УДК 681.5(519.8765)

ПОЛУМАРКОВСКАЯ МОДЕЛЬ ОЦЕНКИ КОНФЛИКТНОЙ УСТОЙЧИВОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

И. А. Андреещев, С. А. Будников, А. В. Гладков

ВУНЦ ВВС «Военно-воздушная академия им. проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж)

Поступила в редакцию 20.10.2016 г.

Аннотация. На основе анализа типового сценария действий нарушителя при воздействии на информационную инфраструктуру, ответных реакций подсистемы обеспечения информационной безопасности информационной инфраструктуры произведено формализованное описание конфликта нарушителя и подсистемы обеспечения информационной безопасности. Разработана полумарковская модель функционирования информационной инфраструктуры в условиях конфликта нарушителя и подсистемы обеспечения информационной безопасности. Стационарная вероятность нахождения информационной инфраструктуры в выигрышном состоянии определена как функция эффективности подсистемы обеспечения информационной безопасности. На основе решения многокритериальной задачи оптимизации получены области допустимых значений технических показателей подсистемы обеспечения информационной безопасности при заданной вероятности функционирования информационной инфраструктуры в штатном режиме.
Ключевые слова: конфликтная устойчивость, полумарковская модель, информационная инфраструктура, информационная безопасность.
Annotation. Based on the analysis of typical offender action script when exposed to information infrastructure, responses subsystem to ensure information security of the information infrastructure – produced a formalized description of the conflict of the offender and the subsystem of information security. A semi-Markov model of the functioning information infrastructure in conflict offender and subsystem information security was developed. Stationary probability of finding the information infrastructure in a winning state of the process is defined such as the function of efficiency of information security subsystem. On the basis of the solution of multi-objective optimization problem obtained the tolerance range of technical indicators of information security subsystem at a given probability of the functioning information infrastructure in a normal mode.
Keywords: conflict stability, semi-Markov model, information infrastructure, information security.

В настоящее время средства информатизации (автоматизации) являются важной частью любой технологической инфраструктуры (финансовых систем, нефте- и газопроводов, железнодорожного и авиационного сообщения и др.), составляя информационную инфраструктуру (ИИ) предприятия, отрасли. Одним из основных требований к таким ИИ является обеспечение информационной безопасности (ИБ) [1]. Реализация этого требования закладывается в подсистеме обеспечения информационной безопасности (ПОИБ) либо на этапе разработки на основе априорной информации об уязвимостях, либо на этапе эксплуатации путем внедрения новых или обновленных методов и средств обеспечения ИБ (на техническом и операционном уровне). Однако, указанные подходы не в полном объеме учитывают априорную неопределенность современных компьютерных атак, стохастичность ответных реакций ПОИБ, компенсирующих последствия и возвращающих ИИ к штатному режиму функционирования, в том числе за счет привлечения дополнительных ресурсов.

Указанное выше обусловливает необходимость рассмотрения нового свойства ИИ, связанного с ее конфликтной устойчивостью. В этом случае, под конфликтной устой-

чивостью ИИ понимается ее способность в процессе функционирования поддерживать намеченный штатный режим, не смотря на воздействующие на нее внутри- и внешнесистемные деструктивные и (или) дестабилизирующие факторы, за счет формирования адекватных компенсирующих реакций.

Подход к исследованию конфликтной устойчивости сложных систем в настоящее время широко развивается и считается обоснованным при реализации централизованно-распределенных систем обеспечения ИБ [2]. На данный момент имеется большое количество работ по моделированию информационно-технических воздействий на системы связи на канальном, сетевом и транспортном уровнях OSI, а также моделированию влияния эффектов от таких воздействий на вышестоящие информационно-управляющие системы. Однако в них не рассматривается конфликтное взаимодействие средств информационно-технического воздействия и средств защиты ИИ в качестве конфликта [3].

