

УДК 621.3

*И.Г. Дровникова¹, А.А. Змеев²**(¹Воронежский институт МВД России, ²Военная академия воздушно-космической обороны им. Г.К. Жукова (г. Тверь); e-mail: idrovnikova@mail.ru)*

МОДЕЛИРОВАНИЕ ПРОЦЕССА ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ НА ОСНОВЕ ОЦЕНОЧНЫХ СЕТЕЙ

Описывается модель системы защиты информации от несанкционированного доступа в автоматизированные системы, построенная с использованием сертифицированной оценочной сети (Е-сети). Приводится вербальное и формальное описание модели. Результаты формализации могут служить основой для разработки частной методики формирования требований к системе с помощью методов эволюционного моделирования.

Ключевые слова: защита информации, несанкционированный доступ, автоматизированная система, сеть Петри, оценочная сеть.

Введение

Постоянное ужесточение требований к оперативности, достоверности и конфиденциальности обрабатываемой информации привело к усложнению средств и систем *защиты информации (ЗИ) в автоматизированных системах (АС)*. Поэтому ключевым вопросом теории и практики ЗИ является формирование требований к *системам защиты информации (СЗИ) от несанкционированного доступа (НСД) в АС*^{1,2}.

Существующие подходы к решению этой сложной задачи описаны в Руководящих документах^{2,3} и ГОСТ 34.601-90⁴. Решение сводится к определению функционала СЗИ от НСД (набора функций ЗИ), в то же время ГОСТ Р 51583-2014⁵ требует определять количественные параметры эффективности СЗИ и проводить их оптимизацию.

Перспективной в этом смысле является предложенная в [1] общая методика формирования требований к СЗИ от НСД в АС с использованием методов эволюционного моделирования, основанная на преимуществах применения генетического алгоритма [1, 2], к которым относится возможность нахождения оптимального решения путём последовательного подбора и комбинирования заданных параметров на основе использования механизмов, напоминающих биологическую эволюцию. Однако указанная методика, обладая теоретической

¹ Доктрина информационной безопасности Российской Федерации / Утв. Указом Президента Российской Федерации № 646 от 05.12.2016;

² ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. <http://fstec.ru/component/attachments/download/299>;

³ ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Воениздат, 1992;

⁴ ГОСТ 34.601-90. Автоматизированные системы. Стадии создания. <http://www.insapov.ru/gost-34-601-90.html>;

⁵ ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищённом исполнении. <http://docs.cntd.ru/document/1200108858>

значимостью, не может претендовать на практическую ценность: поскольку объектом исследования в ней не являлась конкретная типовая СЗИ от НСД, то полученные практические результаты не могут быть применимы к широкому спектру сертифицированных СЗИ.

Авторами настоящей статьи сделана попытка, отталкиваясь от методики общего характера [1], найти способ формирования универсальных и практически реализуемых требований к СЗИ от НСД в АС, используя сертифицированные СЗИ.

Для этого решены две связанные задачи:

1. Адаптирована и вербально представлена модель широко используемой сертифицированной СЗИ от НСД в АС "Dallas lock".

2. Формализован процесс функционирования СЗИ от НСД в АС на основе указанной сертифицированной системы.

Вербальная модель

"Dallas lock"⁶ представляет собой СЗИ, работающую под управлением операционных систем как семейства Windows, так и Linux. Эта система сертифицирована по 1Б, 1В, 1Г, 1Д, 2А, 2Б, 3А, 3Б классам защищённости при создании АС⁷. На сегодняшний день "Dallas lock" используется во многих государственных и коммерческих структурах, имея множество сертификатов совместимости с другими программными продуктами.

"Dallas lock" состоит из следующих подсистем обеспечения ЗИ в АС⁶:

- самодиагностики;
- управления доступом;
- администрирования параметров СЗИ от НСД;
- идентификации и аутентификации пользователей;
- контроля целостности рабочей среды пользователей АС;
- регистрации и учёта.

Одним из ключевых моментов моделирования СЗИ от НСД в АС, который определяет качество разрабатываемой модели, является формализация процесса функционирования указанных систем. Широко известный подход к формализации базируется на представлении этого процесса в виде ориентированного графа [3]. Конкретизируем математические объекты, развивая описание СЗИ от НСД с помощью ориентированного графа.

