УДК 004.056.5:004.52

Е.Н. МАЩЕНКО, А.О. СМАГИНА

Севастопольский национальный технический университет, Украина

ИССЛЕДОВАНИЕ ГАРАНТОСПОСОБНОСТИ ЧЕЛОВЕКО-МАШИННОЙ СИСТЕМЫ НЕОДНОРОДНОГО СОСТАВА НА ОСНОВЕ ПОЛУМАРКОВСКОЙ МОДЕЛИ

Рассмотрена задача исследования гарантоспособности человеко-машинной системы неоднородного состава и нахождения вероятности пребывания системы в полностью защищенном состоянии, вероятности пребывания системы в процессе отражения атаки определенного типа. Предложена полумарковская модель, описывающая реакцию системы на атаки различного типа. Проведено имитационное моделирование полумарковских процессов с непрерывным множеством состояний, в результате чего исследованы характеристики гарантоспособности с точки зрения контроля доступа. Полученные результаты могут быть использованы в системах поддержки принятия решений.

Ключевые слова: *гарантоспособность, человеко-машинная система, полумарковская модель, контроль доступа.*

Введение

В настоящее время функционирование современных человеко-машинных систем (ЧМС) требует специальной организации защиты доступа к их ресурсам. Используемые средства контроля доступа не всегда могут обеспечить требуемый уровень безопасности, что приводит к необходимости модификации системы защиты [1].

Как утверждают авторы работы [2] и эта концепция далее будет развита нами: «повышение свойств информационной безопасности (целостности, конфиденциальности) приводит с одной стороны, к повышению готовности благодаря уменьшению вероятности успешных атак, а с другой, – к дополнительным затратам времени на проведение профилактических работ, что может вызвать потери готовности». В рамках данной статьи предлагается развитие методов системного анализа, ориентированных на решение задач противодействия внешним атакам на ЧМС, направленным на нарушение их нормального функционирования. Из всех первичных свойств гарантоспособности в данном случае наиболее важными представляются такие свойства, как безотказность, функциональная безопасность, целостность, конфиденциальность [3].

Для систем неоднородного состава предлагается установить защиту следующей структуры: для получения доступа к ресурсам ЧМС необходим последовательный ввод трех ключей – программной компоненты (П-компоненты), аппаратной компоненты (Т-компоненты) и пароль оператора (Ч-компоненты). Предполагаем, что атака нарушителя может быть направлена на взлом этих ключей и завершена успешно, если нарушитель получил несанкционированное право доступа ко всей системе, т.е. к каждой ее компоненте. Если у нарушителя нет хотя бы одного из ключей, атаки могут быть продолжены. Интервалы между атаками являются случайными величинами. После обнаружения факта успешной атаки в системе начинается случайный процесс восстановления, который оканчивается восстановлением защиты системы [4, 5].

Задача заключается в построении полумарковской модели человеко-машинной системы неоднородного состава и нахождении следующих характеристик: вероятность нахождения системы в полностью защищенном состоянии; вероятности нахождения системы в процессе отражения атаки определенного типа. Методика построения полумарковских моделей приведена в [6].

1. Формальная постановка задачи

Граф (рис. 1) соответствует системам неоднородного состава, состоящим из человека-оператора, выполняющего функции ЛПР, связанные с управлением политикой безопасности, настройкой программ или обслуживанием технической части, программной части П, и технической части Т.

