УДК: 663.1:004.056 DOI: 10.24411/2075-4094-2018-16128

МЕТОДИКА ОЦЕНКИ НАДЕЖНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В.П. ГУЛОВ[*], В.П. КОСОЛАПОВ[*], Г.В. СЫЧ[*], А.В. СКРЫПНИКОВ[**], В.А. ХВОСТОВ[**]

[*]*ГБОУ ВО «Воронежский государственный медицинский университет им. Бурденко Н.Н. Минздрава России», ул. Студенческая, д.10, Воронеж, Россия, 394000*
[**]*ГБОУ ВО «Воронежский государственный университет инженерных технологий», пр-т. Революции, д.19, Воронеж, 394000, Россия*

Аннотация. Основой безопасности персональных данных, обрабатываемых в медицинских информационных системах, является высокое качество работы программных систем защиты информации от несанкционированного доступа. Наряду с требованием низкой ресурсоемкости и высоких показателей удобства использования, понятности и модифицируемости, одной из наиболее важных характеристик является надежность таких систем. При этом под надежностью понимается эффективность выполнения защитных функций в течение требуемого времени. Для проведения оценки этого показателя проведен анализ принципов построения и функционирования систем от несанкционированного доступа, используемых в медицинских информационных системах для обеспечения защиты. Для проведения оценки надежности систем защиты предложена методика, основанная на применении метода прямого перебора элементов программной системы с монотонной структурой. Количественное описание надежности систем защиты осуществляется по составной функции наиболее общего вида, отображающей функционирование системы в целом. При этом под отказом системы от несанкционированного доступа выбрано такое состояние, при котором нарушается состояние безопасности информации. Методика позволяет с приемлемой для практических приложений целей получить оценки надежности работы систем защиты информации применяемых при защите персональных данныхв медицинских информационных системах.

Ключевые слова: информационная безопасность, система с монотонной структурой, программный модуль, сложная программная система.

METHODOLOGY OF EVALUATION THE RELIABILITY OF THE INFORMATION PROTECTION SYSTEM FROM UNAUTHORIZED ACCESS TO THE MEDICAL INFORMATION SYSTEM

V.P. GULOV[*], V.P. KOSOLAPOV[*], G.V. SICH[*], A.V. SKRIPNIKOV[**], V.A. KHVOSTOV[**]

[*] *Voronezh State N. N. Burdenko Medical University of the Ministry of health of Russia, Studencheskaya Str., 10, Voronezh, 394036, Russia*
[**] *Voronezh State University of Engineering Technologies, Revolution Avenue, 19, Voronezh, 394000, Russia*

Abstract. The basis for the security of personal data (PDD) processed in medical information systems (IS) is the high quality of the operation of software information protection systems (PIC) from unauthorized access. Along with the requirement of low resource intensity and high indicators of ease of use, understandability and modifiability, one of the most important characteristics is the reliability of the ISS. At the same time, reliability means the effectiveness of performing protective functions for the required time. To assess this indicator, an analysis was made of the principles of constructing and operating the NTP from NDs used in medical information systems to provide protection (PDN). For the evaluation of the reliability of the CPS, a technique based on the application of the method of direct enumeration of the elements of a software system with a monotonic structure was proposed. Quantitative description of the reliability of protection systems is carried out by a composite function of the most general type, which reflects the functioning of the system as a whole. In this case, under the refusal of the NPL from the NSD, a state is selected in which the security state of the information is violated. With acceptable for practical applications, this methodology allows to estimating the reliability of the information protection systems used to protect personal data in medical information systems.

Key words: information security, system with a monotonous structure, software module, complex software system.

Как результат применения программных (программно-аппаратных) *систем защиты информации* (СЗИ) для обеспечения информационной безопасности *медицинских информационных систем* (МИС) от *несанкционированного доступа* (НСД) обнаруживается ряд проблем. Основной проблемой является уменьшение надежности СЗИ от НСД во времени, что подтверждается в ходе эксплуатации таких систем. В связи с этим, обоснованию их надежности необходимо уделять повышенное внимание. Однако

методической основы формирования требований к надежности СЗИ от НСД уделено не достаточное внимание, что обуславливает актуальность предложенной в данной статье методики оценки надежности.

В соответствии со сложившимся к настоящему времени методическим подходом оценки надежности сложных *программных систем* (ПС) в [2], необходимо провести анализ архитектурны и характеристики функционирования СЗИ от НСД.

