А. В. Бацких

ИМИТАЦИОННАЯ МОДЕЛЬ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ МОДИФИЦИРОВАННОЙ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ДОСТУПОМ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ПРОГРАММНОМ ОКРУЖЕНИИ CPN TOOLS

SIMULATION MODEL OF THE FUNCTIONING OF THE MODIFIED ACCESS CONTROL SUBSYSTEM OF THE INFORMATION PROTECTION SYSTEM AGAINST UNAUTHORIZED ACCESS IN THE CPN TOOLS SOFTWARE ENVIRONMENT

В статье на основе графовой модели процесса функционирования модифицированной подсистемы управления доступом типовой широко используемой в автоматизированных системах органов внутренних дел системы защиты информации от несанкционированного доступа «Страж NT 4.0» разработана имитационная модель ее функционирования в динамическом режиме с помощью сетей Петри. Проведено моделирование процесса функционирования подсистемы в программном окружении CPN Tools. Результаты имитационного моделирования представлены в табличной форме в виде значений вероятностно-временных характеристик модифицированной подсистемы управления доступом. Использование полученных результатов в качестве исходных данных при проведении оценки эффективности функционирования подсистем управления доступом и формировании количественных требований к системам защиты информации позволит повысить реальную защищенность существующих и разрабатываемых автоматизированных систем органов внутренних дел.

In the article, based on the graph model of the functioning of the modified access control subsystem of the standard widely used in automated systems of internal Affairs bodies of the information protection system against unauthorized access «Sentinel NT 4.0», a simulation model of its functioning in dynamic mode using Petri nets is developed. Simulation of the subsystem functioning process in the CPN Tools software environment is performed. The simulation results are presented in tabular form as values of probabilistic and temporal characteris-

tics of the modified access control subsystem. Using the results obtained as input data for evaluating the effectiveness of the functioning of the access control subsystems and forming quantitative requirements for information security systems will increase the real security of existing and developing automated systems of internal Affairs bodies.

Введение. Защита информационного ресурса от несанкционированного доступа (НСД) является составной частью общей проблемы обеспечения информационной безопасности (ИБ) современных объектов информатизации органов внутренних дел (ОВД). Встроенные в операционные системы средства, направленные на защиту информации от НСД, показывают свою несостоятельность, поскольку все чаще обнаруживаются уязвимости, позволяющие получить доступ к конфиденциальной информации в обход политики безопасности. Для предотвращения попыток осуществления НСД к информационному ресурсу автоматизированных систем (АС) ОВД применяются системы защиты информации (СЗИ) от НСД в соответствии с требованиями действующей нормативной документации [1—3]. Необходимость обеспечения высокой степени защищенности конфиденциальной информации обуславливает актуальность модификации действующих, а также разработки и внедрения новых СЗИ от НСД в АС, эксплуатируемых на объектах информатизации ОВД [4].

Одним из перспективных направлений повышения реальной защищенности информационного ресурса АС ОВД является совершенствование процедуры аутентификации, осуществляемой подсистемой управления доступом СЗИ от НСД, на основе использования новых информационно-телекоммуникационных технологий, в частности — биометрических систем [5]. С этой целью предлагается модифицировать подсистему управления доступом СЗИ от НСД путем реализации в ней двухфакторной аутентификации, основанной на распознавании клавиатурного почерка штатного пользователя при наборе им парольной фразы. Опыт эксплуатации современных защищенных АС на объектах информатизации ОВД показал, что максимальное влияние на эффективность функционирования подсистем управления доступом оказывает непосредственная зависимость ресурсоемкости СЗИ от НСД от вычислительного ресурса АС ОВД. Использование новых информационно-телекоммуникационных технологий для повышения реальной защищенности информации современных АС в процессе их эксплуатации на объектах информатизации ОВД не должно усугублять указанный недостаток, что диктует объективную необходимость исследования влияния предлагаемой технологии биометрической аутентификации на эффективность функционирования системы защиты и АС ОВД в целом. Это предполагает разработку имитационной модели модифицированной подсистемы управления доступом СЗИ от НСД и анализ ее функционирования в динамическом (временном) режиме путем определения вероятностно-временных характеристик (ВВХ).

Постановка задачи. Методика исследования процесса функционирования модифицированной подсистемы управления доступом путем определения ее ВВХ включает следующие этапы:

1. На основе графовой модели процесса функционирования предлагаемой модифицированной подсистемы на примере типовой широко используемой в АС ОВД СЗИ от НСД «Страж NT 4.0» создание имитационной модели ее функционирования в динамическом режиме с помощью сетей Петри.

