Для цитирования: *Бокова О.И., Дровникова И.Г., Попов А.Д., Рогозин Е.А. Модель процесса функционирования системы защиты информации от несанкционированного доступа, созданная в программной среде имитационного моделирования «CPN TOOLS». Вестник Дагестанского государственного технического университета. Технические науки. 2019; 46 (1): 90-102. DOI:10.21822/2073-6185-2019-46-1-90-102*
For citation: *Bokova O.I., Drovnikova I.G., Popov A.D., Rogozin E.A. Model of the process of functioning of the information protection system from unauthorized access created in the software environment of imitation modeling "CPN TOOLS". Herald of Daghestan State Technical University. Technical Sciences. 2019; 46 (1): 90-102. (In Russ.) DOI:10.21822/2073-6185-2019-46-1-90-102*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 519.7: 004.05
DOI:10.21822/2073-6185-2019-46-1-90-102

МОДЕЛЬ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, СОЗДАННАЯ В ПРОГРАММНОЙ СРЕДЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ «CPN TOOlS»

Бокова О.И.[2], Дровникова И.Г.[1], Попов А.Д.[4], Рогозин Е.А.[3]
[1-4] Воронежский институт МВД России,
[1-4]394065, г. Воронеж, пр. Патриотов, 53, Россия,
[1]e-mail: o.i.bokova@gmail.com, [2]e-mail: idrovnikova@mail.ru,
[3]e-mail: evgenirogozin@yandex.ru, [4]e-mail: anton.holmes@mail.ru

Резюме. Цель*. В настоящее время проведение вычислительного эксперимента над системой защиты информации от несанкционированного доступа, эксплуатируемой в автоматизированной системе, является трудоёмким процессом. Наибольшую сложность в данном направлении исследований представляет определение вероятностно-временных характеристик и формирование отчётов в процессе функционирования системы защиты информации. С целью анализа, получения и исследования вероятностно-временных характеристик данной системы необходимо разработать математическую модель её функционирования с использованием аппарата имитационного моделирования.* ***Метод.*** *Одним из методов решения указанной проблемы является вычислительный эксперимент, в основе которого лежит построение имитационной модели. В качестве программного продукта имитационного моделирования была выбрана среда «CPN Tools», основными достоинствами которой являются: высокий уровень визуализации, возможность формирования различных отчётов по работе системы, быстрая модифицируемость моделей для решения другого класса задач, а также интеграция с другими программными средствами для формирования графических зависимостей. Результат. Разработана имитационная модель системы защиты информации от несанкционированного доступа в программной среде «CPN Tools», позволяющая получать её вероятностно-временные характеристики, а также проводить исследования защищённости автоматизированной системы с учётом отвлечения значительных вычислительных ресурсов на процесс функционирования системы информационной безопасности при эксплуатации в автоматизированной системе в защищённом исполнении. Вывод. Имитационная модель системы защиты информации от несанкционированного доступа в программной среде «CPN Tools» может использоваться как инструмент при оценке защищённости специальными органами по аттестации объектов информатизации и структурными подразделениями уполномоченных ведомств, а также при проектировании подобных систем с целью недопущения логических ошибок, определения их временных характеристик и сравнения с имеющимися в соответствии с техническим заданием на разрабатываемую систему защиты информации от несанкционированного доступа.*

Ключевые слова: *автоматизированная система, система защиты информации, несанкционированный доступ, имитационная модель, программная среда, вероятностно-временные характеристики, защита информации*

COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

MODEL OF THE PROCESS OF FUNCTIONING OF THE INFORMATION PROTECTION SYSTEM FROM UNAUTHORIZED ACCESS CREATED IN THE SOFTWARE ENVIRONMENT OF IMITATION MODELING "CPN TOOLS"

Oksana I. Bokova,[2] Irina G. Drovnikova[1], Anton D. Popov[42], Evgenii A. Rogozin[3]

[1-4]Voronezh Institute of the Ministry of the Interior of the Russian Federation,
[1-4]53 Patriotov Str., Voronezh 394065, Russia,
[1]e-mail: o.i.bokova@gmail.com,[2]e-mail: idrovnikova@mail.ru,
[3]e-mail: evgenirogozin@yandex.ru, [4]e-mail: anton.holmes@mail.ru

Abstract Objectives *At present, conducting a computational experiment on a system for protecting information from unauthorized access operated in an automated system is a time consuming process. The greatest difficulty in this area of research is the determination of probabilistic-temporal characteristics and the formation of reports during the operation of the information protection system. In order to analyze, obtain and study the probabilistic-time characteristics of this system, it is necessary to develop a mathematical model of its operation using an imitational modeling tool.* ***Method.*** *One of the methods for solving this problem is a computational experiment, which is based on the construction of a simulation model. The CPN Tools environment was chosen as a software simulation product, the main advantages of which are: a high level of visualization, the ability to generate various reports on the system operation, fast modifiability of models for solving a different class of problems, as well as integration with other software means for the formation of graphical dependencies.* ***Result.*** *A simulation model of the system for protecting information from unauthorized access in the "CPN Tools" software environment was developed. protected performance.* ***Conclusion.*** *The presented im-model model of protecting information from unauthorized access in the software environment "CPN Tools" can be used as a tool in assessing the security of special bodies for the attestation of informatization objects and structural divisions of authorized departments. It can also be used in the design of such systems in order to prevent logical errors, determine their temporal characteristics and compare with the existing ones in accordance with the technical specifications for the system being developed to protect information from unauthorized access.*

Keywords: *automated system, information protection system, unauthorized access, simulation model, software environment, probabilistic-temporal characteristics, information protection*

Введение. В настоящее время вопросы, связанные с формированием требований к системам защиты информации (СЗИ) от несанкционированного доступа (НСД), являются важными и актуальными для автоматизированных систем (АС) в защищённом исполнении. Согласно ГОСТ Р 50922-2006 РД «Основные термины и определения» [1] под защищёнными АС (как объектом защиты) понимаются такие АС, которые необходимо защищать в соответствии с целями защиты информации. Анализируя средства и системы информационной безопасности (ИБ), можно утверждать, что СЗИ от НСД является одной из основных преград для противодействия угрозам НСД к информационному ресурсу АС. Поэтому формирование требований к современным АС в защищённом исполнении приобретает первостепенное значение.

Существующая практика формирования требований к СЗИ от НСД при разработке, сертификации и эксплуатации данных систем показала, что они представляются в виде функционала в соответствии с классом защищённости АС на основе нормативных документов ФСТЭК России, к которым можно отнести руководящий документ «Классы защищённости АС» [2], ГОСТ Р 15408-2013 «Единые критерии безопасности» [3] и др. Основным недостатком данного подхода является то, что не представляется возможным контролировать поведение СЗИ от НСД в АС при её функционировании в масштабе реального времени. Таким образом, используемая в

настоящее время методика формирования требований к СЗИ от НСД в АС требует совершенствования [4].

