

И.Г. ДРОВНИКОВА, Т.В. МЕЩЕРЯКОВА, А.Д. ПОПОВ, Е.А. РОГОЗИН,
С.М. СИТНИК

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ПРЕОБРАЗОВАНИЯ ЛАПЛАСА И ЧИСЛЕННОГО МЕТОДА ГИВЕНСА

Дровникова И.Г., Мещерякова Т.В., Попов А.Д., Рогозин Е.А., Ситник С.М.
Математическая модель оценки эффективности систем защиты информации с использованием преобразования Лапласа и численного метода Гивенса.

Аннотация. В статье представлена динамическая модель функционирования системы защиты информации (СЗИ) от несанкционированного доступа (НСД) в автоматизированных информационных системах (АИС), созданная на основе аппарата сетей Петри. Разработана математическая модель оценки динамического показателя эффективности функционирования СЗИ от НСД в АИС на основе использования операционного метода преобразования Лапласа и численного метода решения системы линейных алгебраических уравнений (СЛАУ) методом Гивенса (методом вращения). Представлен алгоритм расчета динамического показателя эффективности СЗИ от НСД в АИС с учетом выбранного метода решения СЛАУ, который в дальнейшем может быть использован при разработке комплекса программ анализа, моделирования и оценки динамического показателя эффективности СЗИ от НСД в АИС. Выбор и разработка показателя эффективности функционирования СЗИ от НСД в АИС в данной статье осуществлялся на основе анализа ГОСТ 28195-89.

Ключевые слова: система защиты информации, автоматизированная информационная система, несанкционированный доступ, конечный марковский процесс, эффективность, сеть Петри.

1. Введение. Современные тенденции развития вычислительных систем характеризуются постоянным усложнением структуры, добавлением различных механизмов, созданием новых версий систем. СЗИ от НСД в АИС не являются исключением. Сложный характер взаимодействия компонентов рассматриваемой системы послужил толчком к появлению новых задач, связанных с моделированием динамики функционирования, анализом, описанием причинно-следственных связей объектов при проектировании СЗИ от НСД в АИС [1, 2]. Адекватным инструментом для решения подобных задач являются сети Петри.

Анализ [3, 4] позволил выявить положительные особенности использования сетей Петри при моделировании сложных систем, к которым, несомненно, можно отнести СЗИ от НСД:

- сети Петри удобны для моделирования параллельных процессов;
- с их помощью можно представить моделируемый объект;
- они позволяют исследовать моделируемый объект в динамике его функционирования;
- с их помощью можно программировать моделируемые процессы.

Моделирование процесса функционирования СЗИ от НСД в АИС на основе аппарата сетей Петри планируется использовать для разработки математической модели анализа и оценки динамического показателя эффективности этих систем [1].

СЗИ от НСД — сложная организационно-программная система, которая представляет собой часть комплекса мероприятий, направленных на защиту информации (ЗИ) в АИС от НСД. Целью создания СЗИ от НСД при разработке АИС в защищенном исполнении является обеспечение ЗИ от незаконного доступа к информационному ресурсу (уничтожения, модификации, блокирования, копирования и иных действий, ведущих к нарушению функционирования АИС в целом) [1].

Анализ нормативной документации, регламентирующей ЗИ от НСД, позволил выделить основные этапы и задачи разработки СЗИ от НСД в АИС [1, 5-11]. Представленный алгоритм был оптимизирован и доработан, в частности, в него был включен новый этап разработки, позволяющий количественно оценить динамический показатель эффективности СЗИ от НСД в АИС, что позволит провести исследование процесса функционирования СЗИ от НСД в динамическом (временном) режиме. Требования к оценке эффективности СЗИ от НСД прописаны в ряде нормативных документов [1, 5-10], но до настоящего времени решение данной проблемы не найдено, так как:

- существующая методика количественной оценки СЗИ от НСД в АИС в соответствии с нормативной базой разработана не в полной мере;
- не реализован комплексный подход к решению задачи количественной оценки СЗИ от НСД в АИС;
- не разработан комплекс программ анализа и количественной оценки при проектировании СЗИ от НСД в АИС.

В этой связи в [1] были осуществлены следующие исследования:

- разработаны основные этапы и задачи проектирования СЗИ от НСД в АИС;
- создана вербальная (описательная) модель СЗИ от НСД в АИС [2];
- разработана графовая модель процесса функционирования СЗИ от НСД в АИС с конечным числом состояний [2];
- разработана динамическая модель функционирования защитных механизмов СЗИ от НСД в АИС на основе аппарата сетей Петри. Динамика представлена при помощи графа разметок.

Следующий этап исследования заключается в построении формализованной модели использования СЗИ от НСД в АИС. Для этого воспользуемся описанием процесса применения этих систем в виде марковского случайного процесса, а именно марковской цепи с конеч-

ным числом состояний — конечный марковский процесс (КМП), в котором обращение к СЗИ от НСД соответствует входу в начальное состояние, а завершение выполнения своих защитных функций по данному обращению — входу в конечное состояние.

Система взглядов российских ученых, относительно поднятой проблемы, выражается в наиболее значимых нормативных актах по информационной безопасности (ИБ), ими являются руководящие документы (РД) Федеральной службы по техническому и экспортному контролю (ФСТЭК) [8-10], в соответствии с которыми при сертификации СЗИ от НСД АИС на основе класса защищенности данные документы определяют функциональный состав рассматриваемых систем. В тоже время в документе ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» в п. 3.б. сказано, что при эксплуатации защищенных АИС необходимо проводить оценку их эффективности, которая должна включать в себя соответствующие математические модели и алгоритмы. Данный пункт проработан недостаточным образом и требует углубленного научного исследования. Таким образом, оценка эффективности СЗИ от НСД в АИС сводится к определению их функционального состава, что представляется нам неполным с точки зрения функционирования в динамическом (временном) диапазоне. Это является существенным недостатком существующей методики оценки эффективности в соответствии с нормативными документами ФСТЭК.

Система взглядов иностранных ученых на проблему, связанную с повышением защищенности разрабатываемых и существующих АИС отражены в соответствующих стандартах [12-16], например «Критерии оценки безопасности информационных технологий» [15-16], которые были разработаны в США. Цель данного стандарта состоит в определении требований безопасности, предъявляемых к программному и специальному обеспечению АИС, а именно для формирования профиля защиты. К перечисленным видам обеспечения АИС можно также отнести исследуемую СЗИ от НСД. В этом документе введено такое понятие, как критерий адекватности или адекватность, которое связано непосредственно с реализацией систем и средств ЗИ от НСД и политикой безопасности защищенных АИС в целом. Соответствующий нормативный акт ограничивается формальными требованиями, связанными с поддержанием работоспособности СЗИ от НСД. А эффективность определяется соотношением между задачами перед СЗИ от НСД и реализованным набором функций защиты, то есть способ оценки эффективности в иностранных документах схож со способом, указанным в РД ФСТЭК России. Вышеуказанное позволяет сделать вывод, что воз-

ника настоящая целесообразность в разработке комплексной методики оценки эффективности СЗИ от НСД в АИС.

2. Теоретический анализ. В статье в качестве объекта исследования будем использовать типовую СЗИ от НСД в АИС.

