Оксана И. Бокова[1], Дмитрий И. Коробкин[2], Сергей А. Кухарев[3], Антон Д. Попов[4]
[1, 3, 4]Воронежский институт Министерства внутренних дел Российской Федерации,
просп. Патриотов, 53, г. Воронеж, 394065, Россия
[2]Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина,
ул. Ст. Большевиков, 54а, г. Воронеж, 394016, Россия
[1]e-mail: o.i.bokova@gmail.com, https://orcid.org/0000-0002-4833-2907
[2]e-mail: 516420@mail.ru, https://orcid.org/0000-0002-8236-5534
[3]e-mail: cuharev.serj@yandex.ru, https://orcid.org/0000-0002-9633-8422
[4]e-mail: anton.holmes@mail.ru, https://orcid.org/0000-0002-6583-102X

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ СРЕДЫ CPN TOOLS

DOI: http://dx.doi.org/10.26583/bit.2019.3.07

Аннотация. В статье с помощью имитационного моделирования представлена математическая модель функционирования системы защиты информации (СЗИ) от несанкционированного доступа (НСД) в автоматизированных системах (АС). Данная модель разработана в программной среде CPN Tools с целью дальнейшего ее анализа. Для удобства, наглядности и сохранения логической целостности, модель разбита на подсистемы при помощи встроенного в CPN Tools инструментария. Модель необходима для проведения вычислительного эксперимента, а именно исследования реальных потребительских свойств СЗИ от НСД в АС, а также для разработки программного комплекса анализа и количественной оценки эффективности функционирования этих систем. Результаты имитационного моделирования процесса функционирования СЗИ от НСД в АС могут быть представлены в виде различных характеристик каждого состояния, которые характеризуют работу как системы в целом, так и ее подсистем. Разработанная имитационная модель может быть использована при создании подобных систем, при их эксплуатации, при сертификации систем информационной безопасности, при аттестации объектов информатизации и при периодическом контроле используемых программных средств защиты информации на данных объектах. Используемый CPN Tools язык программирования Meta language позволяет контролировать случайный переход маркера из начального состояния в конечное через промежуточное, устанавливать временные задержки и др. Имитационная модель СЗИ от НСД в АС в дальнейших исследованиях будет использоваться для построения моделей воздействия различных видов угроз к данной системе согласно банку данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации.

Ключевые слова: CPN Tools, сети Петри, система защиты информации, несанкционированный доступ, имитационная модель, автоматизированная система, strongly connected components.
Для цитирования: БОКОВА, Оксана И. et al. РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ СРЕДЫ CPN TOOLS. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 80-89, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1220>. Дата доступа: 17 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.07.

Oksana I. Bokova[1], Dmitry I. Korobkin[2], Sergey A. Kukharev[3], Anton D. Popov[4]
[1, 3, 4]Voronezh Institute of the Interior,
Prospect Patriotov, 53, Voronezh, 394065, Russia
[2]N.E. Zhukovsky and Y.A. Gagarin Air Force Academy,
Str. Bolsheviks, 54 a, Voronezh, 394016, Russia
[1]e-mail: o.i.bokova@gmail.com, https://orcid.org/0000-0002-4833-2907
[2]e-mail: 516420@mail.ru, https://orcid.org/0000-0002-8236-5534
[3]e-mail: cuharev.serj@yandex.ru, https://orcid.org/0000-0002-9633-8422
[4]e-mail: anton.holmes@mail.ru, https://orcid.org/0000-0002-6583-102X

Development of an imitation model of information protection system from unauthorized access using the cpn tools software

DOI: http://dx.doi.org/10.26583/bit.2019.3.07

Abstract. The paper presents a mathematical model of functioning of the system of information protection (IPS) from unauthorized access (UA) in automated systems (AS). This model was developed in framework of the CPN Tools software environment. For convenience, visibility and preservation of logical integrity, the model is divided into subsystems using the tools built into CPN Tools. The model is necessary for a computational experiment, namely, to study the real consumer properties of IPS from UA in AS, as well as for development a software package for analyzing and quantifying the effectiveness of these systems. The results of the simulation of functioning of the IPS from the UA in the AS can be presented in the form of various characteristics of each state, which characterize the work of the system as a whole and its subsystems. The developed simulation model can be used to create similar systems, during their operation, during certification of information security systems, during certification of informatization facilities, and during periodic monitoring of used information protection software at these facilities. The programming language Meta language used by CPN Tools allows you to monitor random transitions of the marker from the initial state to the final through the intermediate one, to set time delays, etc. The simulation model of IPS from UA to AS will be used in further studies to build the models of impact of various types of threats to this system according to the bank data threats to information security of the Federal Service for Technical and Export Control of Russia.