2. Проведение моделирования процесса функционирования модифицированной подсистемы управления доступом, используя программную среду имитационного моделирования CPN Tools.

3. Представление в табличной форме результатов имитационного моделирования в виде значений ВВХ модифицированной подсистемы управления доступом.

Метод исследования. Моделирование процесса функционирования подсистемы управления доступом СЗИ от НСД является сложной и трудоемкой задачей, в которой приходится учитывать значительное количество параметров. Влияние этих параметров нередко взаимно противоположно, а часто — неопределенно и непредсказуемо. С целью анализа процесса функционирования модифицированной подсистемы управления доступом СЗИ от НСД в АС ОВД на примере современной темы з сертифицированной сисащиты «Страж NT 4.0» будем использовать математический аппарат сетей Петри в качестве наглядного представления моделируемой динамической системы.

Моделирование в сетях Петри осуществляется на событийном уровне. В процессе работы сети определяются действия, происходящие в системе, состояния, предшествующие этим действиям, и состояния, которые примет система после выполнения действия. Анализ сетей Петри позволяет получить информацию о структуре и динамическом поведении моделируемой системы [6, 7].

В основе сетей Петри лежат два непересекающихся множества пассивных и активных элементов: позиций (состояния, места) и переходов (действия, события). Позиции и переходы соединяются направленными дугами. Отслеживание динамического хода системы осуществляется с помощью меток (фишек, маркеров).

Для создания, отладки и анализа имитационных моделей с помощью иерархических, временных, цветных сетей Петри (Color Petri Nets) применяют специализированный программный пакет CPN Tools [8—10]. Имитационное моделирование в CPN Tools является дискретно-событийным, то есть предполагает мгновенную смену состояний сети Петри. В среде CPN Tools существует возможность программирования на унифицированном языке моделирования Unified Modeling Language (UML). К главным достоинствам программного продукта CPN Tools относится: высокая наглядность процесса действия системы; быстродействие; возможность генерации, анализа пространства состояний строящейся модели и формирования отчетов по ее работе в виде невременной и временной (для оценивания конкретного значения используется интервал времени) статистики [9].

Результаты имитационного моделирования динамики функционирования ключевых подсистем СЗИ от НСД, реально эксплуатируемых в АС ОВД, проведенного в программе CPN Tools на примере СЗИ от НСД «Страж NT 3.0», представлены [11, 12].

Модели исследования. Построение модели модифицированной подсистемы управления доступом на основе сети Петри осуществляется в три этапа: 1) объявление множеств и переменных; 2) формирование сети; 3) моделирование и анализ сети. Графически состояния обозначаются кругами или овалами (r_i, r_{0i}), переходы — прямоугольниками (t_i, t_{0i}).

На основе разработанной графовой модели «Включение ПК и идентификация пользователя», описывающей процесс функционирования модифицированной подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» в защищенных АС ОВД (механизм входа пользователя в систему посредством его идентификации и аутентификации), предлагается вид сети Петри рассматриваемой модели, приведенный на рис. 1.

Позиция r00 является входной перед началом работы состояний r_i, описывающих выполняемые подсистемой защитные функции [13]. Для подсчета количества фишек, прошедших через состояния r_i, добавлены связки t_{0i} и r_{0i}. Безостановочную работу модели обеспечивает цикл, возвращающий фишки в позицию r00.

Для исследования ВВХ модифицированной подсистемы управления доступом СЗИ от НСД осуществим моделирование процесса ее функционирования с учетом времени. Добавим в сеть временные метки, показывающие, с какого момента времени метка будет доступна в позиции. Реальные временные характеристики подсистемы зафиксированы в ходе эксперимента при помощи секундомера. Поскольку время в CPN Tools является безразмерным неотрицательным целым числом, а в реальности оно непрерывно, то для получения временной статистики процесса функционирования подсистемы установим следующую взаимосвязь между модельным (машинным) временем и реальным временем: 1 такт = 1 с.