Разработка аппарата на основе сетей Петри послужит решению проблем, возникающих при проектировании СЗИ от НСД в АИС [1], а именно:

- проанализировать выполняемые системой функции на предмет их наличия и связей согласно техническому заданию;
- определить, насколько эффективно функционирует система с точки зрения причинно-следственных связей и других логических структур построения;
- определить узкие места, из-за которых могут возникать ошибки в работе системы.

Компоненты СЗИ от НСД в АИС представляют собой множество событий (далее переходы). Событие есть конкретная функция, которая выполняется системой при определенных условиях. Условия (далее позиции) — это действия пользователя в системе, при которых событие будет выполняться.

Обозначим сеть Петри как $C_{СЗИ} = (P, T, I, O, W)$, она определяется позициями, переходами, входными и выходными функциями, где $P = \{p_1, p_2, \dots, p_n\}$ — множество позиций, $T = \{t_1, t_2, \dots, t_m\}$ — множество переходов $n \geq 0, m \geq 0$, I и O — входная и выходная функция соответственно. Количества n и m являются мощностями множеств P и T . Произвольные элементы множества P обозначим как p_i , где $i = 1, \dots, n$, а элементы множества T — как t_j , где $j = 1, \dots, m$; W — кратность дуг.

Графическим представлением сети Петри является двудольный ориентированный граф. Это можно объяснить тем, что все вершины графа Петри делятся на два множества, множество переходов и множество позиций таким образом, что каждая дуга направленно соединяет элементы одного множества с другим. Из этого следует, что графическое представление сети Петри состоит из позиций — кружков, переходов — планок, входных и выходных функций, изображаемых как стрелки, которые представляются дугами.

Граф сети Петри представим как $G = (H, R)$, где $H = (h_1, h_2, \dots, h_z)$ — множество вершин, а $R = \{x_1, x_2, \dots, x_u\}$ — комплект направленных дуг. Множество позиций H можно разбить на

два подмножества — позиций P и переходов T , которые не пересекаются так, что $H = P \cup T, P \cap T = \emptyset$. В сети должна присутствовать хотя бы одна дуга $R \neq \emptyset$. Автономное расположения позиций и переходов не является допустимым в сети Петри.

Динамика функционирования сети Петри обеспечивается при помощи маркеров (фишек), которые обозначим как M , графически представляются точками внутри позиций. Неформально динамику функционирования сети Петри можно представить как совокупность локальных действий пользователя, работающего с СЗИ от НСД в АИС, которые называются срабатываниями переходов (рисунок 1).

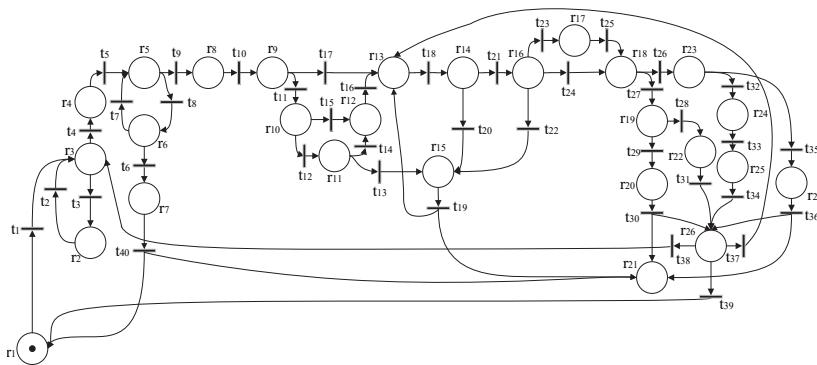


Рис. 1. Начальная разметка сети Петри типовой СЗИ от НСД в АИС

Переход в разработанной сети Петри в соответствии с [2, 4] считается возбужденным или активированным, если в каждой его входной позиции имеются маркеры, количество которых не менее кратности соответствующих дуг. Переход может сработать, если выполнены все условия реализации события, то есть входные позиции должны содержать хотя бы одну фишку. При срабатывании перехода меняется состояние моделируемой системы, что в конкретном примере будет характеризоваться работой пользователя в системе.

Матрица инцидентности к сети Петри, изображенной на рисунке 1, задается с помощью двух таблиц. Они указывают на связи между инцидентными вершинами $(t_1 - t_{40})$ множеств $P = (r_1 - r_{27})$ и $T = (t_1 - t_{40})$, где $(r_1 - r_{27})$ — все позиции, а $(t_1 - t_{40})$ — все переходы графа сети Петри [4, 5].

3. Динамическая модель функционирования типовой СЗИ от НСД на основе сетей Петри. Динамику функционирования механизмов защиты при определенных действиях пользователя в СЗИ от НСД в АИС возможно описать при помощи маркировки сети Петри в результате срабатывания ее переходов. Представим данную динамику в виде графа разметок ориентированного графа G , который показывает срабатывания каждого состояния исследуемой системы. Переходы t_i в данном графе представим в виде дуг. Разметку представим в виде последовательности цифр, описывающих положение маркеров в позиции при срабатывании того или иного перехода, m_i — количество маркеров, а индексы используются для компактного представления, как, например, при $r_{общ} = 27$ для графа $G(m_{1-25}, m_{2-26}, m_{3-27})$. Начальная разметка графа $G(1, 0_2, 0_{3-27})$ представлена на рисунке 2.

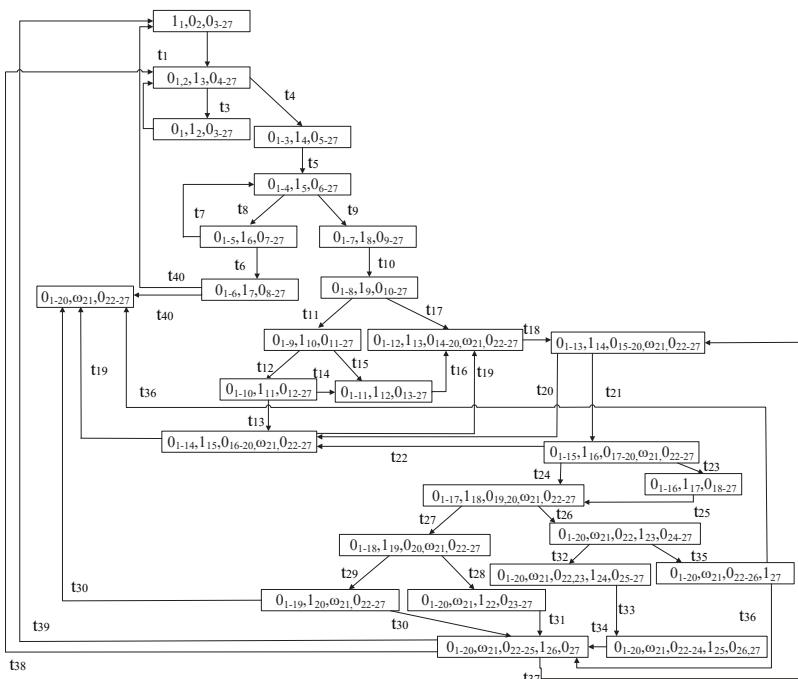


Рис. 2. Граф разметок сети Петри типовой СЗИ от НСД в АИС

В позиции r_{21} возможно накопление неограниченного количества маркеров, так как она имитирует собой журнал регистрации событий НСД в СЗИ. Соответственно, при повторном прохождении по графу разметка графа G в позиции r_{21} будет с символом ω — это количество маркеров, которое характеризует объем записей в журнале событий СЗИ от НСД. Журнал событий является настраиваемым, то есть администратор может установить объем, при котором он автоматически сохраняется в памяти компьютера с дальнейшей его очисткой в СЗИ.