Keywords: CPN Tools, Petri nets, information protection system, unauthorized access, simulation model, automated system, strongly connected components.

For citation: BOKOVA, Oksana I. et al. Development of an imitation model of information protection system from unauthorized access using the cpn tools software. IT Security (Russia), [S.l.], v. 26, n. 3, p. 80-89, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1220>. Date accessed: 17 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.07.

Введение

Современный этап жизнедеятельности человека характеризуется глубокой информатизацией, которая связана с разработкой, эксплуатацией АС различного назначения. В связи с этим злоумышленниками постоянно совершенствуются способы получения конфиденциальной информации. Для предотвращения попыток НСД в АС внедряются СЗИ от НСД [1, 2]. Зачастую штатные пользователи таких систем пренебрегают своими должностными полномочиями и нарушают правила работы с защищенными системами. Пользовательские ошибки являются самыми распространенными, поэтому в работе допускаем, что была допущена ошибка и вредоносная программа проникла в АС [3]. Будем считать, что нарушитель является внутренним с высоким потенциалом. Рассмотрим именно этот случай для съемного носителя информации CD/DVD/HD/Flesh.

Вредоносная программа может быть реализована в виде отдельного программного продукта (ПП) с функцией автозапуска при подключении к персональному компьютеру (ПК) в случае, когда пользователь сам отключает антивирусное программное обеспечение (ПО), т.к. зачастую АС потребляют большое количество ресурсов, и следовательно, работать становится неудобно, а зачастую невозможно из-за сильной загруженности [3].

Данные аспекты необходимо учитывать при разработке и эксплуатации СЗИ от НСД для определения ее вероятностно-временных характеристик в виде времен выполнения защитных функций, которые в дальнейшем планируется использовать при оценке эффективности ее функционирования [4], для установки взаимосвязей ее подсистем и компонентов, а также построения её логической структуры в целом. Данная задача может быть решена при помощи построения имитационной модели СЗИ от НСД, которая и будет предопределять вышеперечисленные характеристики.

В качестве программной среды построения имитационной модели в данной статье используем программу, разработанную в университете Орхуса (Дания) – CPN Tools [4-8]. Отличительной особенностью CPN Tools является наличие обширного инструментария, позволяющего анализировать различные аспекты функционирования моделей на базе сетей Петри [9-10] (безопасность и ограниченность позиций, уровень активности переходов, наличие тупиковых маркировок и т.д.). CPN Tools используется во множестве реальных проектов в области телекоммуникации, при моделировании сетей и сетевых устройств, при верификации протоколов связи и т.д. В данной среде для построения моделей используются иерархические, временные, раскрашенные сети Петри, которые представляют собой универсальную алгоритмическую систему. Имитационное моделирование в CPN Tools является дискретно-событийным, что предполагает мгновенную смену состояния сети Петри в определенные моменты времени.

Построение модели

Моделирование СЗИ от НСД представляет собой сложный процесс. Первоначальным этапом разработки модели является построение ее подсистем и их компонентов, полностью идентичных реально функционирующей СЗИ от НСД с целью получения ее свойств и характеристик [1, 2, 11-15]. Проведенный анализ показал, что модель может состоять из следующих подсистем:

- подсистема «Включение ПК и идентификация пользователя»;
- подсистема «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов»;
- подсистема «Работа пользователя с файлами и программами»;
- подсистема «Работа пользователя с прикладным программным обеспечением»;
- подсистема «Деструктивное воздействие на СЗИ от НСД».

Введем следующие обозначения для вершин и переходов. Вершины в нашей модели используются двух видов – с индексами r1 и т.д., представляют собой функции, выполняемые СЗИ от НСД, а вершины с индексами r01 и т.д. являются дополнительными, требующимися для ввода вероятностей. И, соответственно, переходы с индексами t1 и т.д. являются основными, а t01 и т.д. являются дополнительными.

Первая модель отображает вход пользователя в СЗИ от НСД посредством его аутентификации (рис. 1). Данная модель даёт визуальное представление о том, что происходит в системе при входе пользователя. Из рисунка 1 видно, что при неправильном вводе пароля (после третьего раза) следует блокировка ПК, что позволяет обеспечить защиту ПК от брутфорса. Переход t01 обеспечивает передачу маркера в подсистему «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов в системе». В таблице 1 приведены состояния рассматриваемой подсистемы.