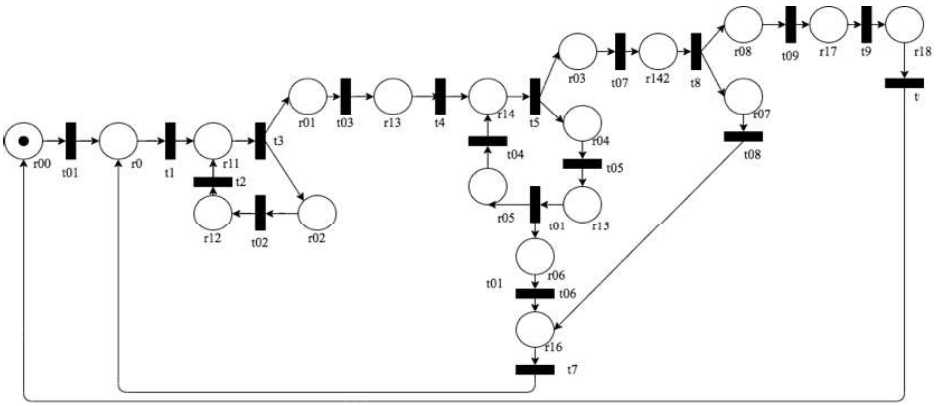
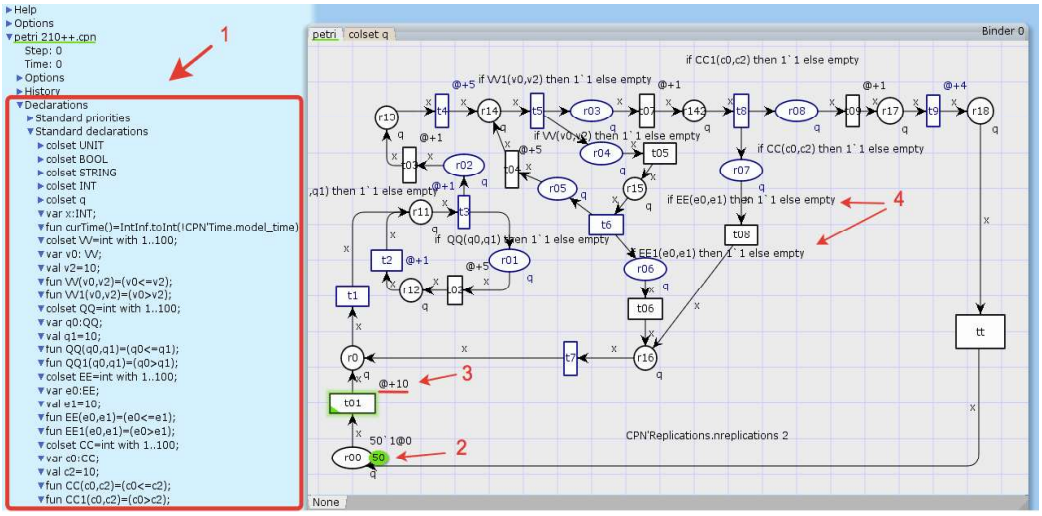


Рис. 1. Вид сети Петри для модифицированной подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» в защищенных АС ОВД

После запуска программного продукта CPN Tools появляется экран, в левой части которого расположено меню, позволяющее выполнять настройки сетей, а в правой — рабочее поле, где строится сеть. На рис. 2 представлена модель, имитирующая работу модифицированной подсистемы управления доступом СЗИ от НСД «Страж NT 4.0».



1 — сегмент кода на языке UML для настройки сети;
2 — количество меток;
3 — временные метки;
4 — условия срабатывания перехода

Рис. 2. Имитационная модель модифицированной подсистемы управления доступом СЗИ от НСД «Страж NT 4.0», построенная при помощи программной среды CPN Tools

Результаты исследования. Для корректной работы модели необходимо проверить ее на адекватность [14]. Осуществим необходимое количество шагов, в результате которых суммарное количество фишек в состояниях «r12» и «r13», «r142» и «r15», «r05» и «r16», «r17» и «r16» составит 50, из них: в позициях «r12» и «r13» — 7 и 43 фишки (рис. 3), в позициях «r142» и «r15» — 41 и 9 фишек (рис. 4), в позициях «r05» и «r16» — 47 и 3 фишки (рис. 5), а в позициях «r17» и «r16» — 44 и 6 фишек (рис. 6).