Условия запуска перехода T сети Петри: $\forall P \in T_{ex} M_P \geq W_{P,T}$.

Запуск перехода сети Петри: $\forall P \in T_{ex} M_P = M_P - W_{P,T}$,
 $\forall P \in T_{вых} M_P = M_P + W_{P,T}$.

Граф разметок на рисунке 2 будет являться конечным, потому что действия пользователя с АИС завершаться в конкретно его рабочий день.

Проведем анализ основных свойств сети Петри, представленной на рисунке 1 и рисунке 2 [3, 4]: неограниченность; безопасность; сохраняемость; активность; достижимость; покрываемость; эквивалентность.

Чтобы сделать конкретные выводы по работе защитных механизмов типовой СЗИ от НСД, охарактеризуем полученную сеть Петри.

Граф сети Петри является:

- неограниченным, так как количество фишек при проходе по графу изменчиво, то есть не является постоянной величиной;
- небезопасным, так как число фишек в каждой позиции может превышать 1.

На основе выявленных свойств графа выделим ключевые особенности моделируемой СЗИ от НСД:

– динамика функционирования исследуемой системы определяется неограниченностью, небезопасностью и несохраняемостью графа сети Петри. Можно сказать, что динамика обосновывается распараллеливанием процессов защитных механизмов, учетом несанкционированных действий в буфере программы. При проектировании подобных систем немаловажным фактором является оперативность реагирования на НСД;

– на рисунках 1 и 2 видно, что все переходы могут сработать, и в соответствии с этим можно сделать вывод, что структурно-логические связи механизмов защиты построены корректно;

– логику причинно-следственных связей отследим, основываясь на рисунках 1 и 2 [2]. Видно, что каждый компонент при определенных условиях может функционировать, взаимосвязи между ними корректны;

– «уязвимые места» есть фактически в каждом компоненте СЗИ от НСД, вопрос в том, в какой степени он будет являться дальнейшим направлением исследования.

Построим имитационную модель сети Петри, которая моделирует действия пользователя в СЗИ от НСД АИС ОВД при помощи программы CPN Tools. CPN Tools — это моделирующая система, которая описывает модели при помощи языка сетей Петри. Представим разработанную выше модель в данной программе рисунок 3.

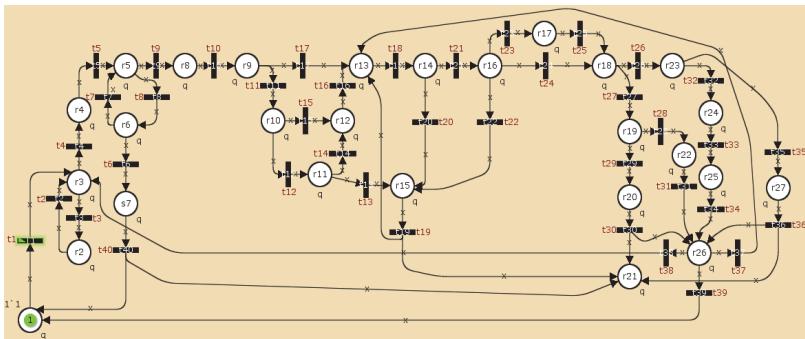


Рис. 3. Сети Петри СЗИ от НСД в АИС построенная при помощи CPN Tools

В таблице 1 собрана статистика попадания маркера во все позиции сети Петри, проход по которому был совершен 100000 раз.

Таблица 1 имеет следующие поля: Name — имя позиции; Count — счетчик проходов по графу начиная с 0; Sum — суммарное количество попадания маркера в конкретную позицию; Avg — среднее значение, но в контексте данной имитационной задачи, так как маркер в сети один, будет являться вероятностью попадания маркера в позицию; Min — минимальное количество маркеров в позиции; Max — максимальное количество маркеров в позиции. Следует отметить, что позиция r_{21} является журналом регистрации событий НСД, поэтому мы наблюдаем большое количество маркеров по окончанию моделирования, особенность в работе можете увидеть на рисунках выше. Сумма значений в поле Avg исключая позицию r_{21} будет являться единицей, что свидетельствует о правильности расчета.

Таблица 1. Статистика попадания маркера в позиции сети Петри

Untimed statistics					
Name	Count	Sum	Avrg	Min	Max
r_1	100001	2907	0.029070	0	1
r_2	100001	4336	0.043360	0	1
r_3	100001	8651	0.086509	0	1
r_4	100001	4315	0.043150	0	1
r_5	100001	5834	0.058339	0	1
r_6	100001	2983	0.029830	0	1
r_7	100001	1464	0.014640	0	1
r_8	100001	2850	0.028500	0	1
r_9	100001	2850	0.028500	0	1
r_{10}	100001	1428	0.014280	0	1
r_{11}	100001	715	0.007150	0	1
r_{12}	100001	1090	0.010900	0	1
r_{13}	100001	12608	0.126079	0	1
r_{14}	100001	12608	0.126079	0	1
r_{15}	100001	8668	0.086679	0	1
r_{16}	100001	6330	0.063299	0	1
r_{17}	100001	2160	0.021600	0	1
r_{18}	100001	4278	0.042780	0	1
r_{19}	100001	2117	0.021170	0	1
r_{20}	100001	1038	0.010380	0	1
r_{21}	100001	611471569	6114.654543	0	12239
r_{22}	100001	1079	0.010790	0	1
r_{23}	100001	2161	0.021610	0	1
r_{24}	100001	1092	0.010920	0	1
r_{25}	100001	1092	0.010920	0	1
r_{26}	100001	4278	0.042780	0	1
r_{27}	100001	1069	0.010690	0	1

Приведем основные характеристики моделируемой сети Петри при помощи CPN Tools в таблице 2.

Таблица 2. Отчет о свойствах сети Петри

Отчет	Комментарий															
State Space Nodes: 99506 Arcs: 153076 Secs: 300 Status: Partial	Пространство состояний вычислено частично и содержит: 99506 узлов, 153076 дуг, 300 секций.															
Best Integer Bounds <table style="margin-left: auto; margin-right: auto;"> <tr> <td></td> <td>Upper</td> <td>Lower</td> </tr> <tr> <td>PetriNetPopov'r18</td> <td>1</td> <td>0</td> </tr> <tr> <td>PetriNetPopov'r19</td> <td>1</td> <td>0</td> </tr> <tr> <td>PetriNetPopov'r20</td> <td>1</td> <td>0</td> </tr> <tr> <td>PetriNetPopov'r21</td> <td>1</td> <td>3828</td> </tr> </table>		Upper	Lower	PetriNetPopov'r18	1	0	PetriNetPopov'r19	1	0	PetriNetPopov'r20	1	0	PetriNetPopov'r21	1	3828	Сеть ограничена сверху, так как все позиции ограничены.
	Upper	Lower														
PetriNetPopov'r18	1	0														
PetriNetPopov'r19	1	0														
PetriNetPopov'r20	1	0														
PetriNetPopov'r21	1	3828														
Home Markings None Dead Transition Instances None Live Transition Instances None	Домашняя маркировка отсутствует, мертвых и живых переходов нет.															