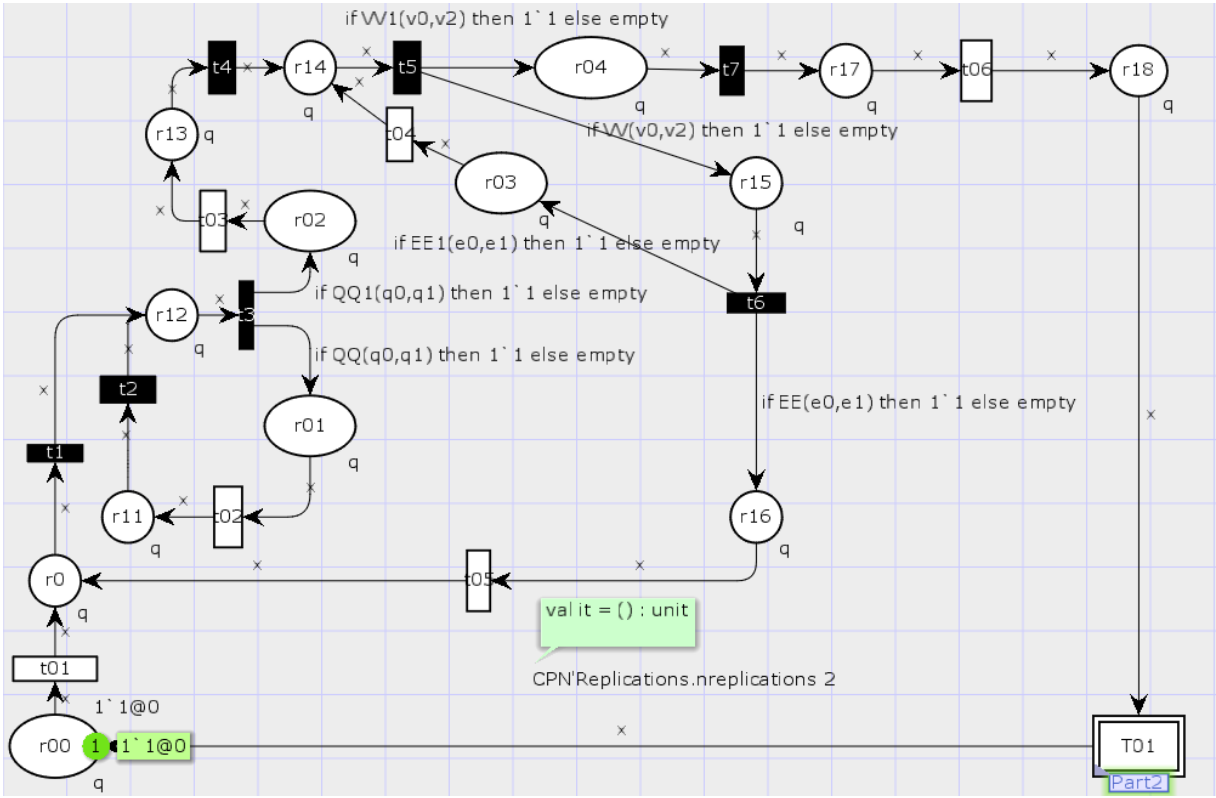

Рис. 1. Включение ПК и идентификация пользователя
(Fig. 1. Turning on the PC and identifying the user)

Таблица 1. Включение ПК и идентификация пользователя

Функции, выполняемые СЗИ от НСД
0. Начало работы СЗИ от НСД (Прекращение выполнения функций СЗИ от НСД)
1.1 Предъявление идентификатора
1.2 Прекращение работы идентификатора
1.3 Допуск к вводу пароля
1.4 Ввод пароля
1.5 Повторный ввод пароля
1.6 Блокировка входа в систему при трехразовом неправильном вводе пароля
1.7 Аутентификация субъекта системы
1.8 Вход в систему

Вторая модель отображает подсистему «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов» (рис. 2). В позиции r241 реализуется вход из подсистемы «Деструктивное воздействие на СЗИ от НСД». После перехода пользователя к работе с носителем вредоносная программа автоматически запускается, и в имитационной модели появляется новый «маркер», который представляет собой деструктивное программное воздействие на СЗИ от НСД, направленное на получение доступа к информации. В таблице 2 приведены состояния рассматриваемой подсистемы.