Помимо этого, в большинстве работ вероятностно-временные характеристики случайных процессов, описывающих действия сторон в конфликте, аппроксимируются, в основном, только экспоненциальными распределениями [4], что дает приблизительные оценки. В работах [5; 6] на основании методологии системного анализа в процессе проектирования и оценки эффективности сложных систем, представленной в [7], обосновано применение аппарата имитационного моделирования с использованием формализма гибридных автоматов с реализацией в интегрированной среде MATLAB + Simulink + Stateflow для описания конфликта «информационная система – источник негативных воздействий». Применение данного подхода позволяет использовать любые законы распределения для описания случайных процессов, а также событийное взаимодействие сторон в конфликте. Однако, недостатком данного подхода, как и имитационного моделирования в целом, является отсутствие возможности получения аналитического выражения, описывающего конфликтное взаимодействие сторон.

Учитывая это, приемлемым подходом для описания информационного конфликта ПОИБ и нарушителя с целью получения аналитических выражений является методология полумарковских случайных процессов, представленная в [8], так как она позволяет рассматривать конфликт ПОИБ и нарушителя как взаимодействие сложных многоуровневых организационно-технических систем, использовать любые законы распределения для описания случайных процессов в конфликте, получать в аналитической форме зависимости «выигрыша» сторон в конфликте от совокупности показателей эффективности проводимых мероприятий.

Целью работы является разработка полумарковской модели функционирования ИИ в условиях конфликта нарушителя и ПОИБ и на ее основе оценка конфликтной устойчивости ИИ.

При проектировании самой ИИ и ПОИБ разработчики используют полные знания о возможных уязвимостях и применяют все возможные средства для их устранения. Тем самым, считается, что на момент ввода в эксплуатацию ИИ полностью защищена. Однако, в процессе эксплуатации, а также при обновлении или модернизации программного и аппаратного обеспечения проявляются новые уязвимости ИИ, обнаружение и своевременное устранение которых затруднительно. Это приводит к необходимости завышения требований к обеспечению ИБ ИИ.

Как известно [2], современные сетевые атаки, проводимые нарушителем, представляют собой сложную последовательность большого числа согласованных по месту, времени и задействованным ресурсам взаимосвязанных этапов по обнаружению уязвимости, выработки замысла использования данной уязвимости, разработки специального программного обеспечения, проведения атаки и доведения ИИ до деградации (снижения эффективности функционирования) или состояния полного отказа.

С другой стороны, защитные действия ПОИБ в процессе эксплуатации ИИ направлены на упреждающий поиск новых уязвимостей, модификацию ИИ для их закрытия,

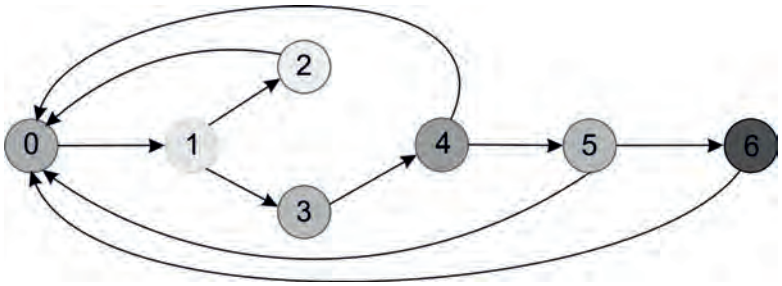


Рис. 1. Граф динамики конфликта нарушителя и ПОИБ

обнаружение признаков компьютерной атаки и ее блокирование в случае правильного обнаружения, выявление признаков деградации ИИ и применение резервов с целью обеспечения штатного режима функционирования.

Таким образом, нарушитель и ПОИБ находятся в состоянии постоянного антагонистического конфликта. Динамика данного конфликта формируется в соответствии с графом, представленном на рис. 1.

При введении в эксплуатацию ИИ считается, что у нее отсутствуют какие-либо уязвимости, что соответствует состоянию штатного режима функционирования «0». Со временем, в соответствии с описанными ранее обстоятельствами, появляется новая уязвимость, и ИИ переходит в состояние подверженности угрозам ИБ, что соответствует переходу «0-1». ПОИБ осуществляет упреждающий поиск новой уязвимости (переход «1-2») и, при ее обнаружении, подготавливает обновление (переход «2-0»). Нарушитель также осуществляет поиск возникшей уязвимости (переход «1-3») и при ее обнаружении подготавливает компьютерную атаку (переход «3-4»).