4. Численный метод оценки эффективности СЗИ от НСД.

Оценка показателя эффективности во временном (динамическом) диапазоне имеет место только тогда, когда все подсистемы СЗИ функционируют. Исследуемый временной диапазон, в котором выявлено несоответствие в работе СЗИ от НСД в АИС, следует детально проанализировать. То есть можно определить конкретно начало работы той или иной функции, что поможет идентифицировать некорректный процесс и определить некорректности в работе СЗИ от НСД в АИС.

Будем считать, что защитные функции СЗИ от НСД в АИС своевременно реализованы, если время $\tau_{инт}$ (интервал времени от момента обращения к защищаемой функции СЗИ от НСД до окончания выполнения функций) не превышает максимальное время τ_{max} (τ_{max} указано в технической документации АИС в разделе «Защита информации от НСД» и представляет собой постоянную величину для конкретных вычислительных ресурсов АИС):

$$\tau_{инт} \leq \tau_{max} . \quad (1)$$

Поэтому оценим эффективность СЗИ от НСД с помощью вероятности своевременного выполнения декларированных функций [17-20]:

$$K_{эф} = P(\tau_{инт} \leq \tau_{max}). \quad (2)$$

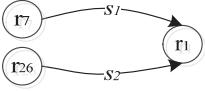
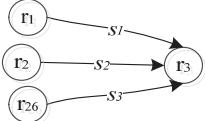
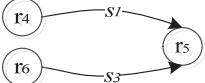
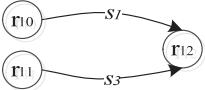
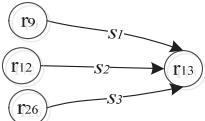
В ГОСТ 28195-89 для оценки динамического показателя эффективности функционирования СЗИ от НСД в АИС присутствует показатель «временной эффективности» программных систем, который позволяет описывать защищенность АИС в целом и под которым следует понимать «способность СЗИ от НСД выполнять заданные действия в интервале времени, отвечающем заданным требованиям» [17] (показатель «временной эффективности» $K_{эф}$ [3]).

На основе формальной модели функционирования СЗИ от НСД в АИС, реализованной при помощи аппарата сетей Петри, опишем процесс функционирования этих систем в виде марковского случайного процесса с конечным числом состояний (марковской цепи). Для этого необходимо определить конечные состояния, в которых может оказаться СЗИ от НСД в процессе ее функционирования. Как известно из [17], КМП можно охарактеризовать матрицей переходов СЗИ от НСД в одно из состояний $n = \overline{1, 27}$. Определим марковскую матрицу, которая описывает КМП из состояния a в состояние b , не превысив заданное время τ_{max} . В данный момент времени СЗИ от НСД может находиться в одном из конечных чисел состояний $\{S_1, S_2, \dots, S_n; n = 27\}$. В некоторый момент времени $t_k (k = 1, \dots)$ СЗИ от НСД случайным образом может осуществлять переходы из одного состояния S_a в другое S_b с переходной вероятностью $P_{ab}(t)$. Данную марковскую цепь с применением формулы полной вероятности опишем следующей формулой [21]:

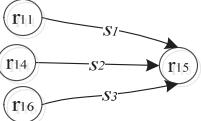
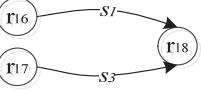
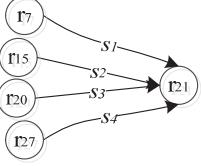
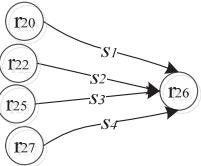
$$P_i = \sum_{j=1}^n P_j P_{ij}. \quad (3)$$

Условимся, что при вхождении в вершину одной дуги графа сети Петри (рисунок 1) вероятность события равна единице. В таблице 3 произведен расчет полной вероятностей перехода, которая учитывает все возможные связи графа сети Петри, кроме вероятностей, равных единице [22].

Таблица 3. Расчет вероятностей перехода

Графическое описание	Описание	Расчет вероятности
	<p>s_1 — выключение компьютера после неоднократного ввода после неправильного пароля; s_2 — завершение работы с СЗИ.</p>	$P(r_1) = P(r_7) \times P(r_1 r_7) + P(r_{26}) \times P(r_1 r_{26})$
	<p>s_1 — предъявление идентификатора; s_2 — в случае, если идентификатор не зарегистрирован в системе предъявите другой; s_3 — повторное предъявление идентификатора.</p>	$P(r_3) = P(r_1) \times P(r_3 r_1) + P(r_2) \times P(r_3 r_2) + P(r_{26}) \times P(r_3 r_{26})$
	<p>s_1 — ввод пароля; s_2 — повторный ввод пароля.</p>	$P(r_5) = P(r_4) \times P(r_5 r_4) + P(r_6) \times P(r_5 r_6)$
	<p>s_1 — идентификационная информация внешнего носителя уже проверялась (механизм контроля устройств не срабатывает); s_2 — проверяется принадлежность внешнего носителя пользователю (срабатывает механизм контроля устройств).</p>	$P(r_{12}) = P(r_{10}) \times P(r_{12} r_{10}) + P(r_{11}) \times P(r_{12} r_{11})$
	<p>s_1 — обращение к объекту, находящемуся в АИС; s_2 — обращение к объекту, находящемуся во внешнем устройстве; s_3 — доступ к объекту был заблокирован, обращение к другому объекту.</p>	$P(r_{13}) = P(r_9) \times P(r_{13} r_9) + P(r_{12}) \times P(r_{13} r_{12}) + P(r_{26}) \times P(r_{13} r_{26})$

Продолжение таблицы 3

Графическое описание	Описание	Расчет вероятности
	<p>s_1 — блокировка при несоответствии внешнего устройства и пользователя;</p> <p>s_2 — блокировка при несоответствии уровня конфиденциальности информации;</p> <p>s_3 — блокировка при попытке присвоения полномочий доступа пользователем.</p>	$P(r_{15}) = P(r_{11}) \times P(r_{15} r_{11}) + P(r_{14}) \times P(r_{15} r_{14}) + P(r_{16}) \times P(r_{15} r_{16})$
	<p>s_1 — допуск к объекту разрешен;</p> <p>s_2 — допуск к объекту на внешнем носителе разрешен (информация преобразована методом гаммирования).</p>	$P(r_{18}) = P(r_{16}) \times P(r_{18} r_{16}) + P(r_{17}) \times P(r_{18} r_{17})$
	<p>s_1 — внесение записи в журнал НСД о неправильном вводе пароля;</p> <p>s_2 — внесение записи в журнал НСД о блокировке доступа к объекту;</p> <p>s_3 — внесение записи в журнал НСД о блокировке преобразования объекта;</p> <p>s_4 — внесение записи в журнал НСД о блокировке удаления объекта.</p>	$P(r_{21}) = P(r_7) \times P(r_{21} r_7) + P(r_{15}) \times P(r_{21} r_{15}) + P(r_{20}) \times P(r_{21} r_{20}) + P(r_{27}) \times P(r_{21} r_{27})$
	<p>s_1 — завершение работы с объектом после блокировки преобразования объекта;</p> <p>s_2 — завершение работы с объектом после пересчета параметров его целостности;</p> <p>s_3 — завершение работы с объектом после его удаления;</p> <p>s_4 — завершение работы с объектом после блокировки удаления объекта.</p>	$P(r_{26}) = P(r_{20}) \times P(r_{26} r_{20}) + P(r_{22}) \times P(r_{26} r_{22}) + P(r_{25}) \times P(r_{26} r_{25}) + P(r_{27}) \times P(r_{26} r_{27})$