Проведённый авторами анализ таких математических объектов позволил сделать следующий вывод: для построения формальной модели динамики функционирования СЗИ от НСД в АС целесообразно использовать так называ-

⁶ Типовая система защиты информации от несанкционированного доступа RU.48957919.501410-02 31 // Техническая документация. Государственный научно-исследовательский институт моделирования интеллектуальных сложных систем, 2017. 16 с.;

⁷ ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Воениздат, 1992

емые оценочные сети (Е-сети), которые, являясь дальнейшим развитием сетей Петри [3-9], развивают традиционные орграфовые формализации данных процессов за счёт введения типовых для аппарата оценочных сетей процедур временной задержки и разрешающих процедур.

Оценочная сеть – это граф, имеющий особенный вид и состоящий, как и сеть Петри, из двух типов вершин – позиций (станций) и переходов, соединённых друг с другом ориентированными рёбрами или дугами, причём каждая дуга может связывать лишь переход с позицией или позицию с переходом. Поэтому оценочная сеть, как и сеть Петри, структурно эквивалентна двудольному ориентированному графу, у которого одно множество вершин содержит позиции, а другое – переходы. Однако, в отличие от сетей Петри, в оценочных сетях имеются несколько типов позиций; на соединения позиций с переходами накладываются особенные ограничения; объекты, или фишки, являющиеся динамическими элементами сети, обладают наборами признаков (атрибутами). Кроме того, в оценочной сети с каждым переходом можно ассоциировать ненулевую временную задержку и процедуру преобразования атрибутов. Поэтому в оценочной сети имеются разрешающие позиции, играющие управляющую роль и позволяющие создавать условные ветвления и переключения при перемещении объектов. Все это значительно расширяет возможности оценочных сетей для моделирования сложных систем, к которым можно отнести и СЗИ от НСД [1].

Формальная модель

Процесс построения оценочной сети довольно подробно описан в [3-9], поэтому его теоретическая часть в настоящей статье не приводится.

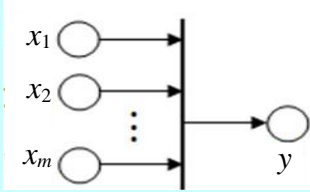
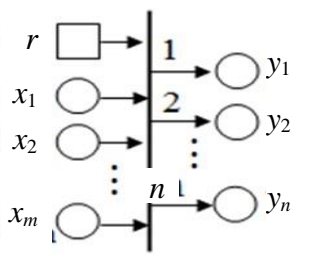
В табл. 1 представлен основной набор элементарных сетей для формального описания процесса функционирования СЗИ от НСД в АС, который состоит из 2-х типов оценочных сетей: сеть типа J (объединение) и сеть типа X (переключатель). Графически данные сети отличаются друг от друга тем, что сеть типа X в отличие от сети типа J содержит разрешительную позицию и более одной выходной. Рассмотрим более подробно каждый из этих типов элементарных сетей.

Сеть типа J . Условие срабатывания перехода – наличие объекта (состояния функционирования СЗИ от НСД) в одной из входных позиций x_1, x_2, \dots, x_m . В конце фазы активности перехода в выходной позиции появляется объект, а все входные позиции освобождаются от объекта.

Сеть типа X . Условие срабатывания перехода – наличие объекта в одной из входных позиций x_1, x_2, \dots, x_m . Выходные дуги перехода пронумерованы в порядке $1, 2, \dots, n$. Вычисляется разрешающая процедура, ассоциированная с разрешительной позицией r . Пусть в результате определено состояние разрешительной позиции, равное целому числу $j \in \{1, 2, \dots, K, \dots, n\}$. Тогда в конце фазы активности перехода объект перемещается в выходную позицию y_j , а состояние разрешительной позиции становится неопределённым.

Таблица 1

Основной набор элементарных сетей для формального описания процесса функционирования СЗИ от НСД в АС

Тип перехода	Графическое представление	Условное обозначение
Объединение		$J(x_1, x_2, \dots, x_m, y)$
Переключатель		$X(r, x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n)$

Оценочная сеть процесса функционирования СЗИ от НСД "Dallas Lock" представлена на рис. 1.