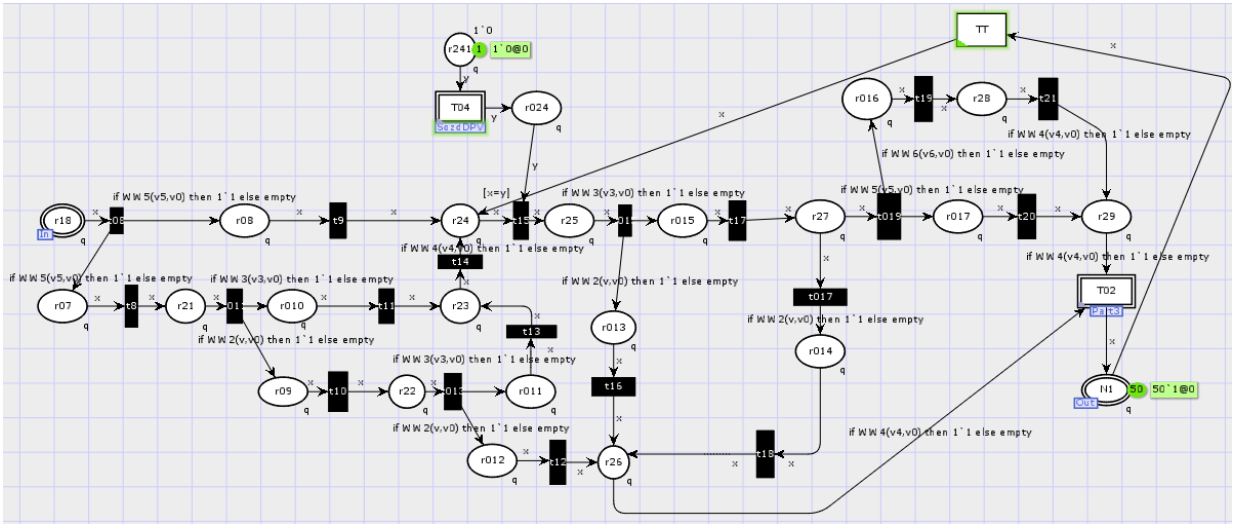

Рис. 2. Инициализация прав пользователя на работу в системе и доступ к каталогу файлов (Fig. 2. Initialization of user rights to work in the system and access to the file directory)

Таблица 2. Инициализация прав пользователя на работу в системе и доступ к каталогу файлов

Функции, выполняемые СЗИ от НСД
1.8 Вход в систему
2.1 Сопоставление идентификационной информации внешнего носителя и пользователя
2.2 Контроль устройств (если устройство не принадлежит пользователю, срабатывает данный механизм)
2.3 Доступ к внешнему носителю
2.4 Обращение к объекту на носителе
2.5 Сопоставление меток конфиденциальности пользователя и ресурса (в СЗИ от НСД реализуется на основе мандатного принципа контроля доступа)
2.6 Блокировка доступа к объекту
2.7 Проверка полномочий доступа пользователя (в СЗИ от НСД реализуется на основе дискреционного принципа контроля доступа)
2.8 Преобразование информации на носителе при помощи шифрования (в СЗИ от НСД применяется метод гаммирования)
2.9 Допуск субъекта к защищаемому объекту

Следующая модель подсистемы СЗИ от НСД описывает работу пользователя с отдельными объектами (рис. 3), она основана на принципе разграничения доступа по аутентификации пользователя и ограничения его прав доступа к отдельным объектам системы. В случае если пользователю запрещено работать с отдельными объектами, то СЗИ от НСД блокирует доступ к объекту и записывает информацию о данном факте в журнале событий. Это помогает выявлять факты НСД пользователя к объектам, к которым он не имеет доступа. Данный функционал заложен во вредоносную программу для того, чтобы провести имитацию реакции СЗИ от НСД на действия злоумышленника. В вершине r29 реализован переход на подсистему «Работа пользователя с прикладными программными продуктами», которая моделирует работу пользователя с отдельными ПП.