Система уравнений (4) представляет собой расчет переходных вероятностей согласно рисунку 1 и таблице 3:

$$\begin{cases}
 P(r_1), P(r_4), P(r_6), P(r_7), P(r_8), P(r_9), P(r_{10}), P(r_4), P(r_{11}), P(r_{14}), \\
 P(r_{17}), P(r_{19}), P(r_{20}), P(r_{22}), P(r_{23}), P(r_{24}), P(r_{25}), P(r_{27}) = 1; \\
 P(r_1) = P(r_7) \times P(r_1 | r_{26}) + P(r_{26}) \times P(r_1 | r_{26}); \\
 P(r_3) = P(r_1) \times P(r_3 | r_1) + P(r_2) \times P(r_3 | r_2) + P(r_{26}) \times P(r_3 | r_{26}); \\
 P(r_5) = P(r_4) \times P(r_5 | r_4) + P(r_6) \times P(r_5 | r_6); \\
 P(r_{12}) = P(r_{10}) \times P(r_{12} | r_{10}) + P(r_{11}) \times P(r_{12} | r_{11}); \\
 P(r_{13}) = P(r_9) \times P(r_{13} | r_9) + P(r_{12}) \times P(r_{13} | r_{12}) + P(r_{26}) \times P(r_{13} | r_{26}); \\
 P(r_{15}) = P(r_{11}) \times P(r_{15} | r_{11}) + P(r_{14}) \times P(r_{15} | r_{14}) + P(r_{16}) \times P(r_{15} | r_{26}); \\
 P(r_{18}) = P(r_{16}) \times P(r_{18} | r_{16}) + P(r_{17}) \times P(r_{18} | r_{17}); \\
 P(r_{21}) = P(r_7) \times P(r_{21} | r_7) + P(r_{15}) \times P(r_{21} | r_{15}) + P(r_{20}) \times P(r_{21} | r_{20}) + P(r_{27}) \times P(r_{21} | r_{27}); \\
 P(r_{26}) = P(r_{20}) \times P(r_{26} | r_{20}) + P(r_{22}) \times P(r_{26} | r_{22}) + P(r_{25}) \times P(r_{26} | r_{25}) + P(r_{27}) \times P(r_{26} | r_{27}).
 \end{cases} \quad (4)$$

В соответствии с теорией марковских процессов время нахождения СЗИ от НСД в АИС в представленных состояниях аппроксимируется экспоненциальным законом, функция распределения, которой представлена в следующем виде [21, 22]:

$$F_S(w) = \lambda e^{-\lambda w}. \quad (5)$$

Обращение к СЗИ от НСД соответствует входу в начальное состояние КМП, а конечное состояние соответствует завершению работы с СЗИ от НСД. Поведение КМП определяется матрицей переходных вероятностей $\|p_{ab}\|$, $a, b = \overline{1, N}$, где $\sum_{n=1}^N p_{ab} = 1$ и матрицей функции распределения $\|F_{ab}(\tau)\|$ или матрицей плотности вероятностей $\|f_{ab}(\tau)\|$ [21, 24-26]. Вероятности перехода p_{ab} , $a = \overline{1, n}, b = \overline{1, n}$ описывают степень объективной возможности появления того или иного события. Параметры представленных функций на данном этапе исследования могут иметь только приблизительные значения. Последующее их уточнение будет проводиться после разработки методики вычислительного эксперимента к СЗИ от НСД в АИС на этапе сбора конкрет-

ных статистических данных работы защитных функций используемой СЗИ от НСД [22-24].

Применение (5) позволяет учитывать случайный характер времени ожидания действий пользователя в АИС.

Из вышесказанного следует, что вероятность перехода $Q_{ab}(\tau)$ КМП из состояния a в состояние b определяется как произведение переходной вероятности и функции распределения:

$$Q_{ab}(\tau) = p_{ab} F_{ab}(\tau), a = \overline{1, n}, b = \overline{1, n}. \quad (6)$$

Вероятность перехода из одного состояния в другое представим в виде одной матрицы $Q_{ab}(\tau)$.

Показатель эффективности СЗИ от НСД в АИС, описывающий вероятностно-временные характеристики функционирования СЗИ от НСД, оценивается вероятностью достижения конечного состояния за время, не превышающее время τ :

$$K_{ab}(\tau) = \delta_{ab} p_a(\tau) + \sum_{k=1}^K p_{ab} \int_0^{\infty} f_{ac}(\tau) p_{cb}(\tau-t) d\tau, a \leq 1, b \leq K. \quad (7)$$

δ_{ab} — символ Кронекера (функция двух переменных), который описывается соотношениями: $\delta_{ab} = \begin{cases} 1, a = b \\ 0, a \neq b \end{cases}$.

В случае, если $a \neq b$, получим уравнение:

$$K_{ab}(\tau) = \sum_{k=1}^K p_{ab} \int_0^{\infty} f_{ac}(\tau) p_{cb}(\tau-t) d\tau, a \leq 1, b \leq K. \quad (8)$$

$K_{ab}(\tau)$ есть интервально переходная вероятность того, что в момент времени τ система находится в ϑ_a состоянии в случае ее пребывания в состоянии ϑ_b при $\tau = 0$.

$p_{cb}(\tau-t)$ есть вероятность того, что система, совершающая переход из ϑ_a в ϑ_b за время τ , пройдет через промежуточные состояния c, w, l, \dots за время $(\tau-t)$.

$p_a(\tau)$ из формулы (7) есть вероятность того, что система не выходит из состояния ϑ_a за время τ , где $F_a(\tau)$ есть функция распределения и определяется как:

$$p_a(\tau) = 1 - F_a(\tau). \quad (9)$$

Тогда получим формулу интервально переходной вероятности вида:

$$K_{ab}(\tau) = \delta_{ab}(1 - F_a(\tau)) + \sum_{k=1}^K p_{ab} \int_0^{\infty} f_{ac}(\tau) p_{cb}(\tau - t) d\tau. \quad (10)$$

Чтобы получить аналитическое решение уравнения (10), необходимо сделать его упрощение при помощи метода одностороннего (прямого) преобразования Лапласа.

$$K_{lap}(v) = \int_0^{\infty} e^{-v\tau} f_{ac}(\tau) d\tau. \quad (11)$$

После упрощения уравнений (6, 10) получим систему алгебраических уравнений:

$$Q_{ablap}(v) = p_{ab} F_{ab}(v), \quad (12)$$

$$K_{ablap}(v) = \delta_{ab} p_{alapl}(v) + \sum_{k=1}^K p_{ab} \int_0^{\infty} f_{aclapl}(\tau) p_{cb}(\tau - t) d\tau, a \leq 1, b \leq K. \quad (13)$$

Решение данной СЛАУ может быть получено различными численными методами решения СЛАУ, например:

1. Методом Гаусса, который был практически применен в [27-29] и в данной статье не рассматривается.