Постановка задачи. Для устранения указанного недостатка необходимо разработать такую методику формирования требований к СЗИ от НСД в АС, которая явилась бы существенным дополнением к имеющейся статистической методике (функционал практически независим от времени) и давала бы ясную картину функционировании СЗИ в масштабе реального времени. Для этого следует учесть существующие недостатки эксплуатации СЗИ от НСД в АС, к которым, несомненно, можно отнести их ресурсоёмкость (отвлечение вычислительных ресурсов АС), что в целом мешает функционированию АС по их основному предназначению (обработка, хранение и передача информации). С учётом выше изложенного разрабатываемая методика формирования требований к СЗИ от НСД в АС должна базироваться на методах математического моделирования, позволяющих исследовать эти системы в реальном (динамическом) режиме и давать практические рекомендации по использованию средств и систем ИБ на объектах информатизации при их разработке, эксплуатации, сертификации и т.д.

Создание и функционирование СЗИ от НСД в АС представляет собой трудоёмкий процесс [5-8], причиной которого является недетерминированность (неопределённость) данных систем. Это означает, что их разработка и администрирование должны осуществляться с учётом компонентов, потенциально являющихся уязвимыми местами в системе. Например, следует учитывать, могут ли теряться данные в процессе взаимодействия различных подсистем, соответствуют ли протекающие процессы времени их функционирования в СЗИ от НСД и т.д. Таким образом, при разработке подобных систем, как правило, возникает значительное количество ошибок, связанных с тем, что разработчик не всегда может учесть взаимосвязь компонентов, что, вероятно, приведёт к сбоям при работе реальной системы, а, следовательно, — к потере большого количества времени, потраченного на пересмотр предметной области, переработку технической документации и т.д.

При проведении вычислительного эксперимента на функционирующей СЗИ от НСД, сертифицированной по 3-му классу защищённости средств вычислительной техники и по 2-му уровню контроля отсутствия недокументированных возможностей, возникли трудности при определении вероятностно-временных характеристик (ВВХ) функционирования подсистемы «Вход в систему», связанные с тем, что выявить данные характеристики возможно только на низком уровне при создании дополнительных функций перехвата Windows Api. Поскольку данный процесс является довольно трудоёмким, в качестве альтернативного пути решения указанной задачи была выбрана разработка математической модели функционирования СЗИ от НСД в АС при помощи имитационного моделирования с использованием специального программного продукта.

Методы исследования. Имитационное моделирование — универсальный метод, используемый как при построении модели, так и при описании с достаточной точностью её поведения во времени. Целью разработки подобных моделей является выбор стратегии функционирования СЗИ от НСД по сравнению с имеющимися для получения её лучшего (оптимального) варианта. Разработка имитационных моделей необходима, поскольку коррекцию ошибок и других недостатков предпочтительнее осуществлять на стадии моделирования, чем при реальном создании СЗИ. А при эксплуатации системы имитационная модель может использоваться для определения её ВВХ с целью оценки эффективности функционирования СЗИ от НСД в АС. Сложившаяся ситуация даёт возможность, используя современные средства моделирования, а также исследования учёных в данной области [9-14], построить подобную модель, основной целью которой служит оценка реального уровня защищённости при создании и эксплуатации СЗИ от НСД в АС.

Построение имитационной модели направлено на определение ВВХ как функционирования СЗИ от НСД в целом, так и её подсистем в АС.

Для имитации функционирования СЗИ от НСД целесообразно использовать программный продукт «CPN Tools», предназначенный для моделирования и анализа, как сетей Петри, так и их разновидностей (цветных сетей Петри, временных сетей Петри).

Выделим основные преимущества пакета «CPN Tools» для имитационного моделирования процесса функционирования СЗИ от НСД:

- наглядность, структурированность и ранжированное описание компонентов имитационной модели;
- модель устраняет недостатки и неопределённости в формальных моделях СЗИ от НСД в АС;
- возможность описания подсистем СЗИ от НСД в АС «Вход в систему», «Разграничения доступа и работа с внешними носителями», «Контроля целостности, регистрации и учёта» а также угроз, влияющих на компоненты системы, в рамках одной сетевой структуры;
- возможность определения ВВХ СЗИ от НСД для оценки эффективности её функционирования с целью проведения вычислительного эксперимента;
- возможность проведения анализа имитационной модели СЗИ от НСД при помощи встроенных механизмов получения различного рода отчётов о её функционировании;
- возможность интеграции СЗИ от НСД в АС, то есть более детального описания её компонентов (например, механизма обработки информации, базы данных и т.д.) [15-18].

Программная среда имитационного моделирования «CPN Tools» доступна, как для операционных систем семейства Windows, так и Linux. В ней существует возможность программирования на унифицированном языке моделирования (UML) «Unified Modeling Language». «CPN Tools» позволяет сгенерировать и проанализировать пространство состояний строящейся модели, получая различного рода отчёты о работе сети.

Имитационное моделирование в «CPN Tools» является дискретно-событийным, то есть предполагающим мгновенную смену состояния сети Петри, что в полной мере соответствует конечному марковскому процессу. Поэтому выбор данного программного продукта является оптимальным для проведения исследования.

«CPN Tools» поддерживает два типа моделирования — интерактивное и автоматическое. При интерактивном моделировании пользователь полностью контролирует работу имитационной модели, а именно самостоятельно, используя встроенные в «CPN Tools» функции, переходит между состояниями до необходимого ему шага моделирования. Отличительной чертой данного типа моделирования является то, что все действия пользователь может наблюдать в графическом режиме, что даёт возможность наблюдать работу модели на каждом шаге моделирования. При автоматическом моделировании пользователь указывает количество шагов, которые должны быть пройдены, устанавливает критерии остановки и точки останова. Затем включается процесс симуляции, который моделирует действия системы без участия пользователя, при этом переход между событиями осуществляется случайным образом. В итоге пользователь видит лишь конечное состояние имитационной модели. Результирующий отчёт о проведённых симуляциях будет автоматически сохранён в каталоге создаваемой модели, он содержит пошаговый отчёт о функционировании модели. Преимущество автоматического моделирования по сравнению с интерактивным, заключается в том, что оно позволяет строить имитационные модели больших размеров, поскольку при симуляции выполняется большее число шагов моделирования в секунду.

Обсуждение результатов. На основе результатов исследований учёных по практическому применению СЗИ от НСД в АС построим имитационную модель сети Петри, моделирующую действия пользователя [4, 9-14, 19-23]. Для этого представим разработанную модель в программной среде «CPN Tools», как показано на рис. 1.