Состояния системы описываются с точки зрения получения нарушителя доступа к функциям ЧМС. В этом случае рассматриваемые системы могут находиться в следующих состояниях:

1) S_0 — право доступа к функциям оператора, П и Т-компонентам закрыто (ЧПТ);

2) S_1 — право доступа к функциям оператора получено, доступ к П и Т-компонентам закрыт ($\overline{\text{Ч}}\text{ПТ}$);

3) S_2 — право доступа к функциям оператора и Т-компоненты закрыто, доступ к П-компоненте получен ($\text{Ч}\overline{\text{П}}\text{Т}$);

4) S_3 — право доступа к функциям оператора и П-компоненте закрыто, доступ к Т-компоненте получен ($\text{ЧП}\overline{\text{Т}}$);

5) S_4 — доступ к Т-компоненте закрыт, право доступ к функциям оператора и П-компоненте получено ($\overline{\text{Ч}}\overline{\text{П}}\text{Т}$);

6) S_5 — право доступа к функциям оператора закрыто, доступ к П и Т-компонентам получен ($\text{Ч}\overline{\text{П}}\overline{\text{Т}}$);

7) S_6 — доступ к П-компоненте закрыт, право доступа к функциям оператора и Т-компоненте получено ($\overline{\text{Ч}}\overline{\text{П}}\overline{\text{Т}}$);

8) S_7 — все три ключа вскрыты ($\overline{\text{Ч}}\overline{\text{П}}\overline{\text{Т}}$).

Стойкость компонент ЧМС характеризуется следующими показателями:

а) для человека-оператора — интенсивность атак ξ и интенсивность восстановления криптостойкости системы ν ($ч^{-1}$);

б) для программной части — интенсивность атак ε ($ч^{-1}$) и интенсивность восстановления криптостойкости системы θ ($ч^{-1}$);

в) для технической части — интенсивность атак λ ($ч^{-1}$) и интенсивность восстановления криптостойкости системы μ ($ч^{-1}$).

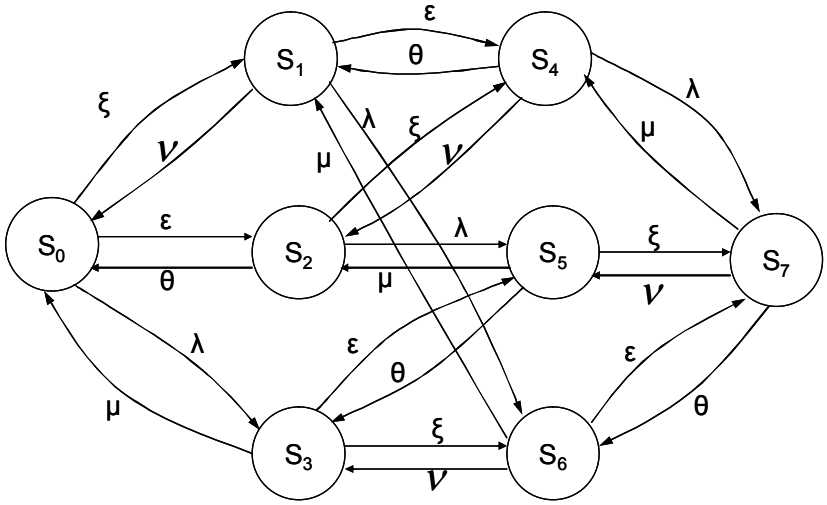

Рис. 1. Граф состояний ЧМС

2. Полумарковская модель системы

Рассмотрим фрагмент системы. В начальный момент времени система находится в защищенном состоянии по всем компонентам. Время до успешного завершения атаки по Ч-компоненте – случайная величина (СВ) α_1 с произвольной функцией распределения (ФР) $F_1\{\alpha_1 \le t\}$, время восстановления Ч-компоненты после успешной атаки – СВ α_2 с произвольной ФР $F_2\{\alpha_2 \le t\}$. Время до успешного завершения атаки по П-компоненте – СВ β_1 с произвольной ФР $G_1\{\beta_1 \le t\}$, время восстановления – СВ β_2 с произвольной ФР $G_2\{\beta_2 \le t\}$. Время до успешного завершения атаки по Т-компоненте – СВ γ_1 с произвольной ФР $H_1\{\gamma_1 \le t\}$, время восстановления – СВ γ_2 с произвольной ФР $H_2\{\gamma_2 \le t\}$. СВ $\alpha_i, \beta_i, \gamma_i$ предполагаются независимыми, имеющими конечные математические ожидания и дисперсии; у ФР $F_i(t)$, $G_i(t)$, $H_i(t)$ существуют плотности $f_i(t)$, $g_i(t)$, $h_i(t)$, $i = 1,2$.