Как объект оценки надежности критически важным свойством СЗИ от НСД является их модульно-иерархическая структура, которая отражает декомпозицию на программные модули и связи между ними. Установившаяся практика иерархического многоуровневого построения сложных ПС применяется для упрощения разработки сложных программных комплексов, их концептуального проектирования и повседневной эксплуатации, уменьшения затрат и времени на разработку, оптимизации усилий и позволяет рассматривать СЗИ от НСД при разработке методик расчётов надежности как программную систему с расчлененной структурой.

Надежность элементов системы с расчлененной структурой позволяет независимое формирование показатели надежности. При этом, показатели надежности могут быть определены заранее, так как отказы в данных обстоятельствах могут рассматриваться как случайные события, независимо от достигнутых состояний остальных программных модулей. Каждый элемент программной системы расчлененной структуры имеет множество выходных параметров, влияющих только на работоспособность этого элемента.

По принципу построения программной системы, языкам описания, объему и остальным характеристикам можно четко выделить следующие иерархические уровни сложных ПС [6]:

– соответствующий компонентам текста программы уровень операторов и операндов программ на языке программирования;

– законченные компоненты текста программы как уровень программных модулей;

– пакетов прикладных программ как уровень функциональных групп программ;

– завершенный программный продукт определенного целевого назначения как уровень комплексов программ.

В качестве целесообразного уровня иерархии сложных ПС для разработки методики оценки надежности СЗИ от НСД необходим выбор уровня программных модулей. Этот выбор обусловлен рядом особенностей данного уровня:

– программный модуль реализует функциональную задачу и, соответственно, достаточно сложный;

– показатель надежности характеризует его в целом, а не его составные части;

– восстановление работоспособности дискретного программного модуля реализуется независимо от восстановления остальных программных модулей СЗИ от НСД.

Для построения схемы связей элементов СЗИ от НСД была использована техническая документация современной СЗИ [1, 2]. В результате была составлена последовательность выполнения программных модулей СЗИ от НСД, представленная на рис. 1.

X_1 – аппаратная составляющая СЗИ от НСД;

X_2 – модуль идентификации и аутентификации;

X_3 – модуль контроля целостности исполняемых файлов;

X_4 – модуль администрирования СЗИ от НСД;

X_5 – локальные базы учетных записей;

X_6 – модуль управления доступом;

X_7 – модуль аудита, сигнализации об НСД и блокировки ПЭВМ;

X_8 – сетевые службы СЗИ;

X_9 – модуль учета и маркировки документов;

X_{10} – модуль преобразования носителей информации;

X_{11} – интерфейс с низкоуровневыми средствами операционной системы;

X_{12} – модуль пользовательских служб СЗИ от НСД.

В соответствии с параметром времени программные модули СЗИ то НСД, приведенные на рис. 1, подразделяться на четыре типа.

Первый тип модулей запускается на исполнение при загрузке защищенной ПЭВМ. К нему относятся: аппаратная составляющая СЗИ от НСД; программный модуль идентификации и аутентификации; программный модуль контроля целостности; программный модуль аудита, сигнализации НСД и блокировки ПЭВМ.

Второй тип модулей запускается на исполнение при выполнении работы пользователя на ПЭВМ. К этому типу относятся: программный модуль разграничения доступа (по правилам дискреционного и мандатного принципов доступа) к защищаемым ресурсам; программный модуль учета и маркировки документов; программный модуль преобразования носителей информации; программный обеспечивающий интерфейс СЗИ от НСД с операционной системой; сетевые службы.

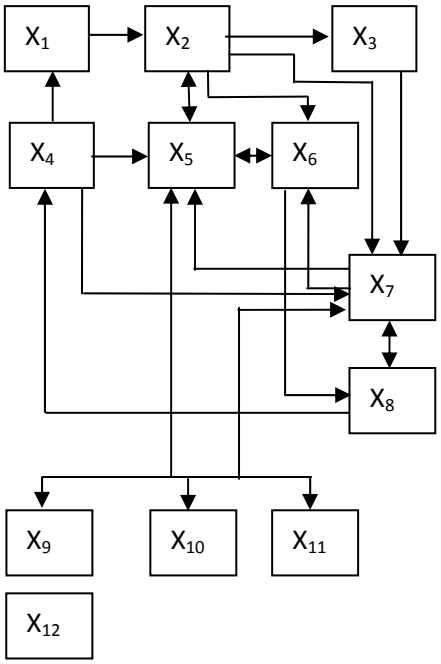

Рис. 1. Последовательность выполнения программных модулей СЗИ от НСД

Третий тип модулей СЗИ от НСД запускается по пользовательскому запросу. К нему относятся ряд пользовательских служб (просмотр прав доступа и смена меток, контроль целостности по запросу, блокировка монитора, маскирующее удаление).