Если ПОИБ быстрее выполнит свои функции (переход «1-2» и «2-0»), чем нарушитель (переход «1-3» и «3-4»), то уязвимость будет закрыта и ИИ вернется к штатному режиму функционирования (состояние «0»). Иначе, она будет подвержена проведению компьютерной атаки нарушителем с использованием обнаруженной уязвимости (состояние «4»). При проведении компьютерной атаки «4-5», ПОИБ осуществляет поиск признаков атаки и, в случае правильного обнаружения, осуществляет ее блокирование (переход «4-0»), при этом считается, что система обнаружения атак обучается и повторное использование уязвимости невозможно. В случае успешного проведения компьютерной атаки, ИИ становится подверженной дальнейшим деструктивным действиям нарушителя (состояние «5»), которые будут направлены на доведение ИИ до состояния отказа (переход «5-6»). Однако, ПОИБ за счет поиска признаков деградации ИИ и введения дополнительных резервов (переход «5-6») может сделать действия нарушителя неэффективными и вернуть ИИ в штатный режим функционирования (состояние «0»). В случае полного отказа ИИ (состояние «6») в течении времени производится ее восстановление и возврат к начальному состоянию (переход «6-0»). После восстановления ИИ считается, что использованная нарушителем уязвимость становится «закрытой» и дальнейшее функционирование ИИ начинается с состояния «0».

Полумарковский процесс, описывающий динамику конфликта, будем задавать следующим образом: состояния $i = 1, 2, ..., 6$ и возможные переходы «i-j» изображены на графе модели (рис. 1), начальное состояние в момент $t = 0$ – «0», независимые функции распределения времени пребывания в i-ом состоянии перед переходом в j-е состояние, если бы выход из состояния i был единственным – $Q_{ij}(t)$, представленные в табл. 1. Обоснование выбора законов распределения для описания вероятностно-временных характеристик описываемых случайных процессов для различных этапов атаки приведено в [9].

Как известно [10], вероятность $P_{ij}(t)$ перехода из состояния i в состояние j за время не более t определяется по формуле:

$$P_{ij}(t) = \int_0^t \prod_{k \neq j} \left(1 - Q_{ik}(\tau)\right) \cdot q_{ij}(\tau)\, d\tau. \qquad (1)$$

Таблица 1

Функции распределения $Q_{ij}(t)$

$Q_{ij}(t)$	Закон распределения	Параметры	$Q_{ij}(t)$	Закон распределения	Параметры
$Q_{01}(t)$	Вейбулла-Гнеденко	a_{01}, b_{01}	$Q_{40}(t)$	Рэлея	a_{40}
$Q_{12}(t)$	Рэлея	a_{12}	$Q_{45}(t)$	Экспоненциальный	λ_{45}
$Q_{13}(t)$	Рэлея	a_{13}	$Q_{50}(t)$	Рэлея	a_{50}
$Q_{20}(t)$	Экспоненциальный	λ_{20}	$Q_{56}(t)$	Экспоненциальный	λ_{56}
$Q_{34}(t)$	Экспоненциальный	λ_{34}	$Q_{60}(t)$	Логнормальный	μ_{60}, σ_{60}

Вероятности p_{ij} перехода из состояния i в состояние j в момент скачка определяются следующим образом:

$$p_{ij} = P_{ij}(\infty) = \int_0^\infty \prod_{k \neq j} (1 - Q_{ik}(\tau)) \cdot q_{ij}(\tau) d\tau. \quad (2)$$

Интервально-переходные вероятности $\Phi_{ij}(t)$ находим путем решения системы интегро-дифференциальных уравнений, записанных в матричном виде в преобразовании Лапласа следующим образом [11]:

$$\Phi^*(s) = \left[1 - p \times p^*(s)\right]^{-1} \cdot \Psi^*(s), \quad (3)$$

где $\Phi(s) = \left[\Phi_{ij}(s)\right]$, $p = \left[p_{ij}\right]$, $p(s) = \left[p_{ij}(s)\right]$ – матрица плотностей вероятности перехода из состояния i в состояние j за время не более t, $\Psi(s) = \left[\delta_{ij} \cdot (1 - F_i(s))\right]$, δ_{ij} – символ Кронекера; знак × обозначает умножение элементов матриц.