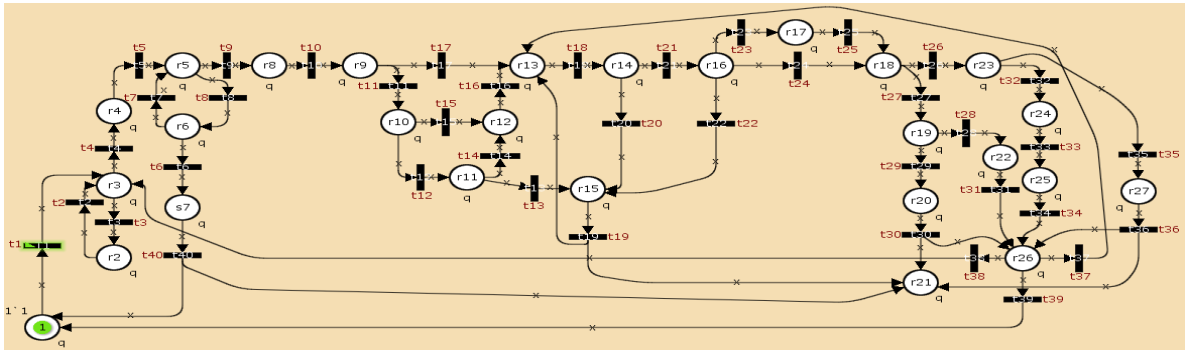

Рис.1.Сеть Петри СЗИ от НСД в АС, построенная в программной среде имитационного моделирования «CPN Tools»

Fig. 1. Petri SZI network from unauthorized access control in the AU, built in the software environment of simulation modeling «CPN Tools»

Имитационная модель является дискретной, динамической, стохастической по причине того, что этими свойствами обладает СЗИ от НСД в АС. Поэтому данная модель будет дискретно-событийной, следственно отражающей свойства во времени, а также мгновенный и случайный переходы из одного состояния в другое [24, 25].

Подробное исследование ВВХ функционирования СЗИ от НСД с обоснованием количества прогонов по сети целесообразно осуществлять на примере моделирования её подсистемы — «Вход в систему» [26].

Поскольку время в «CPN Tools» представляется в виде целого числа, необходимо установить взаимосвязь между реальным и модельным временем функционирования СЗИ от НСД в АС. Выберем для интервала реального времени функционирования СЗИ от НСД следующее соотношение с количеством тактов модельного времени для подсистемы «Вход в систему»: 1 секунда равна 1 такту.

На основе выбранного соотношения установим задержки для всех действий в сети (например, длительность действия «Повторный ввод пароля» в 5 секунд в модели будет составлять 5 тактов модельного времени). Очевидно, что данное соотношение будет оставаться неизменным и при рассмотрении работы всей сети.

Для построения сети и её функционирования приближённо к реальному поведению проведём конфигурацию в виде создания сегмента кода на языке UML (рис. 2), а саму сеть представим на рис. 3.

```
Declarations
  block
  Standard declarations
    colset UNIT
    colset INT
    colset q = int timed;
    var x
    colset BOOL
    colset STRING
    fun curTime()=IntInf.toInt(!CPN'Time.model_time)
    colset W = int with 1..100;
    colset W1 = int with 1..100;
    var v0 : W;
    val v2 = 10;
    var v1 : W1;
    fun W(v0,v2) = (v0<=v2);
    fun W1(v0,v2) = (v0>v2);
    colset QQ= int with 1..100;
    colset QQ1= int with 1..100;
    var q0 : QQ;
    val q1 = 10;
    fun QQ(q0,q1) = (q0<=q1);
    fun QQ1(q0,q1) = (q0>q1);
    colset EE= int with 1..100;
    colset EE1= int with 1..100;
    var e0 : EE;
    val e1 = 10;
    fun EE(e0,e1) = (e0<=e1);
    fun EE1(e0,e1) = (e0>e1);
```

Рис. 2. Настройка сети, имитирующей функционирование подсистемы «Вход в систему» СЗИ от несанкционированного доступа

Fig. 2. Setting up a network that simulates the functioning of the subsystem "Login" GIS from unauthorized access

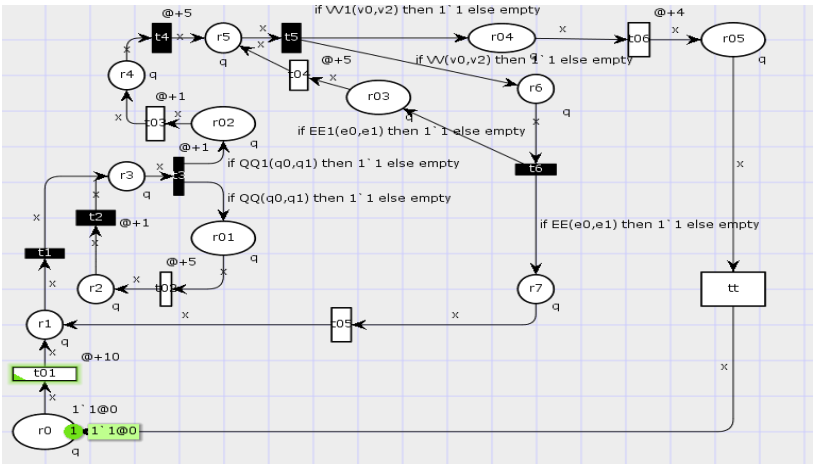

Рис. 3.Имитационная модель подсистемы «Вход в систему» СЗИ от НСД
Fig. 3. Imitation model of the subsystem "Login" GIS from unauthorized access

В «CPN Tools» имеется возможность построить пространство состояний с помощью инструмента «Отображение узла пространства состояния с заданным номером». Пространство состояний представляет собой неупорядоченное множество всех компонентов исследуемой системы, которое включает взаимосвязи между ними и информацию о них. Пространство состояний представляется в виде графа сети Петри, узлами которого являются достижимые маркировки исследуемой модели. Для этого создадим новую страницу и воспользуемся имеющимся инструментом (рис. 4).