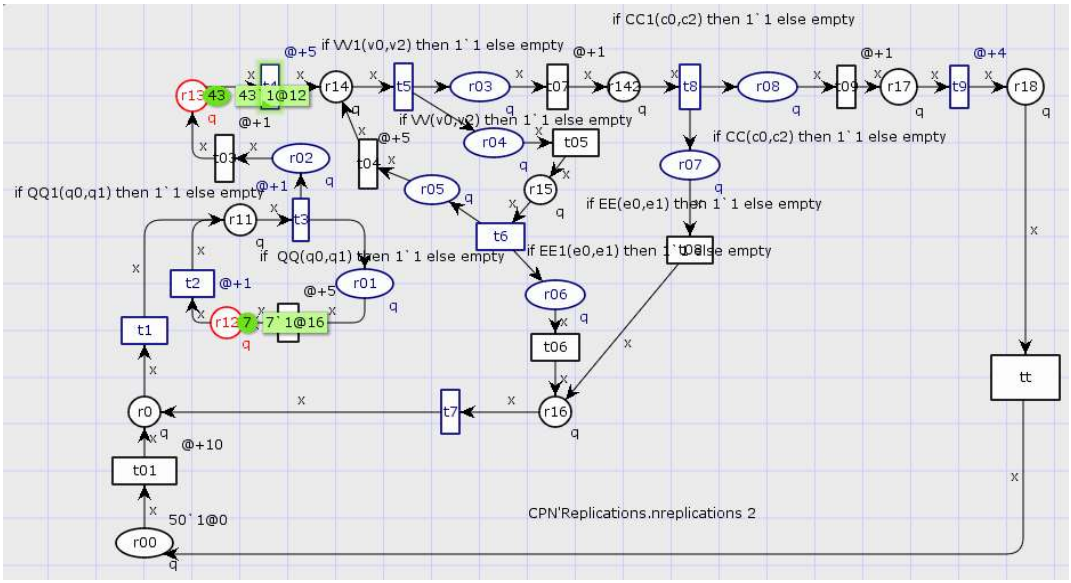


Рис. 3. Прогон модели для определения количества фишек в состояниях «r12» и «r13»

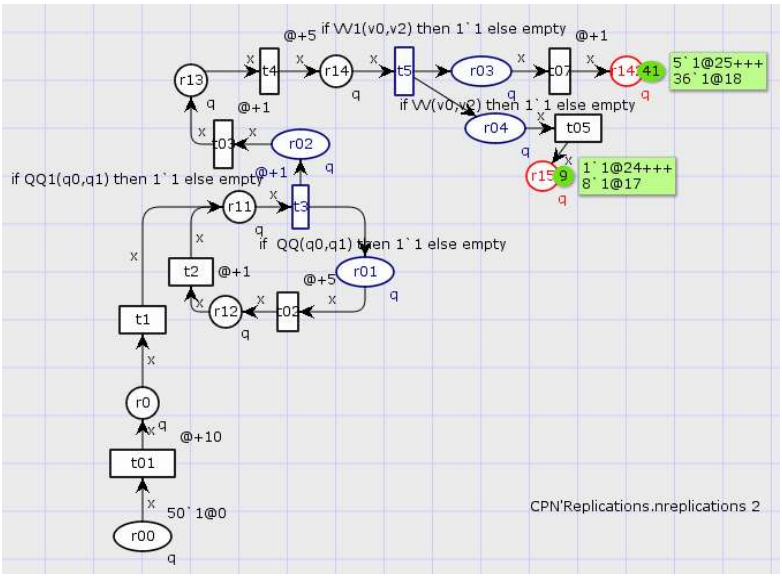


Рис. 4. Прогон модели для определения количества фишек в состояниях «r142» и «r15»

Тогда частоту появления фишек в состояниях «r12», «r142», «r05» и «r17» вычислим следующим образом:

$$p_{r12} = \frac{7}{50} = 0{,}14;\ p_{r142} = \frac{9}{50} = 0{,}18; \qquad (1)$$

$$p_{r05} = \frac{3}{50} = 0{,}06;\ p_{r17} = \frac{6}{50} = 0{,}12.$$

Определим необходимое количество прогонов по сети для вероятности появления события с точностью $\varepsilon = 0{,}01$ и достаточностью $D = 0{,}99$ по формуле

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

где Φ_0 — функция Лапласа.

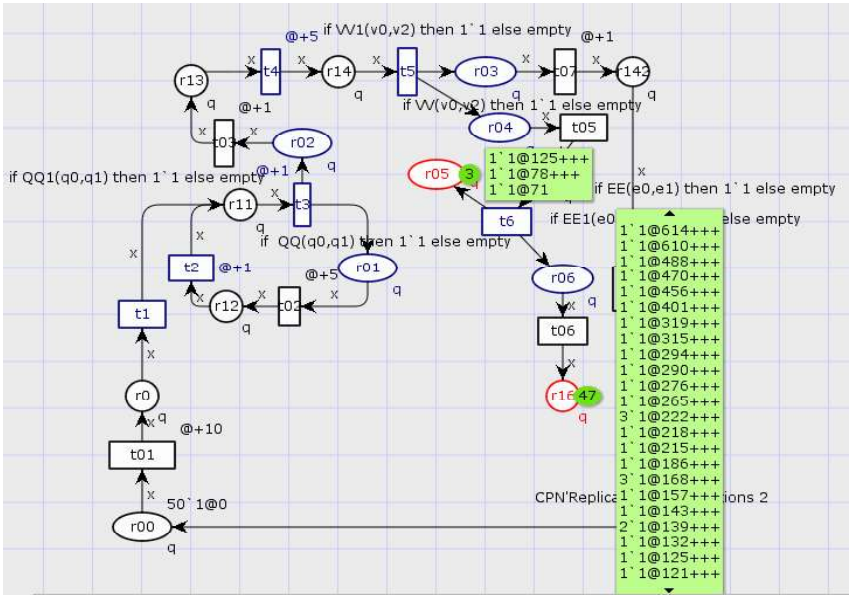


Рис. 5. Прогон модели для определения количества фишек в состояниях «r05» и «r16»