Для упрощения будем считать, что атаки происходят последовательно по следующей схеме: Ч-компонента, П-компонента, Т-компонента. Будем также считать, что восстановление после атак происходит также последовательно в обратном порядке.

Введем следующую кодировку состояний ЧМС: $i\,j\,k$, где i – индикатор контроля доступа к Ч-компоненте: $i = 0$ – защищенное состояние; $i = 1$ – атака на компоненту завершена успешно; j – индикатор контроля доступа к П-компоненте: $j = 0$ – защищенное состояние; $j = 1$ – атака на компоненту завершена успешно; k – индикатор контроля доступа к Т-компоненте: $k = 0$ – защищенное состояние; $k = 1$ – атака на компоненту завершена успешно.

Для описания функционирования системы определим следующие полумарковские состояния:

1) 111 – система находится в полностью защищенном состоянии;

2) 011 – атака по Ч-компоненте завершилась успешно, проводится восстановление;

3) 001 – атака по П-компоненте завершилась успешно, контроль над Ч-компонентой не восстановлен, проводится восстановление Ч- и П-компонент;

4) 000 – атака по Т-компоненте прошла успешно, контроль над всей системой отсутствует, проводится восстановление по всем трем компонентам.

Таким образом, пространство состояний E имеет вид:

$$E = \{111, 011, 001, 000\}.$$

Опишем события переходов:

1) $\{111 \to 011\} = \{I\}$ – успешное завершение атаки по Ч-компоненте;

2) $\{011 \to 001\} = \{\beta_1 < \alpha_2\}$ – момент успешного завершения атаки по П-компоненте наступил раньше восстановления контроля по Ч-компоненте;

3) $\{011 \to 111\} = \{\alpha_2 < \beta_1\}$ – произошло восстановление контроля по Ч-компоненте;

4) $\{001 \to 000\} = \{\gamma_1 < \beta_2\}$ – момент успешного завершения атаки по Т-компоненте наступил раньше восстановления контроля по П-компоненте;

5) $\{001 \to 011\} = \{\beta_2 < \gamma_1\}$ – произошло восстановление контроля по П-компоненте;

6) $\{000 \to 001\} = \{I\}$ – произошло восстановление контроля по Т-компоненте, где $\{I\}$ – единичное событие.

Определим времена пребывания в состояниях системы:

$$\theta_{000} = \gamma_2; \theta_{011} = \min\{\alpha_2, \beta_1\}$$

$$\theta_{001} = \min\{\gamma_1, \beta_2\}; \theta_{111} = \alpha_1.$$

Средние времена пребывания в состояниях:

$$\text{Ì}\ (011) = M(\min\{\alpha_2, \beta_1\}) = \int_0^\infty \overline{F}_2(t)\,\overline{G}_1(t)dt;$$

$$\text{Ì}\ (001) = M(\min\{\gamma_1, \beta_2\}) = \int_0^\infty \overline{H}_2(t)\,\overline{G}_2(t)dt;$$

$$M(111) = M\alpha_1;\ M(000) = M\gamma_2;$$

где $\overline{F}_2(t) = 1 - F_2(t);$ $\overline{G}_1(t) = 1 - G_1(t);$

$\overline{G}_2(t) = 1 - G_2(t);$ $\overline{H}_2(t) = 1 - H_2(t);$

Граф состояний и переходов системы изображен на рис. 2.