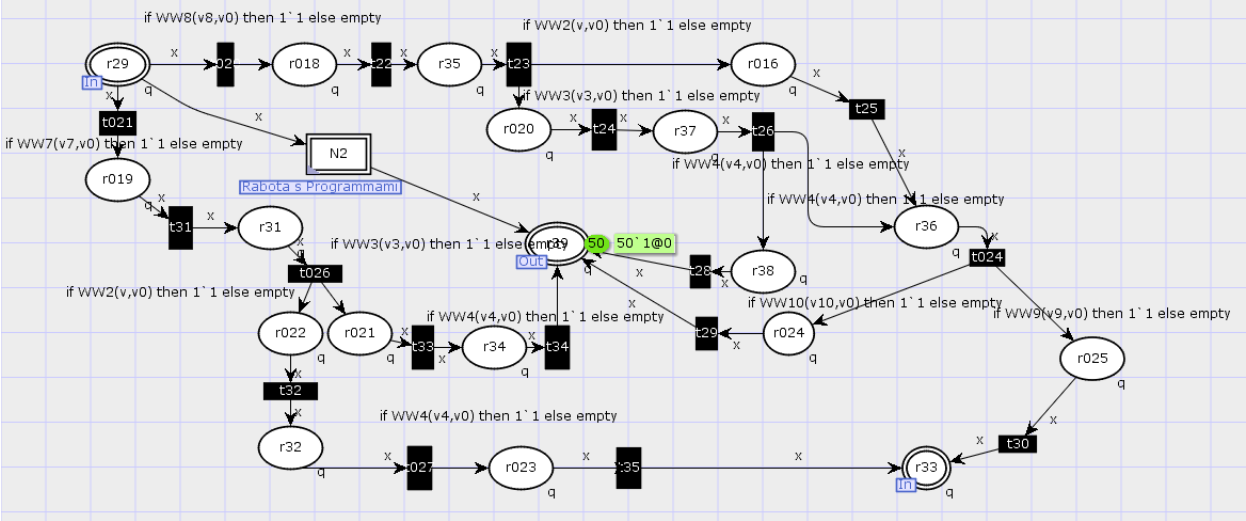

Рис. 3. Работа пользователя с файлами и программами
(Fig. 3. User work with files and programs)

Таблица 3. Работа пользователя с файлами и программами

Функции, выполняемые СЗИ от НСД
2.9 Допуск субъекта к защищаемому объекту
3.1 Запрос на преобразование объекта
3.2 Блокировка преобразования объекта
3.3 Регистрация нарушений работы с СЗИ от НСД
3.4 Пересчет параметров целостности файла
3.5 Запрос на удаление
3.6 Блокировка удаления
3.7 Преобразование объекта перед удалением
3.8 Удаление объекта
3.9 Завершение работы с объектом

Модель подсистемы «Работа пользователя с прикладными программными продуктами» (рис. 4) включает в себя наиболее распространенное ПО. Данная подсистема взаимодействует с подсистемой «Работа пользователя с файлами и программами», соединительной вершиной между ними является r411. Необходимо отметить, что в модели мы рассматриваем работу только с одним ПП, без возможности использовать другие программы параллельно. Данная система отражает работу пользователя с типовым составом ПП, в частности, с такими как Microsoft Office, ABBY Fine Reader, Nero, WinRar, Total Commarder.

Модель «Деструктивное воздействие на СЗИ от НСД» (рис. 5) описывает действия злоумышленника по внедрению вредоносной программы посредством накопленных у него сведений о системе. Предварительный сценарий вредоносного воздействия злоумышленника на защищенный информационный ресурс АС разработан на основе анализа угроз, представленных в банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации.

Вывод данной модели осуществлён в вершину r24 «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов», которая отображает работу пользователя с внешним носителем информации.