Четвертый тип модулей запускается при администрировании и управлении СЗИ от НСД.

Таким образом, СЗИ от НСД можно характеризовать как сложную структуру. Структура СЗИ не может быть сведена к последовательно-параллельным или параллельно-последовательным соединениям. В литературе по проблемам надежности [2] такие системы обычно называются системами с монотонной структурой. Их можно характеризовать следующим свойством: при отказе любого элемента ухудшается надежность всей системы или ее полный отказ.

Оценка надежности систем представляющей собой монотонную структуру осуществляется в соответствии с методикой разработанной в [3]. Учитывая небольшое количество программных модулей СЗИ, а также на основе вывода о сложности использования методов оценки надежности систем с монотонной структурой на основе метода разложения относительного особого элемента, использования имитационного моделирования функционирования СЗИ, минимальных разрезов и путей при расчетах применяется метод основанный на прямом переборе элементов.

С учетом выбранного метода оценки надежности СЗИ от НСД как ПС с монотонной структурой введем критерий отказа этой системы, определяющий деление множества возможных состояний на два подмножества: подмножество *j* работоспособных состояний $\{\Omega\}$ и подмножество состояний отказа $\{\Psi\}$.

Как показано в [6-8] в качестве количественного описания надежности используется каждая функция ПС в отдельности, или по составная функция общего вида, отображающая работу ПС в целом. Проведя анализ состава выполняемых СЗИ функций [1], при выборе критериев отказа можно применить подход с использованием составной функции. В качестве составной функции СЗИ необходимо выбрать обеспечение информационной безопасности АС. Под отказом СЗИ в таком случае понимается состояние, при котором в системе нарушена безопасности информации.

В качестве признаков состояния отказа СЗИ необходимо выбрать следующие:

– реализована возможность входа в операционную среду АС без идентификации и аутентификации;

– возможен доступ к информации в обход установленной политики разграничения доступа;

– можно реализовать запись информации высшего уровня конфиденциальности на носители низшего уровня;

– не выполняется контроль целостности файлов настройки операционной системы;

– отсутствует реакция на реализацию угроз безопасности информации.

Условием отказа СЗИ от НСД является появление хотя бы одного из указанных выше признаков нарушения работоспособности.

Система защиты, состоит из n программных модулей. Каждый модуль находится в состоянии отказа или в состоянии работоспособности. Система защиты, соответственно может находиться в 2^n различных состояниях:

H_0 – все n программных модулей СЗИ работоспособны;

H_i – отказал i - ый программный модуль СЗИ, остальные работоспособны;

H_{ij} – отказал i -ый и j -ый программные модули СЗИ, остальные работоспособны;

……

$H_{1,2,\ldots n}$ – отказали все программные модули СЗИ.

Пусть для каждого состояния $H_a \in \{H\}$ определена вероятность этого события P_a. Тогда вероятность работоспособного состояния СЗИ определяется как:

$$P\{H_a \in \Omega\} = \sum_{H_a \in \Omega} P_a \qquad (1)$$

С учетом независимости программных модулей вероятности состояний H_a определяются в соответствии с формулами [2]:

$$P_0 = \prod_{i=1}^{n} P_i \; ; \qquad P_{i,j} = \gamma_i * \gamma_j \prod_{k=1, k\neq i,j}^{n} P_k \; ; \qquad (2)$$

$$P_{1,2,3,\ldots n} = P_0 \prod_{i-1}^{n} \gamma_i = \prod_{i=1}^{n} Q_i$$

где P_i и Q_i вероятности состояния работоспособности и отказа i - ого программного модуля; $\gamma_i = Q_i / P_i$.

Исходя из принципов построения и функционирования СЗИ от НСД, можно определить ее состояния, при которых отказы отдельных программных модулей не приводят к отказу в целом в соответствии с введенным критерием. Перечень таких состояний представлен в табл. 1.