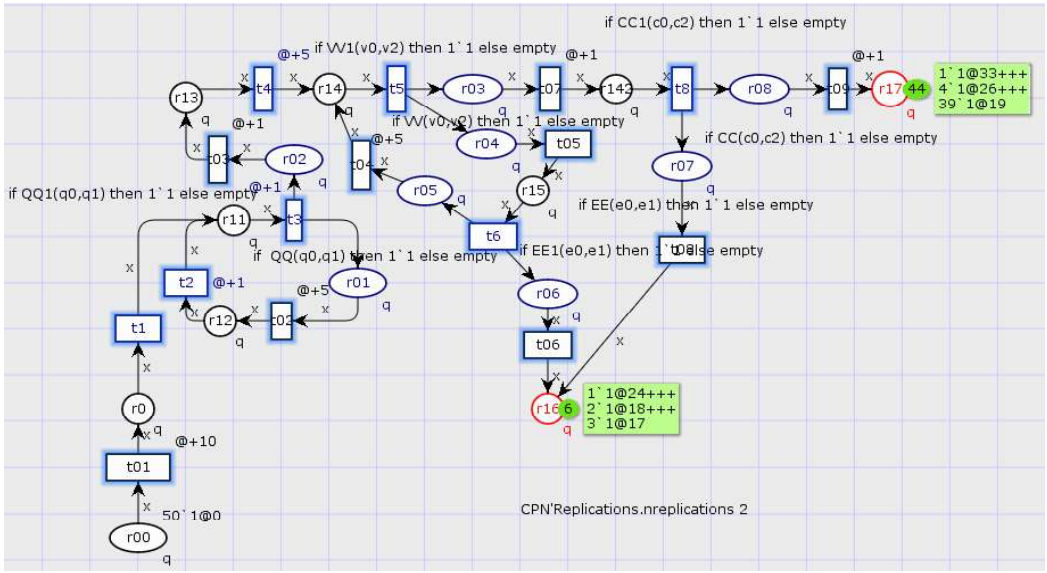


Рис. 6. Прогон модели для определения количества фишек в состояниях «r17» и «r16»

Соответственно, необходимое количество прогонов «r12», «r142», «r05» и «r17» для данных состояний будет следующим:

$$N_{r12} = \frac{0.14(1-0.14)}{0.01^2} 2.58^2 = 8014{,}3 \approx 8015;$$
$$N_{r142} = \frac{0.18(1-0.18)}{0.01^2} 2.58^2 = 9824{,}6 \approx 9825; \quad (3)$$
$$N_{r05} = \frac{0.06(1-0.06)}{0.01^2} 2.58^2 = 3754{,}2 \approx 3755;$$
$$N_{r17} = \frac{0.12(1-0.12)}{0.01^2} 2.58^2 = 7029{,}2 \approx 7030.$$

Для определения необходимого количества прогонов по сети выберем максимальное из рассчитанных значений, округлив его в большую сторону. Тогда для модифицированной подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» необходимое количество прогонов по сети составит $N \approx 9825$ (рис. 7).