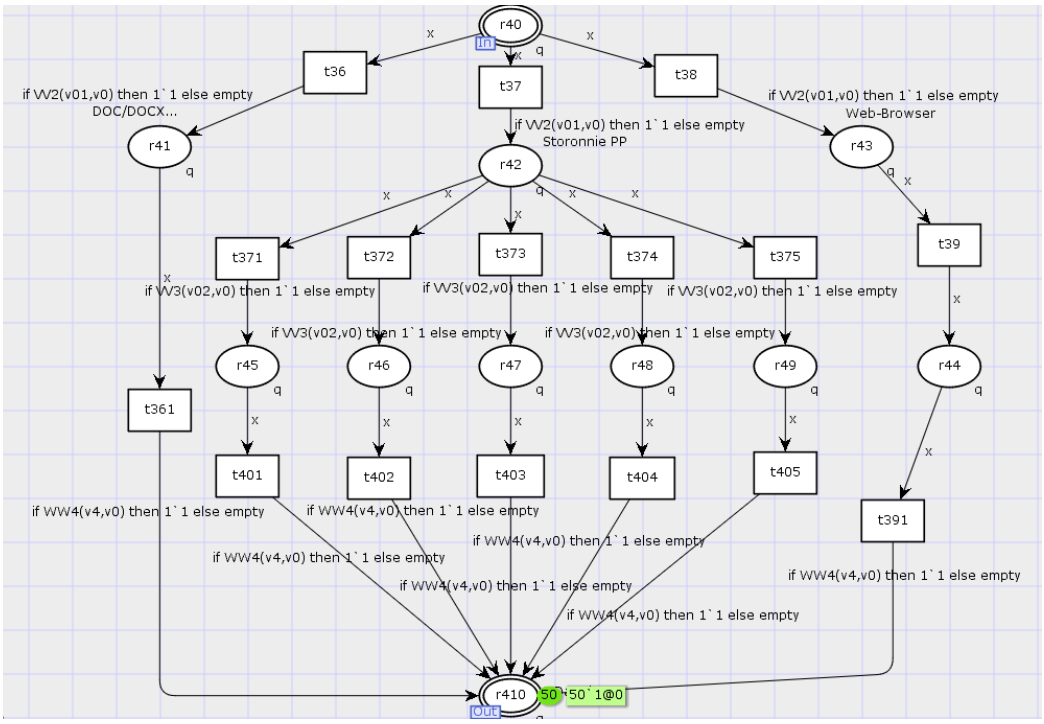

Рис. 4. Работа пользователя с файлами и программами
(Fig. 4. User work with files and programs)

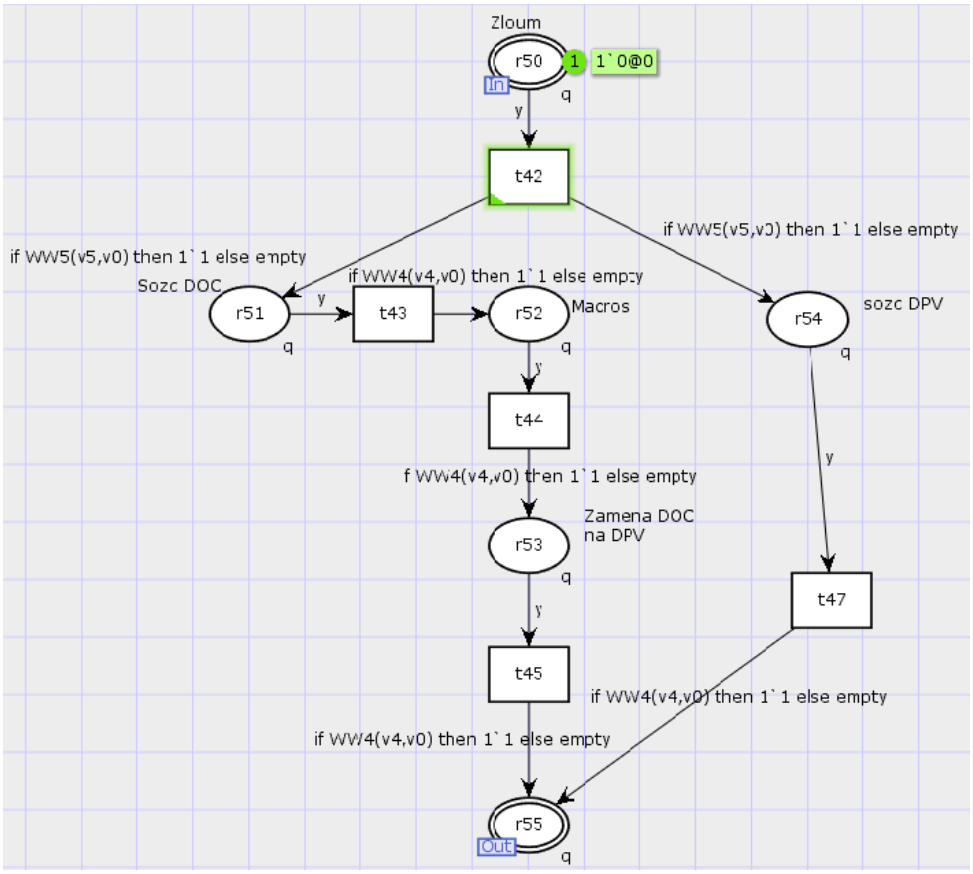

Рис. 5. Деструктивное воздействие на средства защиты информации
от несанкционированного доступа
(Fig. 5. Destructive impact on the means of information protection from unauthorized access)