Таблица 1

Перечень работоспособных состояний СЗИ

№ состояния	Состояния программных модулей											
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}
0	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	0	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	0	1	1	1	1
3	1	1	1	1	1	1	1	1	1	1	0	1
4	1	1	1	1	1	1	1	1	1	1	1	0
5	1	1	1	0	1	1	1	0	1	1	1	1
6	1	1	1	0	1	1	1	1	1	1	0	1
7	1	1	1	0	1	1	1	1	1	1	1	0
8	1	1	1	1	1	1	1	0	1	1	0	1
9	1	1	1	1	1	1	1	0	1	1	1	0
10	1	1	1	1	1	1	1	1	1	1	0	0
11	1	1	1	0	1	1	1	0	1	1	0	1
12	1	1	1	1	1	1	1	0	1	1	0	0
13	1	1	1	0	1	1	1	0	1	1	1	0
14	1	1	1	0	1	1	1	1	1	1	0	0
15	1	1	1	0	1	1	1	0	1	1	0	0

В табл. 1 $x_i = 1$ и $x_i = 0$ означает, что программный модуль СЗИ находится соответственно в работоспособном состоянии и в состоянии отказа.

Подставив выражения (2) в (1) применительно к перечню работоспособных состояний СЗИ от НСД, представленному в табл. 1, получим окончательное выражение методики для расчета вероятности правильного выполнения защитных функций системы:

$$P_{szi} = P_0(1 + \gamma_4 + \gamma_8 + \gamma_{11} + \gamma_{12} + \gamma_4\gamma_8 + \gamma_4\gamma_{11} + \gamma_4\gamma_{12} + \gamma_8\gamma_{11} + \gamma_8\gamma_{12} + \gamma_{11}\gamma_{12} +$$
$$\gamma_4\gamma_8\gamma_{11} + \gamma_8\gamma_{11}\gamma_{12} + \gamma_4\gamma_8\gamma_{12} + \gamma_4\gamma_{11}\gamma_{12} + \gamma_4\gamma_8\gamma_{11}\gamma_{12})$$

Показатель p_i, входящий в математические выражения (2), имеет смысл вероятности безотказной работы программного модуля СЗИ от НСД в течение заданного времени. Как показано в [6], наилучшей аппроксимацией для данного показателя является экспоненциальный закон распределения.

$P_i(t) = 1 - \exp(-\lambda_i t)$, где t – параметр времени; λ_i – параметр потока ошибок в процессе эксплуатации i-го программного модуля СЗИ от НСД.

Значение параметра λ_i с достаточной для проводимых расчетов точностью можно определить как: $\lambda_i = \overline{\lambda_{cp}} * V_{np}$, где $\overline{\lambda_{cp}}$ – средняя интенсивность проявления ошибок в процессе эксплуатации программной системы (составляет величину примерно 10^{-7} на символ объектного кода программы [6]); V_{np} – объем программы в символах объектного кода.

С использованием разработанной методики оценки надежности СЗИ от НСД были проведены расчеты вероятности правильного выполнения защитных функций системы в течение десяти часов. В качестве исходных данных использовались значения параметра V_{np} программных модулей СЗИ «Ребус», полученные в результате ее сертификационных испытаний. Результаты расчетов представлены на рис. 2.

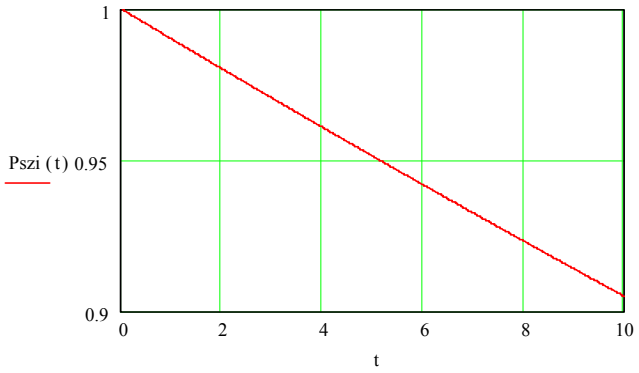

Рис. 2. Зависимость вероятности правильного выполнения защитных функций СЗИ от времени

Таким образом, для расчета вероятности правильного выполнения защитных функций СЗИ от НСД в МИС применим метод прямого перебора элементов программной системы с монотонной структурой, позволяющий с приемлемой для практических расчетов точностью получать значения показателя надежности ее работы.