2. Методом последовательных итераций (метод Зейделя).

В данной статье будет рассмотрено практическое применение решения СЛАУ методом Гивенса.

5. Решение системы линейных алгебраических уравнений методом Гивенса (методом вращения). Из (12, 13) имеем:

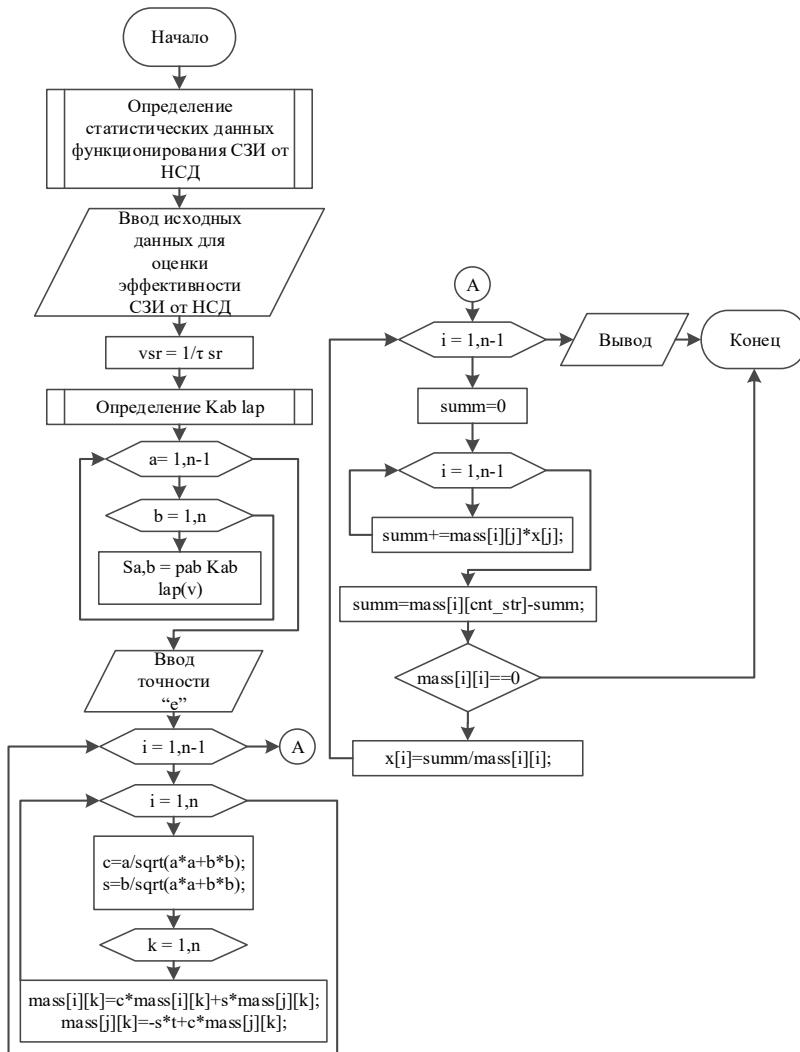


Рис. 4. Алгоритм расчета эффективности функционирования СЗИ от НСД в АИС ОВД методом Гивенса

- определение вероятностно-временных характеристик работы СЗИ;
- преобразование Лапласа;
- перебор элементов матрицы, характеризующей вероятностно-временные характеристики работы СЗИ;

– прямой и обратный ход решения СЛАУ методом Гивенса.

8. Заключение. В данной статье в соответствии с [1], где приведены основные этапы и задачи разработки СЗИ от НСД в АИС, разработана динамическая модель функционирования СЗИ от НСД в АИС на основе сети Петри, показано применение методов операционного исчисления Лапласа и численного метода решения СЛАУ методом Гивенса для разработки алгоритмов оценки динамического показателя эффективности функционирования СЗИ от НСД в АИС. Разработанные модели и алгоритмы, приведенные в статье, в дальнейшем могут быть использованы для разработки комплекса программ анализа, моделирования и исследования динамических свойств СЗИ от НСД при их разработке с целью повышения защищенности существующих и перспективных (разрабатываемых) АИС.

Литература

1. *Розозин Е.А., Попов А.Д., Шагиров Т.В.* Проектирование систем защиты информации от несанкционированного доступа в автоматизированных системах органов внутренних дел // Вестник Воронежского института МВД России. 2016. № 2. С. 174–183.
2. *Розозин Е.А., Попов А.Д.* Модель функционирования типовой системы защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД // Вестник Воронежского института МВД России. 2016. № 4. С. 122–132.
3. *Питерсон Д.Ж.* Теория сетей Петри и моделирование систем: пер. с англ. // М.: Мир. 1984. 264 с.
4. *Котов В.Е.* Сети Петри // М.: Наука. 1984. 160 с.
5. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации №646 от 05.12.2016 г.
6. ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении // М.: Стандартинформ. 2014. 27 с.
7. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания // М.: Стандартинформ. 2014. 6 с.
8. ФСТЭК РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
9. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
10. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
11. Trusted Computer System Evaluation Criteria. US Department of Defense 5200.28-STD. 1993.
12. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. – Department of Trade and Industry. London. 1991.
13. Federal Criteria for Information Technology Security. National Institute of Standards and Technology & National Security Agency. Version 1.0. 1992.

14. Canadian Trusted Computer Product Evaluation Criteria. Canadian System Security Center Communication Security Establishment, Government of Canada. Version 3.0e. 1993.
15. Common Criteria for Information Technology Security Evaluation. National Institute of Standards and Technology & National Security Agency (USA), Communication Security Establishment (Canada), Communications-Electronics Security Group (United Kingdom), Bundesamt für Sicherheit in der Informationstechnik (Germany), Service Central de la Sécurité des Systèmes d'Information (France), National Communications Security Agency (Netherlands). Version 2.1. 1999.
16. ГОСТ Р 15408-2013. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий // М.: Стандартинформ. 2014.
17. ГОСТ 28195-89. Оценка качества программ средств. Общие положения.// Издательство стандартов. 1989. 32 с.
18. *Скрыль С.В. и др.* Показатели эффективности информационной деятельности в условиях комплексного технического контроля обеспечения защищенности речевой информации // Приборы и системы. Управление, контроль, диагностика. 2016. № 2. С. 28–34.
19. *Скрыль С.В., Голубков Д.А., Половинкин В.А.* Показатели эффективности информационных процессов в интегрированных системах безопасности в условиях обеспечения антивирусной защиты // Вестник Воронежского института МВД России. 2014. № 4. С. 212–220.
20. *Скрыль С.В. и др.* Оценка характеристик компонент защиты информации от несанкционированного доступа для реализации функций обеспечения целостности и доступности информации // Приборы и системы. Управление, контроль, диагностика. 2014. № 7. С. 21–25.
21. *Тихонов В.И., Миронов М.А.* Марковские процессы //М.: Сов. Радио. 1977. 488 с.
22. *Венцель Е.С.* Теория вероятностей // Москва. Наука. 1969. 576 с.
23. *Дубровин А.С. и др.* Общенаучные итоги создания эталонной модели защищенной автоматизированной системы // Фундаментальные исследования. 2015. № 2-15. С. 3247–3251.
24. *Ptitsyn P.S., Radko D.V., Lankin O.V.* Designing architecture of software framework for building security infrastructure of global distributed computing systems // ARPN Journal of Engineering and Applied Sciences. 2016. vol. 11. no. 19. С. 11599–11610.
25. *Ланкин О.В.* Метод оценки эффективности функционирования систем интеллектуальной защиты информации от несанкционированного доступа // Информация и безопасность. 2011. № 2. pp. 267–270.
26. *Дунин В.С., Бокова О.И.* Оценка эффективности системы интеллектуального управления защитой информации в инфокоммуникационных системах ОВД. // Вестник Воронежского государственного университета инженерных технологий. 2011. № 4. С. 62–73.
27. *Змеев С.А., Солод Д.В., Сиренький Е.И., Застрожных И.И.* Модель оценки эффективности программных систем защиты информации в системах электронного документооборота // Вестник Воронежского института ФСИН России. 2013. № 1. С. 82–85.
28. *Зиновьев П.В., Застрожных И.И., Розозин Е.А.* Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного документооборота // Воронеж: Воронеж. гос. техн. ун-т, 2015. 106 с.
29. *Змеев А.А.* Методы и средства повышения защищенности автоматизированных систем // Воронеж: Воронежский институт МВД России. 2013. 108 с.
30. *Калиткин Н.Н.* Численные методы // М.: Наука. 1978. 512 с.