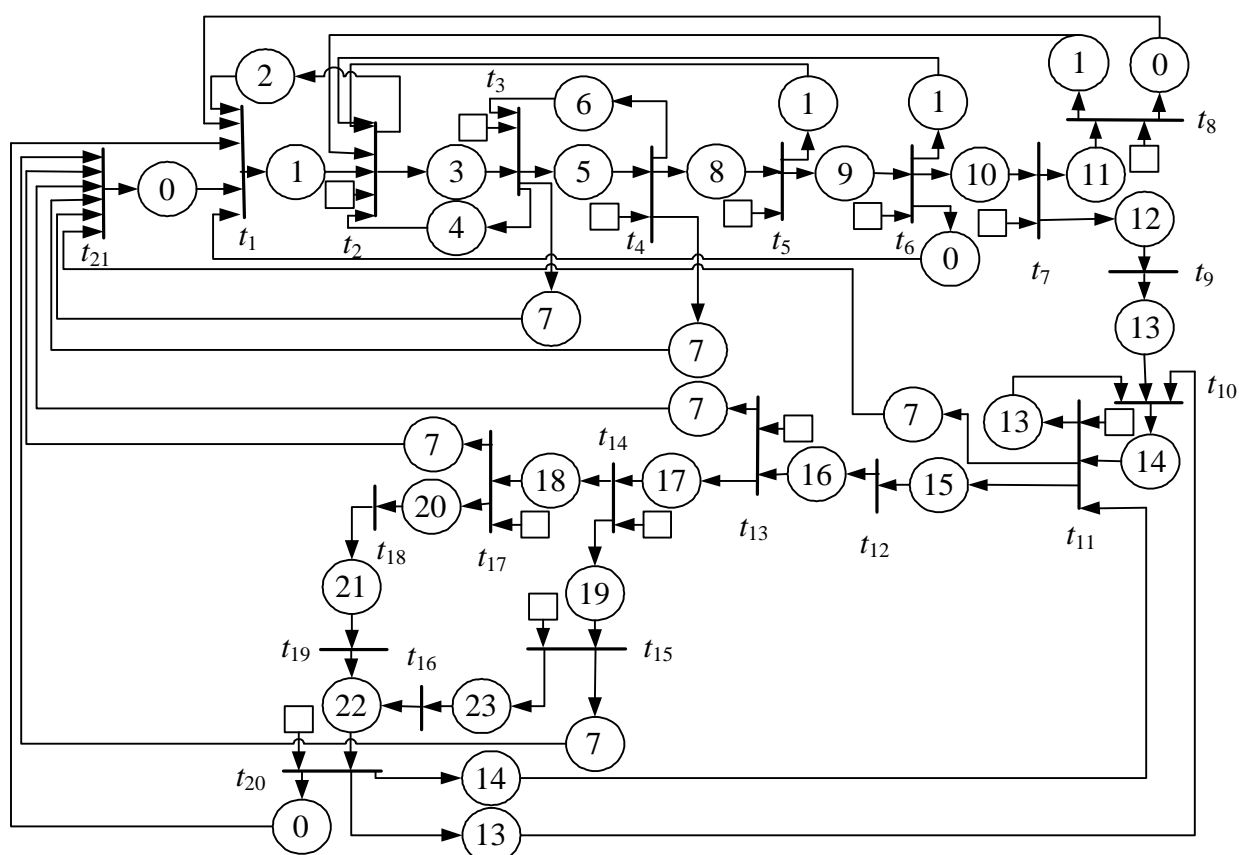


Рис. 1. Формальная модель процесса функционирования СЗИ от НСД в АС на основе оценочной сети

Здесь пребывание СЗИ от НСД в простой позиции соответствует выполнению такой функции ЗИ, номер которой указан в кружочке, изображающем данную простую позицию. Перечень функций ЗИ с временами их выполнения (в секундах) и соответствующими элементарными сетями представлен в табл. 2.

Таблица 2

**Сведения о сервисных задачах и функциях защиты информации,
характеризующих процесс функционирования СЗИ от НСД "Dallas lock"**