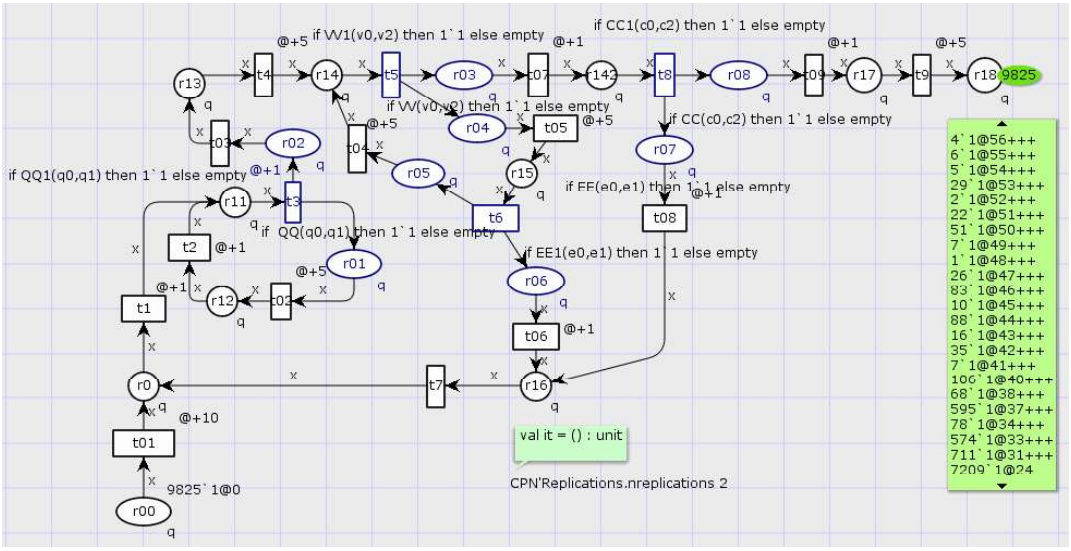


Рис. 7. Имитационная модель модифицированной подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» с необходимым количеством прогонов

Для сбора временных статистических данных применяется панель «Monitoring». Сохраняем модель и осуществляем прогон сети. Функция «CPN'Replications.nreplications 2» может использоваться для автоматического запуска заданного количества симуляций (например, 2). В итоге получим значения изучаемых характеристик в виде файла отчета с расширением .html, который находится в той же папке, где хранится модель. Результаты имитационного моделирования процесса функционирования модифицированной подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» представлены в табл. 1.

Таблица 1

Временная статистика процесса функционирования модифицированной подсистемы управления доступом СЗИ от НСД «Страж NT 4.0»

	Timed statistics				
Name	Count	Avrg	Min	Max	Time Avrg
Marking_size_petri'r0_1	22802	4093.750000	0	9825	10
Marking_size_petri'r11_1	24079	516.875000	0	9825	1
Marking_size_petri'r12_1	2239	242.083333	0	1005	6
Marking_size_petri'r13_1	20810	0.000000	0	187	1
Marking_size_petri'r14_1	19335	2116.333333	0	8820	5
Marking_size_petri'r142_1	15914	330.791667	0	7939	1
Marking_size_petri'r15_1	1765	183.541667	0	881	5
Marking_size_petri'r16_1	3152	65.625000	0	807	1
Marking_size_petri'r17_1	14344	298.791667	0	7171	1
Marking_size_petri'r18_1	7173	1493.958333	0	7171	5

Таблица содержит следующие столбцы: Name — имя позиции; Count — счетчик проходов по графу, начиная с 0; Avrg — среднее значение в контексте данной имитационной задачи (среднее количество маркеров в позиции); Min — минимальное количество маркеров в позиции; Max — максимальное количество маркеров в позиции; Time Avrg — среднее время нахождения в одном из состояний графовой модели, формально описывающей процесс функционирования подсистемы управления доступом.

Таблица 2

Сравнительные результаты времени пребывания в заданных состояниях существующей и модифицированной подсистем управления доступом СЗИ от НСД «Страж NT 4.0»

Существующая подсистема управления доступом			Модифицированная подсистема управления доступом		
№ состояния	Функции, выполняемые подсистемой	Время, с	№ состояния	Функции, выполняемые подсистемой	Время, с
0	Начало работы подсистемы (прекращение выполнения функций подсистемой)	10	0	Начало работы подсистемы (прекращение выполнения функций подсистемой)	10
1.1	Предъявление идентификатора	1	1.1	Предъявление идентификатора	1
1.2	Прекращение работы идентификатора (в случае новой попытки требуется заново ввести)	6	1.2	Прекращение работы идентификатора (в случае новой попытки требуется заново ввести)	6
1.3	Допуск к вводу пароля	1	1.3	Допуск к вводу пароля	1
1.4	Ввод пароля	5	1.4	Ввод пароля	5
1.5	Повторный ввод пароля	5	1.5	Повторный ввод пароля	5
1.6	Блокировка входа в систему при трехразовом неправильном вводе пароля	1	1.6	Блокировка входа в систему при трехразовом неправильном вводе пароля (при несоответствии клавиатурного почерка)	1
1.7	Аутентификация пользователя	1	1.7	Исследование клавиатурного почерка пользователя	1
1.8	Вход в систему	5	1.8	Аутентификация пользователя	1
			1.9	Вход в систему	5

Представленная в табл. 2 сравнительная временная статистика процесса функционирования существующей [15] и модифицированной подсистем управления доступом СЗИ от НСД «Страж NT 4.0» позволяет констатировать, что реализация двухфакторной аутентификации, основанной на распознавании клавиатурного почерка штатного пользователя при наборе им парольной фразы, несущественно влияет на временной показатель функционирования подсистемы.