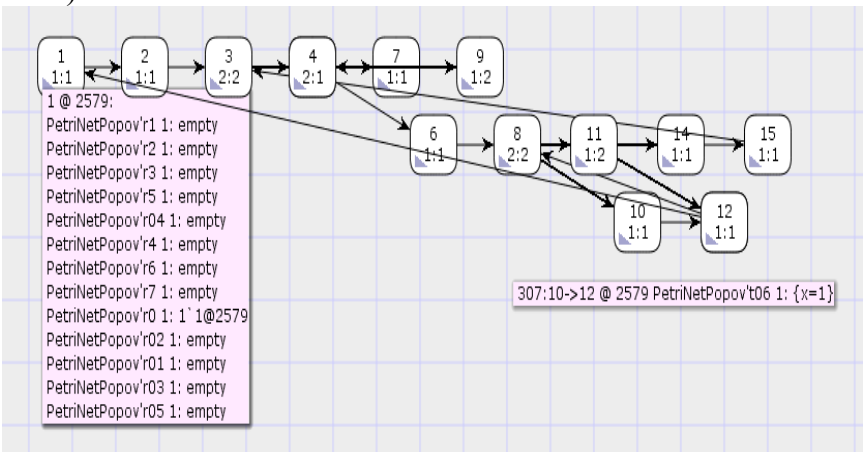

Рис. 4.Пространство состояний подсистемы «Вход в систему» СЗИ от НСД
Fig. 4. State space of the subsystem "Login" GIS from unauthorized access

«CPN Tools» предоставляет несколько средств для анализа свойств рассматриваемой системы с использованием пространства состояний. Первоочередным обычно является создание отчёта о состоянии пространства, содержащего информацию о стандартных поведенческих свойствах модели CPN, таких как отсутствие или наличие взаимоблокировок, минимальное и максимальное количество маркеров в позициях.

Пользователь также может интерактивно отображать отдельные части пространства состояний и проверять отдельные состояния и события, что может стать эффективным способом отладки системы. «CPN Tool»s реализует набор функций, которые позволяют пользователю перемещаться по пространству состояний несколькими способами и тем самым исследовать свойства системы.

В пространстве состояний легко заметить, что все вершины имеют потомков, и сеть не является тупиковой. Таким образом, можно констатировать, что все компоненты подсистемы СЗИ от НСД «Вход в систему» взаимосвязаны между собой и исключают ситуацию блокировки.

Более полной информацией о пространстве состояний служит отображение имени сработавшего перехода на дуге между двумя узлами и маркировкой, соответствующей конкретно-

му узлу (в данном примере это узлы 10 и 12, рис. 4). Для отображения маркировки узла пространства состояний следует кликнуть левой кнопкой мыши на треугольнике соответствующего узла. Пространство состояний с отображением маркировок в узлах и сработавших переходов подсистемы «Вход в систему» СЗИ от НСД представлено на рис. 4.

Для проверки полученной сети на адекватность [27] осуществим необходимое количество шагов, в результате которых суммарное количество фишек в позициях «r2» и «r4», «r04» и «r6», «r5» и «r7» составит 50. В состояниях «r2» и «r4» — это 6 и 44 фишки (рис. 5), в состояниях «r04» и «r6» — 45 и 5 фишек (рис. 6), в состояниях «r5» и «r7» — 49 и 1 фишка (рис.7).

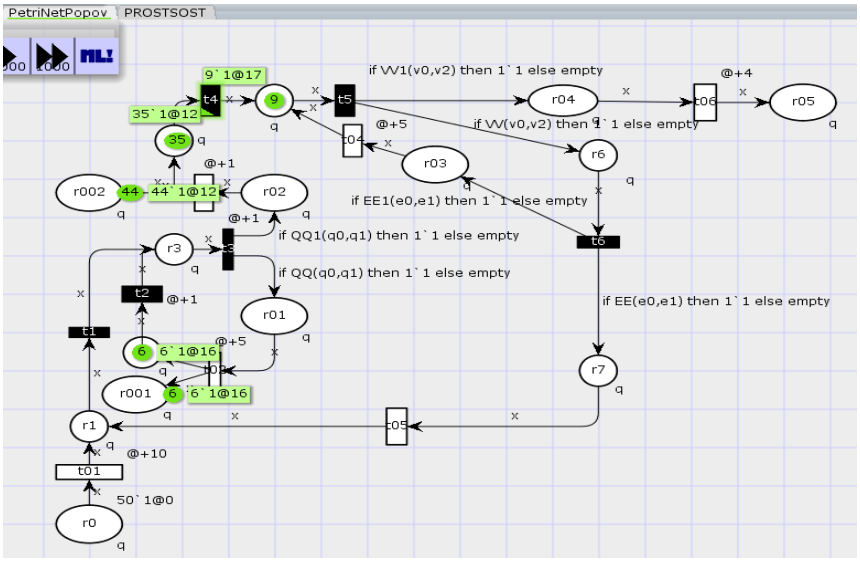

Рис. 5. Прогон модели для определения количества фишек в позициях «r2» и «r4»
Fig. 5. Run the model to determine the number of chips in the positions of "r2" and "r4"

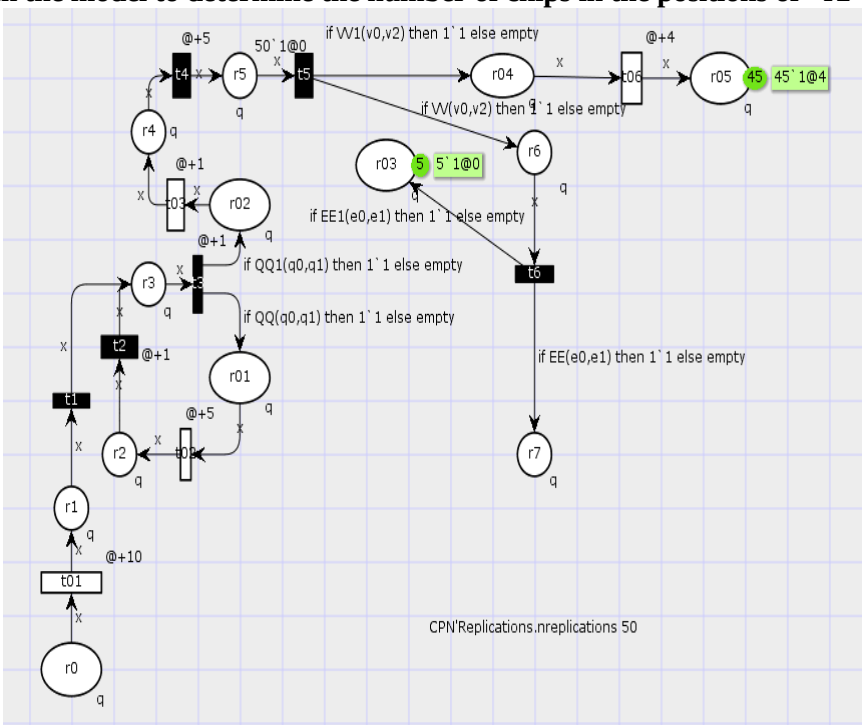

Рис. 6. Прогон модели для определения количества фишек в позициях «r04» и «r6»
Fig. 6. Run the model to determine the number of chips in the positions "r04" and "r6"