Литература

1. Гулов В.П., Полтавченко А.Г., Попов А.С., Хвостов В.А., Чумаков А.А. Обоснование комплекта средств защиты информации на объектах биологической деятельности при проведении вирусологических исследований // Научно-медицинский вестник Центрального Черноземья. 2012. №47 (1 квартал) С. 14–19.

2. Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/ Bulletin/E2015-2/ 5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/ 11910.

3. Гулов В.П., Попов А.С., Хвостов В.А., Чумаков А.А. Обоснование комплекта средств защиты информации при проведении молекулярно-биологических и генно-инженерных исследований // Прикладные информационные аспекты медицины. 2011. Т. 16, № 2 С. 59–64

4. Информационная технология ISO/МЭК 8631-89. Программные конструктивы и условные обозначения для их представления.

5. Липаев В.В. Надежность и функциональная безопасность комплексов программ реального времени. М.: Изд. Светлица, 2013.

6. Липаев В.В. Проблемы программной инженерии. Лекции ведущих ученых России. Красноярск: СФУ, 2011.

7. Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. URL: http://www.rubinteh.ru/public/opis30.pdf (дата обращения: 04.11.2017).

8. Страж NT. Руководство администратора. URL: http://www.guardnt.ru/download/doc/ ad-

min_guide_nt_3_0.pdf (дата обращения: 03.11.2017).

References

1. Gulov VP, Poltavchenko AG, Popov AS, Hvostov VA, CHumakov AA. Obosnovanie komplekta sredstv zashchity informacii na ob"ektah biologicheskoj deyatel'nosti pri provedenii virusologicheskih issledovanij. Nauchno-medicinskij vestnik Central'nogo CHernozem'ya. 2012;47 (1):14-9. Russian.

2. Gulov VP, Hvostov VA, CHesnokov PE. Detal'nyj algoritm mnozhestva realizacij ugroz informacionnoj bezopasnosti v medicinskoj informacionnoj sisteme. Vestnik novyh medicin-skih tekhnologij. EHlektronnoe izdanie. 2015 [cited 2015 Jun 30];2[about 6 p.]. Russian. Available from: http://www.medtsu.tula.ru/VNMT/ Bulletin/E2015-2/ 5191.pdf. DOI: 10.12737/ 11910.

3. Gulov VP, Popov AS, Hvostov VA, CHumakov AA. Obosnovanie komplekta sredstv zashchity informacii pri provedenii molekulyarno-biologicheskih i genno-inzhenernyh issledovanij. Pri-kladnye informacionnye aspekty mediciny. 2011;16(2):59-64. Russian.

4. Informacionnaya tekhnologiya ISO/MEHK 8631-89. Programmnye konstruktivy i uslovnye oboznacheniya dlya ih predstavleniya. Russian.

5. Lipaev VV. Nadezhnost' i funkcional'naya bezopasnost' kompleksov programm real'nogo vremeni. Moscow: Izd. Svetlica; 2013. Russian.

6. Lipaev VV. Problemy programmnoj inzhenerii. Lekcii vedushchih uchenyh Rossii. Krasnoyarsk: SFU; 2011. Russian.

7. Sistema zashchity informacii ot nesankcionirovannogo dostupa «Strazh NT». Opisanie primeneniya. Russian. Available from: http://www.rubinteh.ru/public/opis30.pdf.

8. Strazh NT. Rukovodstvo administratora. Russian. Available from: http://www.guardnt.ru/download/doc/ ad-min_guide_nt_3_0.pdf.

Библиографическая ссылка:
Гулов В.П., Косолапов В.П., Сыч Г.В., Скрыпников А.В., Хвостов В.А. Методика оценки надежности системы защиты информации от несанкционированного доступа медицинской информационной системы // Вестник новых медицинских технологий. Электронное издание. 2018. №4. Публикация 2-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2018-4/2-4.pdf (дата обращения: 13.07.2018). DOI: 10.24411/2075-4094-2018-16128. *
* номера страниц смотреть после выхода полной версии журнала: URL: http://medtsu.tula.ru/VNMT/Bulletin/E2018-4/e2018-4.pdf