31. Амосов А.А., Дубинский Ю.А., Копченова Н.В. Вычислительные методы для инженеров // М.: Высшая школа. 1994. 544 с.

Дровникова Ирина Григорьевна — д-р техн. наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел, Воронежский институт МВД России. Область научных интересов: системы защиты информации, эволюционное моделирование, автоматизированные информационные системы, теория вероятности, управление в социально-экономических системах. Число научных публикаций — 210. idrovnikova@mail.ru; пр. Патриотов, 53, Воронеж, 394086; р.т.: +7(472)200-51-88.

Мешерякова Татьяна Вячеславовна — канд. физ.-мат. наук, начальник кафедры автоматизированных информационных систем органов внутренних дел, Воронежский институт МВД России. Область научных интересов: математическое моделирование, теория вероятности, применение методов математического моделирования в эпидемиологии. Число научных публикаций — 62. meshet73@mail.ru; пр. Патриотов, 53, Воронеж, 394086; р.т.: +7(473)200-51-81.

Попов Антон Дмитриевич — адъюнкт кафедры автоматизированных информационных систем органов внутренних дел, Воронежский институт МВД России. Область научных интересов: защита информации от НСД в АИС, проектирование и управление процессами защиты информации на основе количественной оценки СЗИ от НСД в АИС, тестирование и анализ СЗИ, разработка АИС, прикладная информатика. Число научных публикаций — 25. anton.holmes@mail.ru; пр. Патриотов, 53, Воронеж, 394086; р.т.: +7(473)200 51-80.

Рогозин Евгений Алексеевич — д-р техн. наук, профессор, академик РАЕН, профессор кафедры автоматизированных информационных систем органов внутренних дел, Воронежский институт МВД России. Область научных интересов: защита информации от НСД в АИС, проектирование и управление процессами защиты информации на основе количественной оценки СЗИ от НСД в АИС, прикладная информатика. Число научных публикаций — 240. evgenirogozin@yandex.ru; пр. Патриотов, 53, Воронеж, 394086; р.т.: +7(473)200-51-88.

Ситник Сергей Михайлович — канд. физ.-мат. наук, доцент, доцент кафедры математики и моделирования систем, Воронежский институт МВД России. Область научных интересов: дифференциальные уравнения и их приложения в теории сигналов. Число научных публикаций — 270. smsitnik2017@yandex.ru; пр. Патриотов, 53, Воронеж, 394086; р.т.: +7(473)200-52-11.

DROVNIKOVA I.G., MESHCHERYAKOVA T.V., POPOV A.D., ROGOZIN E.A.,
SITNIK S.M.

MATHEMATICAL MODEL FOR ESTIMATING THE EFFICIENCY OF INFORMATION SECURITY SYSTEMS BY MEANS OF LAPLACE TRANSFORMATION AND GIVENS METHOD

Drovnikova I.G., Meshcheryakova T.V., Popov A.D., Rogozin E.A., Sitnik S.M. Mathematical model for estimating the efficiency of information security systems by means of Laplace transformation and Givens method.

Abstract. The article presents a dynamic model of the information security system (ISS) functionality for unauthorized access in automated information systems (AIS) created on the basis of Petri net machines. The authors developed a mathematical model for dynamic operating performance ratio assessment in ISS against the unauthorized access in AIS based on the Laplace transform method and a numerical technique of solving simultaneous linear algebraic equations (SLAE) by Givens method. They authors also suggest a calculation technique for dynamic operating performance ratio algorithm in ISS against the unauthorized access in AIS by applying the selected method for solving equations (SLAE) for further development of evaluation programs complex as far as for modeling and assessment of dynamic performance ratio in ISS against the unauthorized access in AIS. Selection and development of the operating performance ratio was based on the analysis of GOST (RF Standard-Setting Authority) 28195-89.

Keywords: information security system, automated information system, unauthorized access, stopping time, effectiveness, Petri net machines.

Drovnikova Irina Grigorevna — Ph.D., Dr. Sci., associate professor, professor of automated information systems in interior affairs department, Voronezh Institute of the Ministry of Interior. Research interests: information systems security, evolutionary modeling, automated information systems, probability theory, social-and-economic system management. The number of publications — 210. idrovnikova@mail.ru; 53, Prospekt Patriotov, Voronezh, 394086, Russia; office phone: +7(472)200-51-88.

Meshcheryakova Tatiana Vyacheslavovna — Ph.D., head of automated information systems in interior affairs department, Voronezh Institute of the Ministry of Interior. Research interests: mathematical modeling, probability theory, the use of methods of mathematical modeling in epidemiology. The number of publications — 62. mesher73@mail.ru; 53, Prospekt Patriotov, Voronezh, 394086, Russia; office phone: +7(473)200-51-81.

Popov Anton Dmitrievich — Ph.D. student of automated information systems in interior affairs department, Voronezh Institute of the Ministry of Interior. Research interests: information protection against unauthorized access in AIS, design and management of information security processes based on quantitative assessment of ISS, testing and analysis of ISS, AIS development, applied computer science. The number of publications — 25. anton.holmes@mail.ru; 53, Prospekt Patriotov, Voronezh, 394086, Russia; office phone: +7(473)200-51-80.

Rogozin Evgeniy Alekseevich — Ph.D., Dr. Sci., professor, academician of RANS, professor of automated information systems in interior affairs department, Voronezh Institute of the Ministry of Interior. Research interests: information security from the unauthorized access in AIS, design and management of information security processes based on the quantitative assessment of ISS security from the unauthorized access in AIS, applied informatics. The number of publications — 240. evgenirogozin@yandex.ru; 53, Prospekt Patriotov, Voronezh, 394086, Russia; office phone: +7(473)200-51-88.