Заключение. Модификация подсистемы управления доступом путем реализации двухфакторной аутентификации, основанной на распознавании клавиатурного почерка штатного пользователя при наборе им парольной фразы, позволит повысить эффективность функционирования СЗИ от НСД и АС ОВД в целом, существенно не увеличивая временной показатель функционирования подсистемы.

Разработанная имитационная модель может быть использована при оценивании эффективности функционирования подсистемы управления доступом СЗИ от НСД с целью повышения реальной защищенности существующих и разрабатываемых АС ОВД. При этом ВВХ подсистемы (в виде средних времен выполнения ею защитных функций), полученные с помощью программного пакета CPN Tools, послужат исходными данными для анализа и проведения количественной оценки эффективности функционирования модифицированной подсистемы управления доступом в АС при их эксплуатации в защищенном исполнении на объектах информатизации ОВД в соответствии с требованиями действующей нормативной документации.

ЛИТЕРАТУРА

1. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 [Электронный ресурс]. — URL: http://publication.pravo.gov.ru/Document/View/0001201612060002 (дата обращения: 03.07.2020).

2. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [Электронный ресурс]. — URL: http://fstec.ru/component/attachments//299t (дата обращения: 03.07.2020).

3. ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении [Электронный ресурс]. — URL: http://docs.cntd.ru/document/1200108858 (дата обращения: 02.07.2020).

4. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года : приказ МВД России от 14.03.2012 № 169 [Электронный ресурс]. — URL: http:// policemagazine.ru/forum/showthread.php?t=3663 (дата обращения: 01.07.2020).

5. Бацких А. В., Дровникова И. Г., Рогозин Е. А. К вопросу использования новой информационной технологии, связанной с дополнительной аутентификацией субъектов доступа по клавиатурному почерку, в системах защиты информации от несанкционированного доступа на объектах информатизации органов внутренних дел // Вестник ВИ МВД России. — 2020. — № 2. — С. 21—33.

6. Питерсон Д. Ж. Теория сетей Петри и моделирование систем : пер. с англ. — М. : Мир, 1984. — 264 с.

7. Network security analyzing and modeling based on Petri net and Attack tree for SDN / Y. Linyuan [et al.] // International Conference on Computing, Networking and Communications. — 2016. — P. 133—187.

8. Charaf H., Azzouzi S. A colored Petri-net model for control execution of distributed systems // 4th International Conference on Control, Decision and Information Technologies. — 2017. — P. 277—282.

9. Романников Д. О., Марков А. В. Об использовании программного пакета CPN TOOLS для анализа сетей Петри // Сб. науч. тр. НГТУ. — 2012. — № 2(68). — С. 105—116.

10. Zaitsev D. A., Shmeleva T. R. Simulating Telecommunication Systems with CPN Tools : Students' book. — Odessa : ONAT, 2006. — 60 p.

11. Разработка имитационной модели системы защиты информации от несанкционированного доступа с использованием программной среды CPN Tools / О. И. Бокова [и др.] // Безопасность информационных технологий = IT Security. — 2019. — Т. 26. — № 3. — С. 80—89.

12. Модель процесса функционирования системы защиты информации от несанкционированного доступа, созданная в программной среде имитационного моделирования «CPN Tools» / И. Г. Дровникова [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. — 2019. — Т. 46. — № 1 (2019). — С. 90—102.

13. 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 : 05.13.19. — Воронеж, 2018. — 163 с.

14. Синегубов С. В. Моделирование систем и сетей телекоммуникаций. — Воронеж : Воронежский институт МВД России, 2016. — 336 с.

15. Использование численно-аналитической модели оценки эффективности функционирования системы защиты информации от несанкционированного доступа при анализе ее вероятностно-временных характеристик / А. В. Бацких [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. — 2020. — Т. 47. — № 1. — С. 58—71.

REFERENCES

1. Ob utverzhdenii Doktrinyi informatsionnoy bezopasnosti Rossiyskoy Federatsii : ukaz Prezidenta RF ot 05.12.2016 # 646. — URL: http://publication.pravo.gov.ru/Document/View/0001201612060002 [Elektronnyiy resurs] (data obrascheniya: 03.07.2020).

2. FSTEK RF. Rukovodyaschiy dokument. Kontseptsiya zaschityi sredstv vyichislitelnoy tehniki i avtomatizirovannyih sistem ot nesanktsionirovannogo dostupa k informatsii [Elektronnyiy resurs]. — URL: http://fstec.ru/component/attachments//299t (data obrascheniya: 03.07.2020).