Определим вероятности переходов вложенной цепи Маркова:

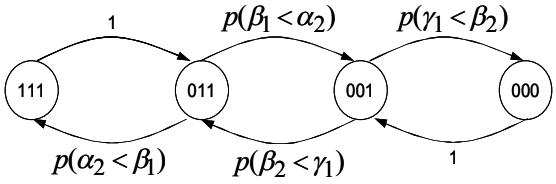

Рис. 2. Граф состояний и переходов системы

$$p\langle 011 \to 001\rangle = p(\beta_1 < \alpha_2) = \int_0^\infty f_2(x_2 + t)g_1(t)dt;$$

$$p\langle 011 \to 111\rangle = p(\alpha_2 < \beta_1) = \int_0^\infty f_2(t)g_1(y_1 + t)dt;$$

$$p\langle 001 \to 011\rangle = p(\beta_2 < \gamma_1) = \int_0^\infty g_2(y_2 + t)h_1(t)dt;$$

$$p\langle 001 \to 000\rangle = p(\gamma_1 < \beta_2) = \int_0^\infty g_2(t)h_1(z_1 + t)dt.$$

На основе построенной модели можно определить следующие характеристики:

1) $P_{\text{защ}}$ – стационарная вероятность того, что система находится в защищенном состоянии по всем компонентам;

2) $P_{\text{ЧПТ}}$ – стационарная вероятность того, что система находится в состоянии взлома всех компонент;

3) $P_{\text{Ч}}$ – стационарная вероятность того, что система находится в состояниях взлома Ч-компоненты;

4) $P_{\text{П}}$ – стационарная вероятность того, что система находится в состояниях взлома П-компоненты.

Определим необходимые для вычисления характеристик подмножества состояний:

1) $E_{\text{защ}}$ – подмножество состояний, в которых система находится в защищенном состоянии по всем компонентам (состояния, в которых все индексы $= 1$): $E_{\text{защ}} = \{111\}$;

2) $E_{\text{ЧПТ}}$ – подмножество состояний, в которых система находится в состоянии взлома всех компонент (состояния, в которых все индексы $= 0$): $E_{\text{ЧПТ}} = \{000\}$;

3) $E_{\text{Ч}}$ – подмножество состояний, в которых произошел взлом Ч-компоненты (состояния, в которых первый индекс $i = 0$): $E_{\text{Ч}} = \{011, 001, 000\}$;

4) $E_{\text{П}}$ – подмножество состояний, в которых произошел взлом П-компоненты (состояния, в которых второй индекс $j = 0$): $E_{\text{П}} = \{001, 000\}$;

Определим следующие времена:

1) $\overline{T}$ – среднее время функционирования системы от события восстановления защиты по всем компонентам до такого же события;

2) $\overline{T}_{ЧПТ}$ – среднее время функционирования системы в состоянии взлома всех компонент;

3) $\overline{T}_{защ}$ – среднее время функционирования системы в защищенном состоянии по всем компонентам;

4) $\overline{T}_{Ч}$ – среднее время функционирования системы в состоянии взлома Ч- компоненты;

5) $\overline{T}_{П}$ – среднее время функционирования системы в состоянии взлома П- компоненты.

Тогда искомые характеристики на основе полумарковской модели определяются следующим образом:

$$P_{защ} = \frac{\overline{T}_{защ}}{\overline{T}} = \frac{\sum_{i \in E_{защ}} \overline{T_i}}{\overline{T}}; \quad (1)$$

$$P_{ЧПТ} = \frac{\overline{T}_{ЧПТ}}{\overline{T}} = \frac{\sum_{i \in E_{ЧПТ}} \overline{T_i}}{\overline{T}}; \quad (2)$$

$$P_{Ч} = \frac{\overline{T}_{Ч}}{\overline{T}} = \frac{\sum_{i \in E_{Ч}} \overline{T_i}}{\overline{T}}; \quad (3)$$

$$P_{П} = \frac{\overline{T}_{П}}{\overline{T}} = \frac{\sum_{i \in E_{П}} \overline{T_i}}{\overline{T}}, \quad (4)$$

где T_i – средние времена пребывания в состояниях заданного подмножества.