Таблица 4. Работа пользователя с файлами и программами

Функции, выполняемые СЗИ от НСД
4 Начало работы с программами
4.1 Работа с документами
4.2 Работа с отдельным ПО
4.3 Работа с браузером и в сети (локальной/глобальной)
4.4 Использование различных серверов в Интернете
4.5 Работа с ПП Microsoft Office
4.6 Работа с ПП ABBY Fine Reader
4.7 Работа с ПП Nero
4.8 Работа с ПП WinRar
4.9 Работа с ПП Total Commarder
4.10 Работа с ПП Lock
4.11 Полученные в ходе работы данные или действия с отдельными обьектами (файлами/папками)

Таблица 5. Деструктивное воздействие на СЗИ от НСД

Деструктивное воздействие злоумышленника на информационный ресурс АС (предварительный сценарий)
5 Действия злоумышленника
5.1 Создание документа
5.2 Создание в документе вредоносной программы в виде макроса запускающегося вместе с открытием документа
5.3 Замена на носителе «чистого» документа вредоносным
5.4 Создание вредоносного ПО с функцией автозапуска
5.5 Запись на носитель вредоносного документа или вредоносной программы

После всех проделанных операций получилась рабочая модель СЗИ от НСД. Это позволяет наглядно представить, что происходит при ее работе на системном уровне, а также учесть предполагаемые действия злоумышленника. Имитационная модель будет являться дискретной, динамической, стохастической по причине того, что этими свойствами обладает СЗИ от НСД в автоматизированной системе, поэтому данная модель будет дискретно-событийной, следовательно, отражающей свойства во времени. Вероятность перехода из одного состояния в другое является мгновенной и зависит от времени пребывания в предыдущем состоянии.

Заключение

В данной статье разработана имитационная модель СЗИ от НСД. Выделены ее ключевые подсистемы и функциональные компоненты согласно технической документации [1, 2]. При помощи инструмента «Hierarchy», встроенного в CPN Tools, реализованы взаимосвязи между подсистемами, что позволяет модели соответствовать реально используемой на объектах информатизации СЗИ от НСД. Разработанная имитационная модель функционирования СЗИ от НСД в программной среде CPN Tools в

отличие от существующих формальных моделей [3] позволяет получить вероятностно-временные характеристики (в виде времен выполнения защитных функций). Это дает возможность не проводить вычислительный эксперимент по исследованию вероятностно-временных характеристик этих систем, которые в дальнейшем планируется использовать при количественной оценке эффективности программных средств и систем информационной безопасности в АС на объектах информатизации. Разработанную имитационную модель СЗИ от НСД в программной среде CPN Tools в дальнейших исследованиях планируется использовать как основу для анализа и создания моделей противодействия различным видам угроз НСД к информационному ресурсу защищенных АС.

СПИСОК ЛИТЕРАТУРЫ:

1. СЗИ «Страж NT». Руководство администратора. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (дата обращения: 25.05.2019).
2. Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. URL: http://www.rubinteh.ru/public/opis30.pdf (дата обращения: 25.05.2019).
3. Попов А.Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учётом их временных характеристик в автоматизированных системах органов внутренних дел: дис канд. техн. наук. Воронеж / 2018. URL: https://ви.мвд.рф/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (дата обращения: 25.05.2019).
4. Вентцель Е.С. Теория вероятностей. (accessed: 25.05.2019) Наука, 1969. – 576 с.
5. Jensen K. and Kristensen L.M. Coloured Petri Nets Modeling and Validation of Concurrent Systems. Berlin: Springer-Verlag, 2009.
6. Синегубов С.В. Моделирование систем и сетей телекоммуникаций. Воронеж: ВИ МВД РФ, 2016. – 336 с.
7. Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students' book. – Odessa: ONAT, 2006. – 60 p.
8. Григорьев В.А., Карпов А.В. Имитационная модель системы защиты информации // Программные продукты и системы. Тверь: МНИИПУ и НИИ «Центрпрограммсистем», 2005. №2. С. 26–30.
9. Питерсон Д.Ж. Теория сетей Петри и моделирование систем: Пер. с англ. – М.: Мир, 1984. – 264 с.
10. Котов В.Е. Сети Петри. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 160 с.
11. Дровникова И.Г., Змеев А.А., Попов А.Д., Рогозин Е.А. Методика исследования вероятностно-временных характеристик реализации сетевых атак в программной среде имитационного моделирования. Вестник Дагестанского государственного технического университета. Технические науки. 2017. 44 (4). С. 99–113. DOI: https://doi.org/10.21822/2073-6185-2017-44-4-99-113.
12. Meedeniya D. A. Indika Perera Model based software design: Tool support for scripting in immersive environments // IEEE 8th International Conference on Industrial and Information Systems, 2013. P. 248–253.
13. Lukaszewski R., Winiecki W. Petri Nets in Measuring Systems Design. IEEE Instrumentation and Measurement Technology Conference Proceedings, 2006. P. 1564–1569.
14. Gehlot V., Nigro C. An introduction to systems modeling and simulation with Colored Petri Nets. 2010. P. 104– 118.
15. Shang Guan Wei [et. al.] Research of System Modeling and Verification Method Combine with UML Formalization Analysis and Colored Petri Net Third International Symposium on Intelligent Information Technology Application, 2009. P. 488–491.