3. GOST R 51583-2014. Poryadok sozdaniya avtomatizirovannyih sistem v zaschischennom ispolnenii [Elektronnyiy resurs]. — URL: http://docs.cntd.ru/document/1200108858 (data obrascheniya: 02.07.2020).

4. Ob utverzhdenii Kontseptsii obespecheniya informatsionnoy bezopasnosti organov vnutrennih del Rossiyskoy Federatsii do 2020 goda : [Elektronnyiy resurs]. — URL: http://policemagazine.ru/forum/showthread.php?t=3663 (data obrascheniya: 01.07.2020).

5. Batskih A. V., Drovnikova I. G., Rogozin E. A. K voprosu ispolzovaniya novoy informatsionnoy tehnologii, svyazannoy s dopolnitelnoy autentifikatsiey sub'ektov dostupa po klaviaturnomu pocherku, v sistemah zaschityi informatsii ot nesanktsionirovannogo dostupa na ob'ektah informatizatsii organov vnutrennih del // Vestnik VI MVD Rossii. — 2020. — # 2. — S. 21—33.

6. Piterson D. Zh. Teoriya setey Petri i modelirovanie sistem : per. s angl. — M.: Mir, 1984. — 264 s.

7. Network security analyzing and modeling based on Petri net and Attack tree for SDN / Y. Linyuan [et al.] // International Conference on Computing, Networking and Communications. — 2016. — R. 133—187.

8. Charaf N., Azzouzi S. A colored Petri-net model for control execution of distributed systems // 4th International Conference on Control, Decision and Information Technologies. — 2017. — R. 277—282.

9. Romannikov D. O., Markov A. V. Ob ispolzovanii programmnogo paketa CPN TOOLS dlya analiza setey Petri // Sb. nauch. tr. NGTU. — 2012. — # 2(68). — S. 105—116.

10. Zaitsev D. A., Shmeleva T. R. Simulating Telecommunication Systems with CPN Tools: Students' book. — Odessa: ONAT, 2006. — 60 p.

11. Razrabotka imitatsionnoy modeli sistemyi zaschityi informatsii ot nesanktsionirovannogo dostupa s ispolzovaniem programmnoy sredyi CPN Tools / O. I. Bokova [i dr.] // Bezopasnost informatsionnyih tehnologiy = IT Security. — 2019. — T. 26. — # 3. — S. 80—89.

12. Model protsessa funktsionirovaniya sistemyi zaschityi informatsii ot nesanktsionirovannogo dostupa, sozdannaya v programmnoy srede imitatsionnogo modelirovaniya «CPN Tools» / I. G. Drovnikova [i dr.] // Vestnik Dagestanskogo gosudarstvennogo tehnicheskogo universiteta. Tehnicheskie nauki. — 2019. — T. 46. — # 1 (2019). — S. 90—102.

13. Popov A. D. Modeli i algoritmyi otsenki effektivnosti sistem zaschityi informatsii ot nesanktsionirovannogo dostupa s uchYotom ih vremennyih harakteristik v avtomatizirovannyih sistemah organov vnutrennih del : dis. ... kand. tehn. nauk : 05.13.19. — Voronezh, 2018. — 163 s.

14. Sinegubov S. V. Modelirovanie sistem i setey telekommunikatsiy. — Voronezh : Voronezhskiy institut MVD Rossii, 2016. — 336 s.

15. Ispolzovanie chislenno-analiticheskoy modeli otsenki effektivnosti funktsionirovaniya sistemyi zaschityi informatsii ot nesanktsionirovannogo dostupa pri analize ee veroyatnostno-vremennyih harakteristik / A. V. Batskih [i dr.] // Vestnik Dagestanskogo gosudarstvennogo tehnicheskogo universiteta. Tehnicheskie nauki. — 2020. — T. 47. — # 1. — S. 58—71.

СВЕДЕНИЯ ОБ АВТОРЕ

Бацких Анна Вадимовна. Адъюнкт кафедры автоматизированных информационных систем ОВД. Воронежский институт МВД России.
E-mail: svatikova96@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-90.

Batskikh Anna Vadimovna. Post-graduate cadet of the chair of Automatic Information Systems in Interior Affairs.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: svatikova96@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-51-90.

Ключевые слова: автоматизированная система; подсистема управления доступом; вероятностно-временные характеристики; имитационная модель; сети Петри; программная среда CPN Tools.

Key words: automated syste; access control subsystem; probability-time characteristics; simulation model; Petri networks; CPN Tools software environment.

УДК 004.056