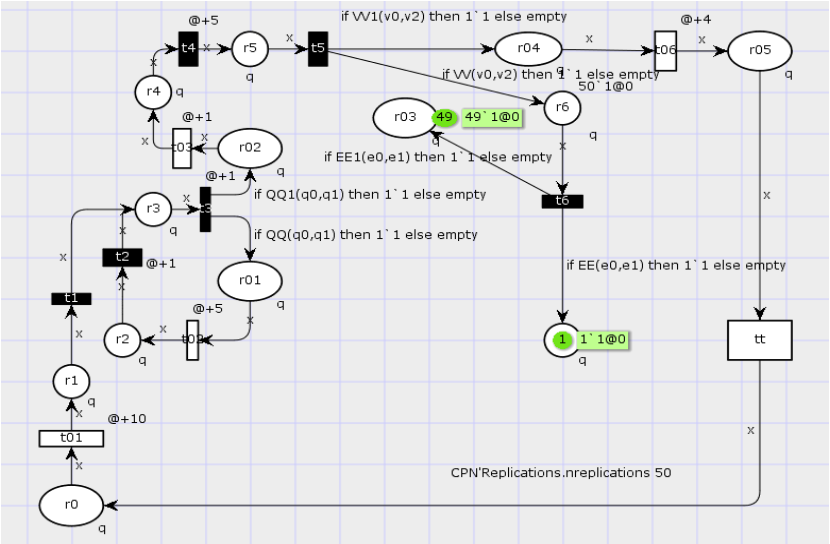

Рис. 7. Прогон модели для определения количества фишек в состояниях «r5» и «r7»
Fig. 7. Run the model to determine the number of chips in the "r5" and "r7" states

С учётом выше изложенного частоту появления фишек в состояниях «r2», «r6», «r7» определим, как:

$$p_{r2} = \frac{6}{50} = 0,12; p_{r6} = \frac{5}{50} = 0,1; p_{r7} = \frac{1}{50} = 0,02. \quad (1)$$

Вычислим с точностью $\varepsilon = 0,01$ и достаточностью $D = 0,99$ необходимое количество прогонов по сети N для вероятности появления события [27]:

$$N = \frac{p(1-p)}{\varepsilon^2}\left[\Phi_0^{-1}\frac{D}{2}\right]^2, \quad (2)$$

где Φ_0 — функция Лапласа.

Соответственно необходимое количество прогонов для позиций «r2», «r6», «r7» будет равно:

$$N_{r2} = \frac{0.12(1-0.12)}{0.01^2}2.58^2 = 7029,1584 \approx 7030;$$
$$N_{r6} = \frac{0.1(1-0.1)}{0.01^2}2.58^2 = 5990,76 \approx 5991; \quad (3)$$
$$N_{r7} = \frac{0.02(1-0.02)}{0.01^2}2.58^2 = 1034,6544 \approx 1035.$$

Для определения необходимого количества прогонов по сети для функционирования подсистемы СЗИ от НСД «Вход в систему» выбираем максимальное из трёх полученных значений, округляя его в большую сторону ($N = 7030$) (рис. 8).

При анализе производительности для сбора достоверных ВВХ функционирования СЗИ от НСД необходимо запустить несколько симуляций. Для осуществления автоматического запуска заданного количества симуляций может использоваться функция CPN'Replications.nreplications. При применении инструмента Evaluate ML к коду «CPN`Replications.nreplication 2» будут выполняться два моделирования (рис. 8).

Основная идея репликации моделирования в программной среде «CPN Tools» состоит в сборе оценок из набора независимых статистически идентичных симуляций, которые начинаются и останавливаются одинаково, используя при этом одни и те же входные параметры.

Две статистически идентичные симуляции временной модели функционирования подсистемы «Вход в систему» СЗИ от НСД начинаются в одинаковом начальном состоянии и останавливаются при выполнении одного и того же критерия останова. В представленной на рис. 8 модели таким данным критерием является то, что в поглощающее состояние должно прийти

7030 маркеров. Анализ производительности посредством автоматического моделирования, как было сказано выше, реализуется на основе данных из сформированных отчётов.

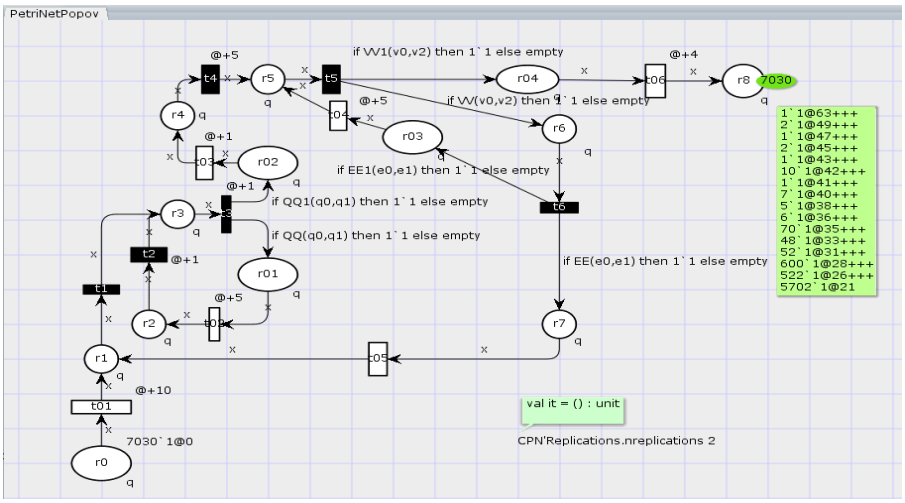

Рис. 8. Имитационная модель функционирования подсистемы «Вход в систему» СЗИ от НСД с необходимым количеством прогонов

Fig. 8. Simulation model of the functioning of the subsystem "Login" NWS from unauthorized access with the required number of runs

Идея данного анализа заключается в проведении нескольких симуляций имитационной модели, в ходе которых собираются данные о производительности системы. Обычно данные предоставляют информацию о нагрузке на различные состояния, вероятности попадания в состояние и т.д. Сбор данных осуществляется при помощи мониторов, которые указывают, какая именно информация будет собираться. Данные могут быть записаны в электронные таблицы файлов журналов для последующей их обработки и формирования отчётов об эффективности функционирования подсистемы с помощью средних значений, стандартного отклонения и доверительных интервалов.