REFERENCES:

[1] SZI «Strazh NT». Rukovodstvo administratora. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (accessed: 25.05.2019) (in Russian).
[2] Sistema zashchity informacii ot nesankcionirovannogo dostupa «Strazh NT». Opisanie primeneniya. URL: http://www.rubinteh.ru/public/opis30.pdf (accessed: 25.05.2019) (in Russian).
[3] Popov A.D. Modeli i algoritmy ocenki effektivnosti sistem zashchity informacii ot nesankcionirovannogo dostupa s uchyotom ih vremennyh harakteristik v avtomatizirovannyh sistemah organov vnutrennih del: dis kand. tekhn. nauk. Voronezh / 2018. URL: https://vi.mvd.rf/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (accessed: 25.05.2019) (in Russian).
[4] Ventcel' E.S. Teoriya veroyatnostej. – M.: Nauka, 1969. – 576 s. (in Russian).

[5] Jensen K. and Kristensen L.M. Coloured Petri Nets Modeling and Validation of Concurrent Systems. Berlin: Springer-Verlag 2009.
[6] Sinegubov S.V. Modelirovanie sistem i setej telekommunikacij. Voronezh: VI MVD RF, 2016. – 336 s. (in Russian).
[7] Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students' book. – Odessa: ONAT, 2006. – 60 p.
[8] Grigor'ev V.A., Karpov A.V. Imitacionnaya model' sistemy zashchity informacii. Programmnye produkty i sistemy. Tver': MNIIPU i NII «Centrprogrammsistem», 2005. №2. S. 26–30 (in Russian).
[9] Piterson D.ZH. Teoriya setej Petri i modelirovanie sistem: Per. s angl. – M.: Mir, 1984. – 264 s. (in Russia).
[10] Kotov V.E. Seti Petri. Moskva: Nauka. Glavnaya redakciya fiziko-matematicheskoj literatury, 1984. – 160 s. (in Russian).
[11] Drovnikova I.G., Zmeev A.A., Popov A.D., Rogozin E.A. Methodology for investigating the probability-time characteristics of network attacks in the simulation modelling software environment. Herald of dagestan state technical university. Technical sciences. 2017. 44 (4). P. 99–113. DOI: https://doi.org/10.21822/2073-6185-2017-44-4-99-113 (in Russian).
[12] Meedeniya D. A. Indika Perera Model based software design: Tool support for scripting in immersive environments. IEEE 8th International Conference on Industrial and Information Systems, 2013. P. 248–253.
[13] Lukaszewski R., Winiecki W. Petri Nets in Measuring Systems Design. IEEE Instrumentation and Measurement Technology Conference Proceedings, 2006. P. 1564–1569.
[14] Gehlot V., Nigro C. An introduction to systems modeling and simulation with Colored Petri Nets. 2010. P 104–118.
[15] Shang Guan Wei [et. al.] Research of System Modeling and Verification Method Combine with UML Formalization Analysis and Colored Petri Net Third International Symposium on Intelligent Information Technology Application, 2009. P. 488–491.

Поступила в редакцию – 04 июля 2019 г. Окончательный вариант – 17 сентября 2019 г.
Received – July 04, 2019. The final version – September 17, 2019.