. Кендалл Д. Стохастические процессы, встречающиеся в теории очередей, и их анализ методом вложенных цепей Маркова. // *Математика*. — 1959. — Т. 3. — № 6. — С. 97—111.
22. Сильвестров Д. С. Полумарковские процессы с дискретным множеством состояний. — М. : Сов. радио, 1980. — 272 с.
23. Корольок В. С., Турбин А. Ф. Полумарковские процессы и их приложения. — Киев : Наукова думка, 1976. — 184 с.
24. Мерзлова Е. Ю. Об оптимальной управлении полумарковскими процессами двумя игроками с противоречивыми интересами : дис. ... канд. физ.-мат. наук : 01.01.05 / Мерзлова Елена Юрьевна. — М., 2006. — 156 с.
25. Дровникова И. Г., Овчинникова Е. С. Обоснование распределения времени реализации сетевых атак в автоматизированных системах органов внутренних дел на основе проведения натурного эксперимента // *Безопасность информационных технологий = IT Security*. — Т. 28ю. — № 3 (2021). — С. 23—38.
26. Бартоломью Д. Стохастические модели социальных процессов / пер. с англ. под ред. О. В. Старовойта. — М. : Финансы и статистика, 1985. — 295 с. — (Математико-статистические методы за рубежом).
27. Язов Ю. К., Анищенко А. В. Сети Петри—Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах : монография. — Воронеж : Кварта, 2020. — 173 с.
28. Дирак П. А. М. Принципы квантовой механики. — М. : Наука, 1979. — 480 с.
29. Владимиров В. И., Владимиров И. В. Основы оценки конфликтно-устойчивых состояний организационно-технических систем (в информационных конфликтах). — Воронеж : ВАИУ, 2008. — 231 с.
30. Керков В. Г. Методические особенности нестационарности конфликта при описании его динамики полумарковским процессом // *Вестник ВГТУ*. — 2010. — Т. 6. — № 9. — С. 124—127.