Номер и наименование функции СЗИ от НСД	Номер перехода	Элементарная сеть
1. Ввод имени пользователя (авторизация)	t_1	$J(x_0, x_0, x_0, x_0, x_0, x_2, y_1)$
2. Повторный ввод имени пользователя	t_2	$X(r_1, x_1, x_1, x_1, x_1, x_4, y_2, y_3)$
3. Ввод пароля	t_3	$X(r_2, x_3, x_6, y_4, y_5, y_7)$
4. Повторный ввод пароля	t_4	$X(r_2, x_3, y_6, y_7, y_8)$
5. Ввод идентификатора	t_5	$X(r_4, x_8, y_1, y_9)$
6. Повторный ввод идентификатора	t_6	$X(r_4, x_8, y_1, y_9)$
7. Блокировка в случае неоднократно неправильно введенного пароля, несоответствия пользователя и предъявляемого идентификатора	t_7	$X(r_5, x_{10}, y_{11}, y_{12})$
8. Проверка доступного времени работы пользователя	t_8	$X(r_6, x_{11}, y_0, y_1)$
9. Контроль доступа	t_9	$J(x_{12}, y_{13})$
10. Проверка срока действия пароля	t_{10}	$J(x_{13}, x_{13}, x_{13}, y_{14})$
11. Разрешений на изменение пароля	t_{11}	$X(r_7, x_{14}, x_{14}, y_7, y_{13}, y_{15})$
12. Вход в систему	t_{12}	$J(x_{15}, y_{16})$
13. Обращение к ресурсу	t_{13}	$X(r_8, x_{16}, y_7, y_{17})$
14. Мандатный механизм управления доступом. Соотносятся метки конфиденциальности пользователя и ресурса	t_{14}	$X(r_9, x_{17}, y_{18}, y_{19})$
15. Обращение к объекту	t_{15}	$X(r_{10}, x_{17}, y_7, y_{23})$
16. Проверка полномочий доступа пользователя, основанного на дискреционном принципе контроля доступа	t_{16}	$J(x_{23}, y_{22})$
17. Допуск субъекта к защищаемому объекту	t_{17}	$X(r_{11}, x_{18}, y_7, y_{23})$
18. Запрос на преобразование объекта	t_{18}	$J(x_{20}, y_{21})$
19. Запрос на удаление	t_{19}	$J(x_{21}, y_{22})$
20. Преобразование объекта перед удалением	t_{20}	$X(r_{22}, x_{18}, y_0, y_{13}, y_{14})$
21. Удаление объекта		
22. Завершение работы с объектом	t_{21}	$J(x_7, x_7, x_7, x_7, x_7, x_7, y_0)$
23. Пересчет параметров целостности объекта		

Разрешающие процедуры реализуют случайные переходы между состояниями функционирования СЗИ от НСД. Для адекватного моделирования оценочной сетью процесса функционирования СЗИ от НСД данные переходы должны быть равновероятными, то есть вероятность P_{ij} перехода из состояния i в следующее за ним состояние j равна $P_{ij} = 1/K$, где K – число переходов из состояния i [3-5]. Преобразование атрибутов объекта осуществляется только

при его прохождении через позиции, соответствующие нулевому состоянию (нулевые позиции). Выход объекта из нулевой позиции соответствует обращению к СЗИ от НСД, а вход объекта в нулевую позицию – окончанию реализации функций СЗИ от НСД по данному обращению. При этом преобразование атрибутов объекта означает переход к обработке нового обращения к СЗИ от НСД, а сами атрибуты характеризуют текущее обращение, например, его номер. Время жизни объекта есть промежуток времени от выхода объекта из нулевой позиции до входа объекта (с теми же атрибутами) в нулевую позицию.

Заключение

Результаты проведённой формализации процесса функционирования СЗИ от НСД на основе оценочной сети могут быть использованы для разработки математической модели динамики функционирования СЗИ от НСД, основанной на теории марковских процессов, позволяющей получить адекватную модель случайных процессов, которую можно использовать в качестве основы целевой функции (функции приспособленности) решения задачи оптимизации параметров и характеристик эффективности функционирования СЗИ от НСД с помощью генетического алгоритма в различных условиях применения АС.

Математическая модель может служить основой для разработки частной методики формирования универсальных и практически реализуемых оптимальных количественных требований к широкому классу сертифицированных по определённому классу защищённости СЗИ от НСД в АС в соответствии требованиями действующей нормативной документации.