3. Имитационное моделирование

Ввиду сложности получения аналитических выражений для искомых характеристик расчет проводился с использованием следующего алгоритма имитационного моделирования полумарковских процессов с непрерывным множеством состояний:

1. Выбирается начальное состояние системы Sk = Sh. Время моделирования устанавливается в ноль.

2. С помощью генератора псевдослучайных чисел генерируются случайные величины α_{kr} с заданным законом распределения (случайные факторы, влияющие на время пребывания в данном состоянии); случайная величина α_{kr} определяет время до перехода из состояния k в состояние r.

3. Выбирается $\min\{\alpha_{kr}\}$ – минимальный случайный фактор, который и будет равен времени пребывания в данном состоянии; время моделирования увеличивается на величину $\min\{\alpha_{kr}\}$:

$$t_{мод} = t_{мод} + \min\{\alpha_{kr}\}.$$

4. Система переходит из состояния k в состояние r: Sk->Sr.

П.п. 2-4 повторяются до тех пор, пока время моделирования не превысит конечного значения: tмод ≥ tкон.

Параметры модели следующие: время моделирования – 5000 мин; интенсивности атак всех типов распределены экспоненциально, время восстановления после атак на Ч-компоненту – равномерно распределено на интервале [1, 3] со средним m=2 мин; время восстановления после атак на П-компоненту – равномерно распределено на интервале [4,6] со средним m=5 мин; время восстановления после атак на Т-компоненту – равномерно распределено на интервале [8, 12] со средним m=10 мин.

Первая группа экспериментов: интенсивность атак на Ч-компоненту ξ изменяется в диапазоне от 0.02 до 0.2 мин$^{-1}$; интенсивность атак на П-компоненту ε - 0,05 мин$^{-1}$; интенсивность атак на Т-компоненту λ – 0,03 мин$^{-1}$.

Результаты моделирования приведены на рис. 3 и в табл. 1.

Таблица 1

Оценка вероятностей $P_{ЧПТ}$, $P_{Ч}$, $P_{П}$

ξ, мин$^{-1}$	0,020	0,022	0,025	0,029	0,033
$P_{ЧПТ}$	0,01	0,02	0,01	0	0,01
$P_{Ч}$	0,03	0,03	0,05	0,06	0,06
$P_{П}$	0,02	0,01	0,01	0,01	0,01
ξ, мин$^{-1}$	0,040	0,050	0,067	0,100	0,200
$P_{ЧПТ}$	0,01	0,01	0,01	0,02	0,01
$P_{Ч}$	0,06	0,09	0,12	0,16	0,3
$P_{П}$	0,02	0,03	0,04	0,06	0,09

Вторая группа экспериментов (рис. 4): интенсивность атак на Ч-компоненту – 0,02 мин-1; интенсивность атак на П-компоненту – изменяется в диапазоне от 0.01 до 0.2 мин-1; интенсивность атак на Т-компоненту – 0,03 мин-1.

Третья группа экспериментов (рис. 5): интенсивность атак на Ч-компоненту – 0,02 мин-1; интенсивность атак на П-компоненту – 0,05 мин-1; интенсивность атак на Т-компоненту изменяется в диапазоне от 0.01 до 0.2 мин-1.