Решением системы уравнений являются интервально-переходные вероятности $\Phi_{ij}(t)$, записанные в виде преобразования Лапласа от плотностей вероятностей переходов из состояния i в состояние j за время не более t. Интервально-переходная вероятность $\Phi_{00}(t)$ нахождения ИИ в состоянии штатного функционирования к моменту времени t, записанная в преобразовании Лапласа, имеет при этом вид (4).

Однако, нахождение оригиналов интервально-переходных вероятностей $\Phi_{ij}(t)$ в случае использования некоторых «неэкспоненциальных» законов функций распределения не представляется возможным ввиду отсутствия прямых и обратных преобразований Лапласа и непреодолимых вычислительных трудностей.

Поэтому, предлагается вместо интервально-переходной вероятности $\Phi_{00}(t)$ для оценки конфликтной устойчивости ИИ использовать стационарную вероятность нахождения ее в состоянии штатного функционирования с вероятностью не ниже заданной:

$$P_{стац0} \geq P_{зад}, \quad (5)$$

где $P_{зад}$ – заданное минимальное значение вероятности нахождения ИИ в состоянии штатного функционирования.

Использование стационарной вероятности возможно исходя из следующего соображения: ввиду того, что усилия сторон в конфликте являются соизмеримыми, интервально-переходные вероятности $\Phi_{ij}(t)$ будут монотонными убывающими/возрастающими функциями от времени, стремящимися к предельному значению – $P_{стац\,j}$ нахождения в состоянии j в установившемся режиме, которые находятся следующим образом [12]:

$$P_{стацi} = \pi_i \cdot \overline{t_i} \Big/ \sum_{k=1}^{n} \pi_k \cdot \overline{t_k}, \quad (6)$$

где π_i – стационарные вероятности состояний вложенной марковской цепи в рассматриваемый полумарковский случайный процесс, $\overline{t_i}$ – безусловные математические ожидания времени пребывания ИИ в i-ом состоянии, определяемые следующим образом:

$$\overline{t_i} = \int_0^\infty \prod_{j \in E} \left[1 - Q_{ij}(t)\right] dt. \quad (7)$$

$$\Phi_{00}(s) = \frac{p_{01}(s) - 1}{s(p_{01}(s)p_{12}(s)p_{20}(s) + p_{01}(s)p_{13}(s)p_{34}(s)p_{40}(s) + V + W - 1)}, \quad (4)$$

где $V = p_{01}(s)p_{13}(s)p_{34}(s)p_{45}(s)p_{50}(s)$, $W = p_{01}(s)p_{13}(s)p_{34}(s)p_{45}(s)p_{56}(s)p_{60}(s)$.

Для нахождения стационарных вероятностей состояний π_i вложенной марковской цепи необходимо решить систему из 7 уравнений, записывающихся в соответствии с формулой полной вероятности в виде $\pi_i = \sum_{j \in E} \pi_j \cdot p_{ji}$, а одно из уравнений заменяется нормировочным $\sum_{i \in E} \pi_i = 1$.

В результате решения системы линейных уравнений в среде Maple получены аналитические выражения стационарных вероятностей состояний графа функционирования ИИ. Аналитический вид зависимостей является громоздким, поэтому приведем только формулу для стационарной вероятности нахождения ИИ в режиме штатного функционирования $P_{стац0}$:

$$P_{стац0} = \frac{2\lambda_{34}\lambda_{20}(a_{12}{}^2 + a_{13}{}^2)b_{01}\Gamma\left(\frac{1}{a_{01}}\right)}{A+B+C+D+E+F+G+H+I+J+K}, \quad (8)$$