При запуске симуляций моделирования создаются каталог вывода репликации и отчёт о её состоянии. Отчёт о моделировании репликации может быть сгенерирован, используя соответствующий инструмент, и содержит общую информацию о выполненных симуляциях в каталоге с именем «replication_report.txt». На рис. 9 представлен отчёт для двух повторений временной модели, в котором выделен раздел для каждой симуляции, определяющий количество смоделированных шагов, время модели и причину её остановки.

```
CPN Tools report for simulation replications
Net: /cygdrive/C/Users/Holmes/Desktop/IMMITACHIONNOE MODEL/CPN Tools1/SZI1/#Popov22222222222222222.cpn
Output directory: /cygdrive/C/Users/Holmes/Desktop/IMMITACHIONNOE MODEL/CPN Tools1/SZI1/output/reps_3

Simulation no.: 1
Steps.........: 54185
Model time....: 43
Stop reason...: No more enabled transitions!
Time to run simulation: 25 seconds


Simulation no.: 2
Steps.........: 54199
Model time....: 45
Stop reason...: No more enabled transitions!
Time to run simulation: 25 seconds
```

Рис. 9. Отчёт о репликации имитационной модели функционирования подсистемы «Вход в систему» СЗИ от НСД

Fig. 9. Report on replication of the simulation model of the operation of the subsystem "Login to the System" of GIS from unauthorized access

Вывод. В данной статье разработана имитационная модель процесса функционирования СЗИ от НСД в программной среде «CPN Tools» и обосновано количество её прогонов. По срав-

нению с другими видами моделей предложенная имитационная модель позволяет улучшить качество разработки и функционирования СЗИ от НСД в АС. Указанная модель необходима для проведения вычислительного эксперимента с целью анализа и исследования реальных потребительских свойств СЗИ от НСД в АС, а также для разработки программного комплекса анализа и количественной оценки эффективности функционирования системы. Результаты имитационного моделирования процесса функционирования СЗИ от НСД в АС могут быть представлены в виде различных характеристик каждого состояния, описывающих работу как системы в целом, так и её подсистем. Предложенная имитационная модель функционирования СЗИ от НСД в АС может использоваться как основа для построения моделей воздействия различных видов угроз [28, 29] информационному ресурсу АС согласно банку данных ФСТЭК России, а также для исследования ВВХ, влияющих на вычислительные ресурсы системы, а, следовательно, на эффективность её функционирования по прямому назначению.

Библиографический список:

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения // М.: Федеральное агентство по техническому регулированию и метрологии, 2006. — 12 с.
2. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Воениздат, 1992. 16 с.
3. ГОСТ Р 15408-2013. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. — М.: Стандартинформ, 2014. 152 с.
4. Математическая модель оценки эффективности систем защиты информации с использованием преобразования Лапласа и численного метода Гивенса / И.Г. Дровникова [и др.] // Труды СПИИРАН. № 3 (52) (2017). С.-Пб.: СПИИРАН, 2017. 2017. № 3(52). С. 234–258. DOI 10.15622/sp.52.
5. Беляева О.В. Имитационное моделирование систем защиты информации / О.В. Беляева, В.А. Грицык // Международный журнал экспериментального образования. 2010. № 5. С. 67.
6. Григорьев В.А. Имитационная модель системы защиты информации / В.А. Григорьев, А.В. Карпов // Программные продукты и системы. 2005. № 2. С. 26–30.
7. «Страж NT». Руководство администратора. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (дата обращения: 23.07.2018).
8. Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. URL: http://www.rubinteh.ru/public/opis30.pdf (дата обращения: 23.07.2018).
9. Charaf H. A colored Petri-net model for control execution of distributed systems / H. Charaf, S. Azzouzi // 4th International Conference on Control, Decision and Information Technologies (CoDIT). 2017. pp. 277–282.
10. Меньших В.В. Получение оценок эффективности системы защиты информации с использованием автоматной модели имитации функционирования защищённой информационной системы / В.В. Меньших, Е.В. Петрова // Информация и безопасность. 2011. Т. 14. № 1. С. 125–128.
11. Jasiul B. Detection and Modeling of Cyber Attacks with Petri Nets / B. Jasiul, M. Szpyrka, J. Sliwa // Entropy. 2014. Vol. 16. Issue 12. pp. 6602–6623.
12. Network security analyzing and modeling based on Petri net and Attack tree for SDN / Y. Linyuan [and others] // 2016 International Conference on Computing, Networking and Communications (ICNC). — 2016. pp. 133–187.
13. Павловский Ю.Н. Имитационные модели и системы / Ю.Н. Павловский. — М.: Фазис: ВЦ РАН, 2000. С. 134.
14. Краснощёков П.С. Оптимизация в автоматизированном проектировании / П.С. Краснощёков, В.В. Морозов, Н.М. Попов. М.: МАКС Пресс, 2008. 323 с.
15. Nikishin K. Implementation of time-triggered ethernet using colored Petri NET / K. Nikishin, N. Konnov, D. Pashchenko // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2017. pp. 1–5.
16. Korniyenko B.Y. Design and research of mathematical model for information security system in computer network / B.Y. Korniyenko, L.P. Galata // Science-Based Technologies. 2017. Vol. 34. Issue 2. pp. 114–118.
17. White S.C. Comparison of Security Models: Attack Graphs Versus Petri Nets / S.C. White, S.S. Sarvestani // Advances in Computers. 2014. vol. 94. — pp. 1–24.
18. Исхаков С.Ю. Имитационная модель комплексной сети систем безопасности / С.Ю. Исхаков, А.А. Шелупанов, А.Ю. Исхаков // Управление, вычислительная техника и информатика. Доклады ТУСУРа. — 2014. — Вып. 2 (32). — С. 82–86.
19. Yang N. Modeling and quantitatively predicting software security based on stochastic Petri nets / N. Yang, H. Yu, Z. Qian, H. Sun // Mathematical and Computer Modelling. — 2012. — Vol. 55. — Issues 1–2. — pp.102–112.
20. Klaic A. Conceptual Modeling of Information Systems within the Information Security Policies / A. Klaic, M. Golub // Journal of Economics / Business and Management. — 2013. — vol. 1. — Issue 4. — pp. 371–376.