Sitnik Sergei Mihaylovich — Ph.D., associate professor, associate professor of mathematics and systems modeling department, Voronezh Institute of the Ministry of Interior. Research interests: differential equations and their applications in signal theory. The number of publications — 270. smsitnik2017@yandex.ru; 53, Prospekt Patriotov, Voronezh, 394086, Russia; office phone: +7(473)200-52-11.

References

1. Rogozin E.A., Popov A.D., Shagirov T.V. [Design protection information systems from unauthorized access in the automated systems of the Law Enforces Agencies]. *Vestnik Voronezhskogo instituta MVD Rossii - Bulletin of the Voronezh Institute of the Ministry of the Interior of Russia*. 2016. vol. 2. pp. 174–183. (In Russ).
2. Rogozin E.A., Popov A.D. [Model operation of the standard information system of protection against unauthorized access to automated information systems of the Law Enforces Agencies]. *Vestnik Voronezhskogo instituta MVD Rossii - Bulletin of the Voronezh Institute of the Ministry of the Interior of Russia*. 2016. vol. 4. pp. 122–132. (In Russ).
3. Peterson J.L. Petri net theory and the modeling of systems. The University of Texas at Austin. Prentice-hall, Inc. 1981. 290 p. (Russ. ed.: Peterson D.Zh. *Teorija setej Petri i modelirovanie system*. Moscow: Mir. 1984. 264 p.).
4. Kotov V.E. *Seti Petri* [Petri nets]. M.: Nauka. 1984. 160 p. (In Russ).
5. *Doktrina informacionnoj bezopasnosti Rossijskoj Federacii* [The information security doctrine of the Russian Federation]. Utverzhdena Ukazom Prezidenta Rossijskoj Federacii № 646. (In Russ).
6. GOST R 51583-2014. [Information protection. Sequence of protected operational system formation. General provisions]. M.: Standartinform. 2014. 27 p. (In Russ).
7. GOST 34.601-90. [Information technology. Set of standards for automated systems. Atomated systems. Stages of development]. M.: Standartinform. 2014. 6 p. (In Russ).
8. FSTEC RF. [Guidance document. Means of computer facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information]. (In Russ).
9. FSTEC RF. [Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and the requirements for data protection]. (In Russ).
10. FSTEC RF. [Guidance document. The concept of protection of computer and automated systems against unauthorized access to information]. (In Russ).
11. Trusted Computer System Evaluation Criteria. US Department of Defense 5200.28-STD. 1993.
12. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. – Department of Trade and Industry. London. 1991.
13. Federal Criteria for Information Technology Security. National Institute of Standards and Technology & National Security Agency. Version 1.0. 1992.
14. Canadian Trusted Computer Product Evaluation Criteria. Canadian System Security Center Communication Security Establishment, Government of Canada. Version 3.0e. 1993.
15. Common Criteria for Information Technology Security Evaluation. National Institute of Standards and Technology & National Security Agency (USA), Communication Security Establishment (Canada), Communications-Electronics Security Group (United Kingdom), Bundesamt für Sicherheit in der Informationstechnik (Germany), Service Central de la Sécurité des Systèmes d'Information (France), National Communications Security Agency (Netherlands). Version 2.1. 1999.
16. GOST R 15408-2013. [The order of creation of the automated systems of protected construction Methods and means of ensuring security. Criteria for assessing the security of information technology]. 2014. (In Russ).
17. GOST 28195-89. [Quality control of software systems. General principles]. Izdatel'stvo standartov. 1989. 32 p. (In Russ).

18. Skryl' S.V., Gromov Ju.Ju., A.V. Shherbakov A.V., Ponomarenko S.A., Ponomarev M.V. [Indicators of effectiveness of information activity in the conditions of complex technical control provide voice information security]. *Pribory i system. Upravlenie, kontrol', diagnostika - Instruments and systems. Management, monitoring, diagnostics*. 2016. vol. 2. pp. 28–34. (In Russ).
19. Skryl' S.V., Golubkov D.A., Polovinkin V.A. [Performance indicators of information processes in integrated security systems in the conditions of anti-virus protection software]. *Vestnik Voronezhskogo instituta MVD Rossii - Bulletin of the Voronezh Institute of the Ministry of the Interior of Russia*. 2014. vol. 4. pp. 212–220. (In Russ).
20. Skryl' S.V. et al. [Sizintsev Evaluation of information security components of the characteristics of the unauthorized access to the realization of functions to ensure the integrity and availability of information]. *Pribory i system. Upravlenie, kontrol', diagnostika - Instruments and systems. Management, monitoring, diagnostics*. 2014. vol. 7. pp. 21–25. (In Russ).
21. Tihonov V.I., Mironov M.A. *Markovskie process* [Markov processes]. M.: Sov. Radio. 1977. 488 p. (In Russ).
22. Vencel' E.S. *Teorija verojatnostej* [Probability theory]. M.: Nauka. 1969. 576 p. (In Russ).
23. Dubrovin A.S. et al. [General scientific results of the creation of a reference model of the protected automated system]. *Fundamental'nye issledovanija - Fundamental Research*. 2015. vol. 2-15. pp. 3247–3251. (In Russ).
24. Ptitsyn P.S., Radko D.V., Lankin O.V. Designing architecture of software framework for building security infrastructure of global distributed computing systems. *ARPAN Journal of Engineering and Applied Sciences*. 2016. vol. 11. no. 19. C. 11599–11610.
25. Lankin O.V. [Performance evaluation method of functioning of the intellectual protection of information systems against unauthorized access]. *Informacija i bezopasnost' - Information and Security*. 2011. vol. 2. pp. 267–270. (In Russ).
26. Dunin V.S., Bokova O.I. [Evaluating the effectiveness of the system of intellectual management of information protection in the infocommunication systems of the Law Enforces Agencies]. *Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernyh tehnologij - Bulletin of Voronezh State University of Engineering Technology*. 2011. vol. 4. pp. 62–73. (In Russ).
27. Zmeev S.A., Solod D.V., Siren'kij E.I., Zastrozhnov I.I. [Model evaluation of the effectiveness of information security software systems in electronic document management systems]. *Vestnik Voronezhskogo instituta FSIN Rossii - Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2013. vol. 1. pp. 82–85. (In Russ).
28. Zinov'ev P.V., Zastrozhnov I.I., Rogozin E.A. *Metody i sredstva ocenki jeffektivnosti podsystemy zashhity konfidencial'nogo informacionnogo resursa pri ejo proektirovanii v sistemah jelektronnogo dokumentooborota* [Methods and tools to evaluate the effectiveness of the protection of confidential information resource subsystem with its design in electronic document management systems]. Voronezhskij gosudarstvennyj tehničeskij universitet. 2015. 106 p. (In Russ).
29. Zmeev A.A. *Metody i sredstva povyshenija zashhishhennosti avtomatizirovannyh sistem* [Methods and means of improving the security of automated systems]. Voronezh: Voronezhskij institut MVD Rossii. 2013. 108 p. (In Russ).
30. Kalitkin N.N. *Chislennye metody* [Numerical methods]. M.: Nauka. 1978. 512 p. (In Russ).
31. Amosov A.A., Dubinskij Ju.A., Kopchenova N.V. *Vychislitel'nye metody dlja inzhenerov* [Computational Methods for Engineers]. M.: Vysshaja shkola. 1994. 544 p. (In Russ).