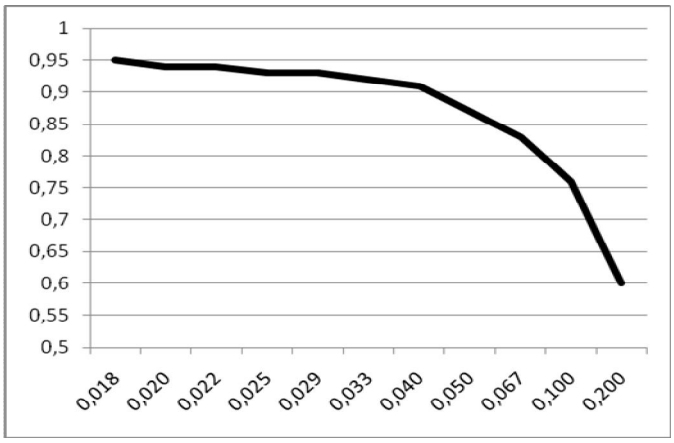

Рис. 3. Зависимость вероятности $P_{защ}$ от интенсивности атак на Ч-компоненту

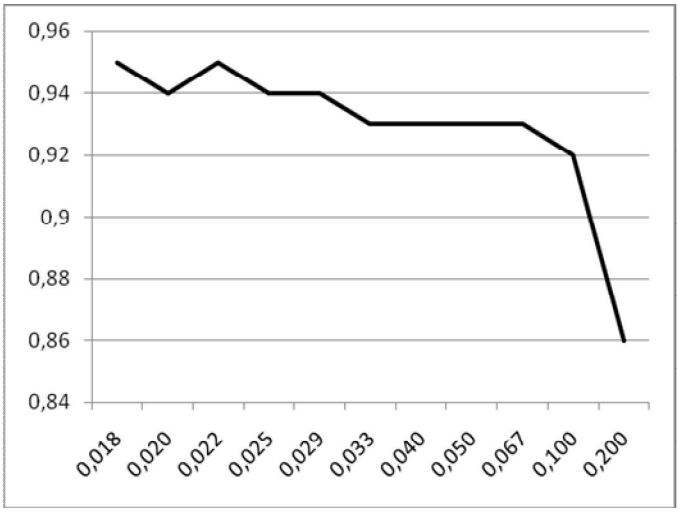

Рис. 4. Зависимость вероятности $P_{защ}$ от интенсивности атак на П-компоненту

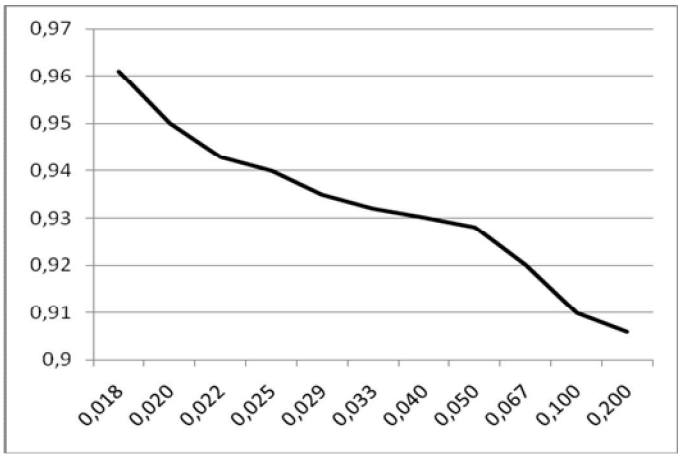

Рис. 5. Зависимость вероятности $P_{защ}$ от интенсивности атак на Т-компоненту

Выводы

Как видно из рис. 3-5, стационарная вероятность того, что система находится в защищенном состоянии по всем компонентам в большой степени зависит от интенсивности атак на Ч-компоненту. Интенсивность атак на П-компоненту оказывает меньшее влияние, и минимальное – интенсивность атак на Т-компоненту. Для обеспечения высокого уровня гарантоспособности необходимо создавать такую систему защиты Ч-компоненты, которая будет гарантировать вероятность полностью защищенного состояния не меньше некоторого предельного уровня, допустимого для систем критического применения.

Таким образом, построена полумарковская модель, описывающая реакцию системы на атаки раз-

личного типа, и исследованы характеристики гарантоспособности с точки зрения контроля доступа.

Перспективами дальнейших исследований является построение комплексных критериев эффективности управления процессами отражения атак в системе неоднородного состава. Полученные результаты могут быть использованы в системах поддержки принятия решений. Кроме того, предполагается расширить комплекс моделей управления процессом отражения атак без ограничений на последовательность восстановлений после отражений атак.