21. Nazareth D. System dynamics model for information security management / D. Nazareth, J. Choi // Information & Management. 2015. vol. 52. Issue 1. — pp. 123–134.
22. Complex Event Processing Modeling by Prioritized Colored Petri Nets / H. Macià [and others] // IEEE Access. 2016. — vol 4. pp. 7425–7439.
23. Стельмашонок Е.В. Возможности имитационного моделирования для исследования функционирования системы защиты информации / Е.В. Стельмашонок, В.Л. Стельмашонок // Петербургский экономический журнал. 2017. №4. С. 57–68.
24. Алгоритм имитационной модели противодействия несанкционированному доступу к автоматизированной информационной системе специального назначения средствами защиты информации / С.С. Кочедыков [и др.] // Математические методы и информационные технологии управления в науке, образовании и правоохранительной сфере. 2017. С. 98–103.
25. Бугров Ю.Г. Повышение качества имитационной модели системы защиты информации / Ю.Г. Бугров, В.В. Мирошников, Д.В. Кочергин // Информация и безопасность. 2008. Т. 11. № 1. С. 69–73.
26. Рогозин Е.А. Модель функционирования типовой системы защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД / Е.А. Рогозин, А.Д. Попов // Вестник Воронежского института МВД России. 2016. № 4. С. 122–132.
27. Синегубов С.В. Моделирование систем и сетей телекоммуникаций / С.В. Синегубов. Воронеж: Воронеж. ин-т МВД России, 2016. — 336 с.
28. Моделирование многоуровневых систем защиты информации REDS / А.В. Володько [и др.] // Телекоммуникационные устройства и системы. 2014. С. 423–426.
29. Климов С.М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак / С.М. Климов // Известия ЮФУ. Технические науки. 2016. № 8 (181). С. 27–36.

References:

1. GOST R 50922-2006. Zashchita informatsii. Osnovnyye terminy i opredeleniya // M.: Federal'noye agentstvo po tekhnicheskomu regulirovaniyu i metrologii, 2006. — 12 c. [GOST R 50922-2006. Data protection. Basic terms and definitions. — M.: Federal'noe agentstvo po tekhnicheskomu regulirovaniyu i metrologii, 2006. 12 p. (in Russ)].
2. FSTEK RF. Rukovodyashchiy dokument. Avtomatizirovannyye sistemy. Zashchita ot nesanktsionirovan-nogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii. — M.: Voyenizdat, 1992. — 16 s. [FSTEC RF. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for information security. — M.: Military Publishing, 1992. — 16 p. (in Russ)].
3. GOST R 15408-2013. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. M.: Standartinform, 2014. 152 c [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. M.: STANDARTINFORM, 2014. 152 p. (in Russ)].
4. Matematicheskaya model' otsenki effektivnosti sistem zashchity informatsii s ispol'zovaniyem pre-obrazovaniya Laplasa i chislennogo metoda Givensa / I.G. Drovnikova [i dr.] // Trudy SPIIRAN. № 3 (52) (2017). S.-Pb.: SPIIRAN, 2017. 2017. № 3(52). S. 234–258. DOI 10.15622/sp.52. [Mathematical model for estimating the efficiency of information security systems by means of Laplace transformation and Givens method / I.G. Drovnikova [and others] // Trudy SPIIRAN — SPIIRAS Proceedings. 2017. Vol. 3(52). pp. 234–258 (in Russ)].
5. Belyayeva O.V. Imitatsionnoye modelirovaniye sistem zashchity informatsii / O.V. Belyayeva, V.A. Gritsyk // Mezhdunarodnyy zhurnal eksperimental'nogo obrazovaniya. 2010. № 5. S. 67. [Belyaeva O.V. Simulation modeling of information security systems / O.V. Belyaeva, V.A. Gricyk // Mezhdunarodnyj zhurnal ehksperimental'nogo obrazovaniya. 2010. vol 5. pp. 67 (in Russ)]
6. Grigor'yev V.A. Imitatsionnaya model' sistemy zashchity informatsii / V.A. Grigor'yev, A.V. Karpov // Programmnyye produkty i sistemy. 2005. № 2. S. 26–30. [Grigor'ev V.A. Simulation model of information security system / V.A. Grigor'ev, A.V. Karpov // Programmnye produkty i sistemy. 2005. Vol. 2. pp. 26–30 (in Russ)].
7. «Strazh NT». Rukovodstvo administratora. «The Guardian NT». [Administrator's guide. Available at: http://www.rubinteh.ru/public/opis30.pdf (accessed 23.07.2018) (in Russ)].
8. Sistema zashchity informacii ot nesankcionirovannogo dostupa «Strazh NT». Opisanie primeneniya. [System of protection of information from unauthorized access «Guardian NT». Description of the application. Available at: http://www.guardnt.ru/download/doc/admin_ guide_nt_3_0.pdf (accessed 23.07.2018) (in Russ)].
9. Charaf H. A colored Petri-net model for control execution of distributed systems / H. Charaf, S. Azzouzi // 4th International Conference on Control, Decision and Information Technologies (CoDIT). 2017. pp. 277–282.
10. Men'shikh V.V. Polucheniye otsenok effektivnosti sistemy zashchity informatsii s ispol'zovaniyem avtomatnoy modeli imitatsii funktsionirovaniya zashchishchonnoy informatsionnoy sistemy / V.V. Men'shikh, Ye.V. Petrova // Informatsiya i bezopasnost'. 2011. T. 14. № 1. S. 125–128.Men'shih V.V. Obtaining assessments of the effectiveness of the information security system using the automatic model of simulating the functioning of a secure in-

formation system / V.V. Men'shih, E.V. Petrova // Informaciya i bezopasnost'. 2011. vol. 16. Issue 1. pp. 125–128 (in Russ)].