Литература

1. Змеев А.А., Мачтаков С.Г., Мецержакова Т.В., Никулина Е.Ю., Rogozin Е.А., Стукалов В.В., Хвостов В.А. Методы и средства эволюционного и структурного моделирования при обосновании требований к программным системам защиты информации: монография / Под ред. Е.А. Рогозина. Воронеж: Воронежский институт МВД России, 2015. 94 с.
2. Goldberg D. Genetic Algorithms in Search, Optimization and Machine Learning. Massachusetts: Addison-Wesley, 1989. 343 p.
3. Дубровин А.С., Макаров О.Ю., Муратов А.В., Попрыгин Г.И., Рогозин Е.А., Сумин В.И., Шишкин В.М. Метод формализации функционирования типовых программных систем защиты информации // Телекоммуникации. 2002. № 8. С. 33-40.
4. Советов Б.Я., Яковлев С.А. Моделирование систем: учеб. для вузов. М.: Высш. шк., 2001. 343 с.
5. Костин А.Е. Принципы моделирования сложных дискретных систем. М.: МИЭТ, 1984. 140 с.
6. Пранявичюс Г.И. Модели и методы исследования вычислительных систем. Вильнюс: Мокслас, 1982. 315 с.
7. Костин А.Е., Шаньгин В.Ф. Организация и обработка структур данных в вычислительных системах. М.: Высш. шк., 1987. 248 с.
8. Мараховский В.Б., Розенблюм Л.Я., Яковлев А.В. Моделирование параллельных процессов. Сети Петри. СПб.: Профессиональная литература, 2014. 400 с.
9. Ломазова И.А. Вложенные сети Петри: моделирование и анализ распределённых систем с объектной структурой. М.: Научный мир, 2004. 208 с.

Статья поступила в редакцию интернет-журнала 15 ноября 2017 г.

I.G. Drovnikova, A.A. Zmeev

MODELING THE PROCESS OF INFORMATION PROTECTION IN AUTOMATED SYSTEMS BASED ON THE ESTIMATION NETWORK

A formal model of the functioning of widely used certified 1B, 1C, 1G, 1D, 2A, 2B, 3A, 3B classes of security system of information protection from unauthorized access to automated systems based on the evaluation network (E-network) is proposed. The results of the formalization of the process of functioning of system of information protection from unauthorized access on the basis of the evaluation network can be used for mathematical modeling of the dynamics of the functioning of system of information protection from unauthorized access to study its probability-time characteristics in various conditions of use, as well as in the development of private methods of forming requirements to the system by using the methods of evolutionary modeling.

Key words: information security, unauthorized access, automated system, Petri net, evaluation network.

References

1. Zmeev A.A., Machtakov S.G., Meshcheryakova T.V., Nikulina E.Yu., Rogozin E.A., Stukalov V.V., Khvostov V.A. *Metody i sredstva evoliutsionnogo i strukturnogo modelirovaniia pri obosnovanii trebovaniia k programmnyim sistemam zashchity informatsii* [Methods and means of evolutionary and structural modeling when justifying the requirements for information security software systems. Ed. by E.A. Rogozin]. Voronezh, Voronezh Institute of the Ministry of Internal Affairs of Russia Publ., 2015. 94 p.
2. Goldberg D. *Genetic Algorithms in Search, Optimization and Machine Learning*. Massachusetts, Addison-Wesley Publ., 1989, 343 p.
3. Dubrovin A.S., Makarov O.Iu., Muratov A.V., Poprygin G.I., Rogozin E.A., Sumin V.I., Shishkin V.M. *Metod formalizatsii funktsionirovaniia tipovykh programmnykh sistem zashchity informatsii* [The method of formalizing the functioning of typical software security systems for information]. *Telekommunikatsii*, 2002, No 8. pp. 33-40.
4. Sovetov B.Ia., Iakovlev S.A. *Modelirovanie sistem: ucheb. dlia vuzov* [Modeling of systems: textbook for universities]. Moscow, Vysshaia shkola Publ., 2001. 343 p.
5. Kostin A.E. *Printsipy modelirovaniia slozhnykh diskretnykh sistem* [Principles of modeling complex discrete systems]. Moscow, National Research University of Electronic Technology Publ., 1984. 140 p.
6. Praniavichius G.I. *Modeli i metody issledovaniia vychislitelnykh sistem* [Models and methods of computer systems research]. Vilnius, Mokslas Publ., 1982. 315 p.
7. Kostin A.E., Shangin V.F. *Organizatsiia i obrabotka struktur dannykh v vychislitelnykh sistemakh* [Organization and processing of data structures in computer systems]. Moscow, Vysshaia shkola Publ., 1987. 248 p.
8. Marakhovskii V.B., Rozenblium L.Ia., Iakovlev A.V. *Modelirovanie parallelnykh protsessov* [Simulation of parallel processes. Petri nets]. *Seti Petri*. St. Petersburg: Professionalnaia literatura Publ., 2014. 400 p.
9. Lomazova I.A. *Vlozhennye seti Petri: modelirovanie i analiz raspredelennykh sistem s obiektnoi strukturoi* [Embedded Petri nets: modeling and analysis of distributed systems with object structure]. Moscow, Nauchnyi mir Publ., 2004. 208 p.