Литература

1. Охтилев, М.Ю. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов [Текст] / М.Ю. Охтилев, Б.В. Соколов, Р.М. Юсупов. – М.: Наука, 2006. – 410 с.

2. Бахмач, Е.С. Отказобесопасные информационно-управляющие системы на программируемой логике [Текст] / под. ред. В.С.Харченко, В.В. Скляра. – Национальный аэрокосмический университет «ХАИ», Научно-производственное предприятие «Радий», 2008. – 380 с.

3. Методы моделирования и дискретной оптимизации вычислительных систем реального времени [Текст] / В.Я. Жихарев, В.М. Илюшко, Л.Г. Кравец и др. – Житомир: ЖГУ, 2004. – 494 с.

4. Смагина, А.О. Статистическая оценка времени пребывания системы неоднородного состава в выделенных состояниях для нестационарного режима [Текст] / А.О. Смагина // Вестник СевГТУ: Информатика, электроника, связь: Сб. науч. тр. – Севатополь: СевНТУ, 2010. – Вып. 101. – С. 69 – 74.

5. Мащенко, Е.Н. Полумарковская модель человеко-машинной системы неоднородного состава [Текст] / Е.Н. Мащенко, А.О. Смагина // Інформаційні технології та інформаційна безпека в науці, техніці та навчанні "ІНФОТЕХ-2011": матеріали міжнар. НПК. – Севастополь, 05-10 верес. 2011. – Севастополь: СевНТУ, 2011. – С. 29 – 30

6. Королюк, В.С. Стохастические модели систем [Текст] / В.С. Королюк. – К.: Наук. думка, 1989. – 208 с.

Поступила в редакцию 23.02.2012

Рецензент: д-р техн наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

ДОСЛІДЖЕННЯ ГАРАНТОЗДАТНОСТІ ЛЮДИНО-МАШИННОЇ СИСТЕМИ НЕОДНОРІДНОГО СОСТАВА НА ОСНОВІ НАПІВМАРКОВСЬКОЇ МОДЕЛІ

О.М. Мащенко, Г.О. Смагіна

Розглянуто задачу дослідження гарантоздатності людино-машинної системи неоднорідного складу, знаходження ймовірності перебування системи в повністю захищеному стані, ймовірності перебування системи в процесі вібиття атаки певного типу. Запропонована напівмарківська модель, що описує реакцію системи на атаки різного типу. Проведено імітаційне моделювання напівмарківсих процесів з неперервною множиною станів, в результаті чого досліджені характеристики гарантоздатності з точки зору контролю доступу. Отримані результати можуть бути використані в системах підтримки прийняття рішень.

Ключові слова: гарантоздатність, людино-машинна система, напівмарковська модель, контроль доступу.

DEPENDABILITY INVESTIGATION OF MAN-MACHINE SYSTEM WITH INHOMOGENEOUS COMPOSITION, BASED ON SEMI-MARKOV MODEL

E.N. Maschenko, A.O. Smagina

The paper considers the issue of investigation of dependability of human-machine system of heterogeneous composition, determination of probability of fully safe system state and probability of system attack reflection state. The semi-Markov model describing the system response to the attacks of various types is proposed. The simulation of semi-Markov processes with continuous set of states in the form of three groups of expiriments is performed. As a result the dependability characteristics are examined in the terms of access control. Obtained results can be applied in the expert support systems.

Key words: dependability, man-machine system, semi-Markov model, access control.

Мащенко Елена Николаевна – канд. техн. наук, доцент, доцент кафедры кибернетики и вычислительной техники Севастопольского национального технического университета, Севастополь, Украина.

Смагина Анна Олеговна - аспирант кафедры кибернетики и вычислительной техники Севастопольского национального технического университета, Севастополь, Украина.