11. Jasiul B. Detection and Modeling of Cyber Attacks with Petri Nets / B. Jasiul, M. Szpyrka, J. Sliwa // Entropy. 2014. vol. 16. Issue 12. pp. 6602–6623.
12. Network security analyzing and modeling based on Petri net and Attack tree for SDN / Y. Linyuan [and others] // 2016 International Conference on Computing, Networking and Communications (ICNC). — 2016. pp. 133–187.
13. Pavlovskiy YU.N. Imitatsionnyye modeli i sistemy / YU.N. Pavlovskiy. — M.: Fazis: VTS RAN, 2000. — S. 134. [Pavlovsky Yu. N. Simulation models and systems / Yu. N. Pavlovsky. M.: Fazis: VC RAN, 2000. 134 p. (in Russ)].
14. Krasnoshchokov P.S. Optimizatsiya v avtomatizirovannom proyektirovanii / P.S. Krasnoshchokov, V.V. Morozov, N.M. Popov. M.: MAKS Press, 2008. 323 s. [Krasnoshchekov P.S. Optimization in computer-aided design / P.S. Krasnoshchekov, V.V. Morozov, N.M. Popov. M.: MAKS Press.] 2008.] 323 p. (in Russ)].
15. Nikishin K. Implementation of time-triggered ethernet using colored Petri NET / K. Nikishin, N. Konnov, D. Pashchenko // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM).]2017. Pp. 1–5.
16. Korniyenko B.Y. Design and research of mathematical model for information security system in computer network / B.Y. Korniyenko, L.P. Galata // Science-Based Technologies. 2017. Vol. 34. Issue 2. pp. 114–118.
17. White S.C. Comparison of Security Models: Attack Graphs Versus Petri Nets / S.C. White, S.S. Sarvestani // Advances in Computers. 2014. Vol. 94. pp. 1–24.
18. Iskhakov S.YU. Imitatsionnaya model' kompleksnoy seti sistem bezopasnosti / S.YU. Iskhakov, A.A. Shelupanov, A.YU. Iskhakov // Upravleniye, vychislitel'naya tekhnika i informatika. Doklady TU-SURa. 2014. Vyp. 2 (32). C. 82–86. [Iskhakov S.Yu. Simulation model of an integrated network of security systems / S.Yu. Iskhakov, A.A. SHelupanov, A.Yu. Iskhakov // Upravlenie, vychislitel'naya tekhnika i informatika. Doklady TUSURa. 2014. Vol. 32. Issue 2. pp. 82–86 (in Russ)]
19. Yang N. Modeling and quantitatively predicting software security based on stochastic Petri nets / N. Yang, H. Yu, Z. Qian, H. Sun // Mathematical and Computer Modelling. 2012. Vol. 55. Issues 1–2. Pp. 102–112.
20. Klaic A. Conceptual Modeling of Information Systems within the Information Security Policies / A. Klaic, M. Golub // Journal of Economics/ Business and Management. 2013. Vol. 1. Issue 4. Pp. 371–376.
21. Nazareth D. System dynamics model for information security management / D. Nazareth, J. Choi // Information & Management. 2015. Vol. 52. Issue 1. pp. 123–134.
22. Complex Event Processing Modeling by Prioritized Colored Petri Nets / H. Macià [and others] // IEEE Access. 2016. vol 4. Pp. 7425–7439.
23. Stel'mashonok Ye.V. Vozmozhnosti imitatsionnogo modelirovaniya dlya issledovaniya funktsioniro-vaniya sistemy zashchity informatsii / Ye.V. Stel'mashonok, V.L. Stel'mashonok // Peterburgskiy ekonomicheskiy zhurnal. 2017. №4. S. 57–68. [Stel'mashonok E.V. The possibilities of simulation for the study of the functioning of the information security system / E.V. Stel'mashonok, V.L. Stel'mashonok // Peterburgskij ehkonomicheskij zhurnal. 2017. vol. 4. Pp. 57–68 (in Russ)].
24. Algoritm imitatsionnoy modeli protivodeystviya nesanktsionirovannomu dostupu k avtomatiziro-vannoy informatsionnoy sisteme spetsial'nogo naznacheniya sredstvami zashchity informatsii / S.S. Kochedykov [i dr.] // Matematicheskiye metody i informatsionnyye tekhnologii upravleniya v nauke, obrazovanii i pravookhranitel'noy sfere. 2017. S. 98–103. [Algorithm of the simulation model of counteraction to unauthorized access to an automated information system of a special purpose by means of information security / S.S. Kochedykov [and otheres] // Matematicheskie metody i informacionnye tekhnologii upravleniya v nauke, obrazovanii i pravoohranitel'noj sfere. 2017. pp. 98–103 (in Russ)].
25. Bugrov YU.G. Povysheniye kachestva imitatsionnoy modeli sistemy zashchity informatsii / YU.G. Bug-rov, V.V. Miroshnikov, D.V. Kochergin // Informatsiya i bezopasnost'. 2008. T. 11. № 1. S. 69–73. [Bugrov Yu.G. Improving the quality of the simulation model of the information security system / Yu.G. Bugrov, V.V. Miroshnikov, D.V. Kochergin // Informaciya i bezopasnost'. 2008. Vol. 11. Issue 1. Pp. 69–73 (in Russ]
26. Rogozin Ye.A. Model' funktsionirovaniya tipovoy sistemy zashchity informatsii ot nesanktsioniro-vannogo dostupa v avtomatizirovannykh informatsionnykh sistemakh OVD / Ye.A. Rogozin, A.D. Popov // Vestnik Voronezhskogo instituta MVD Rossii. 2016. № 4. S. 122–132. [Rogozin E.A. Model operation of the standard information system of protection against unauthorized access to automated information systems of the Law Enforces Agencies / E.A. Rogozin, A.D. Popov // Vestnik Voronezhskogo instituta MVD Rossii — Bulletin of the Voronezh Institute of the Ministry of the Interior of Russia. 2016. № 4. Pp. 122–132 (in Russ)]
27. Sinegubov S.V. Modelirovaniye sistem i setey telekommunikatsiy / S.V. Sinegubov. Voronezh: Voronezh. in-t MVD Rossii, 2016. 336 s. [Sinegubov S.V. Modelirovanie sistem i setej telekommunikacij / S.V. Sinegubov— Voronezh: Voronezh. Institute of MIA of Russia. 2016. 336 p. (in Russ)]
28. Modelirovaniye mnogourovnevykh sistem zashchity informatsii REDS / A.V. Volod'ko [i dr.] // Telekommunikatsionnyye ustroystva i sistemy. 2014. S. 423–426. [Modeling of multi-level information security systems REDS / A.V. Volod'ko [and others] // Telekommunikacionnye ustrojstva i sistemy. 2014. Pp. 423–426 (in Russ)]

29. Klimov S.M. Imitatsionnyye modeli ispytaniy kriticheski vazhnykh informatsionnykh ob"yektov v usloviyakh komp'yuternykh atak / S.M. Klimov // Izvestiya YUFU. Tekhnicheskiye nauki. 2016. № 8 (181). S. 27–36. [Klimov S.M. Simulation models of testing critical information objects in conditions of computer attacks / S.M. Klimov // Izvestiya YUFU. Tekhnicheskie nauki. 2016. Vol. 181 Issue 1. pp. 27–36 (in Russ)]

Сведения об авторах:

Бокова Оксана Игоревна — доктор технических наук, профессор, заместитель начальника Воронежского института МВД России по научной работе.

Дровникова Ирина Григорьевна — доктор технических наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России.

Попов Антон Дмитриевич — преподаватель кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России.

Рогозин Евгений Алексеевич — доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России.

Information about the authors:

Oksana I. Bokova – Dr.Sci. (Technical), Prof., Deputy Head of the Voronezh Institute of the Ministry of Internal Affairs of Russia for Scientific Work.

Irina G. Drovnikova – Dr. Sci. (Technical), Prof., Department of Automated Information Systems of Internal Affairs.

Anton D. Popov – Lecturer at the Department of Automated Information Systems of Internal Affairs Agencies

Evgeny A. Rogozin - Dr. Sci. (Technical), Prof., Department of Automated Information Systems of Internal Affairs.

Конфликт интересов
Авторы заявляют об отсутствии конфликта интересов.
Поступила в редакцию 15.12.2018.
Принята в печать 30.01.2019.

Conflict of interest.
The authors declare no conflict of interest.
Received 15.12.2018.
Accepted for publication 30.01.2019.