где $A = \pi e^{0.5\left(\lambda_{56}{}^2 a_{50}{}^2 + \lambda_{45}{}^2 a_{40}{}^2\right)} erf\left(\frac{\lambda_{56}a_{50}}{\sqrt{2}}\right) \times$

$\times erf\left(\frac{\lambda_{45}a_{40}}{\sqrt{2}}\right) t_6 a_{01} a_{12}{}^2 a_{40} a_{50} \lambda_{20}\lambda_{34}\lambda_{45}\lambda_{56},$

$B = -\pi e^{0.5\left(\lambda_{56}{}^2 a_{50}{}^2 + \lambda_{45}{}^2 a_{40}{}^2\right)} erf\left(\frac{\lambda_{56}a_{50}}{\sqrt{2}}\right) \times$

$\times t_6 a_{01} a_{12}{}^2 a_{40} a_{50} \lambda_{20}\lambda_{34}\lambda_{45}\lambda_{56},$

$C = -\pi e^{0.5\left(\lambda_{56}{}^2 a_{50}{}^2 + \lambda_{45}{}^2 a_{40}{}^2\right)} erf\left(\frac{\lambda_{45}a_{40}}{\sqrt{2}}\right) \times$

$\times t_6 a_{01} a_{12}{}^2 a_{40} a_{50} \lambda_{20}\lambda_{34}\lambda_{45}\lambda_{56},$

$D = \pi e^{0.5\left(\lambda_{56}{}^2 a_{50}{}^2 + \lambda_{45}{}^2 a_{40}{}^2\right)} erf\left(\frac{\lambda_{56}a_{50}}{\sqrt{2}}\right) \times$

$\times erf\left(\frac{\lambda_{45}a_{40}}{\sqrt{2}}\right) a_{01} a_{12}{}^2 a_{40} a_{50} \lambda_{20}\lambda_{34}\lambda_{45},$

$E = \pi e^{0.5\left(\lambda_{56}{}^2 a_{50}{}^2 + \lambda_{45}{}^2 a_{40}{}^2\right)} t_6 a_{01} a_{12}^2 a_{40} a_{50} \lambda_{20}\lambda_{34}\lambda_{45}\lambda_{56},$

$F = -\pi e^{0.5\left(\lambda_{56}{}^2 a_{50}{}^2 + \lambda_{45}{}^2 a_{40}{}^2\right)} erf\left(\frac{\lambda_{56}a_{50}}{\sqrt{2}}\right) \times$

$\times a_{01} a_{12}{}^2 a_{40} a_{50} \lambda_{20}\lambda_{34}\lambda_{45},$

$G = -\pi e^{0.5\left(\lambda_{56}{}^2 a_{50}{}^2 + \lambda_{45}{}^2 a_{40}{}^2\right)} erf\left(\frac{\lambda_{45}a_{40}}{\sqrt{2}}\right) \times$

$\times a_{01} a_{12}{}^2 a_{40} a_{50} \lambda_{20}\lambda_{34}\lambda_{45},$

$H = \pi e^{0.5\left(\lambda_{56}{}^2 a_{50}{}^2 + \lambda_{45}{}^2 a_{40}{}^2\right)} a_{01} a_{12}{}^2 a_{40} a_{50} \lambda_{20}\lambda_{34}\lambda_{45},$

$I = -\sqrt{2\pi} e^{0.5\lambda_{45}{}^2 a_{40}{}^2} erf\left(\frac{\lambda_{45}a_{40}}{\sqrt{2}}\right) a_{01} a_{12}^2 a_{40} \lambda_{20}\lambda_{34},$

$J = \sqrt{2\pi} e^{0.5\lambda_{45}{}^2 a_{40}{}^2} a_{01} a_{12}{}^2 a_{40} \lambda_{20}\lambda_{34} +$

$+\sqrt{2\pi\left(a_{12}{}^2 + a_{13}{}^2\right)} a_{01} a_{12} a_{13} \lambda_{20}\lambda_{34},$

$K = 2\Gamma\left(\frac{1}{a_{01}}\right) a_{12}{}^2 b_{01} \lambda_{20}\lambda_{34} +$

$+2\Gamma\left(\frac{1}{a_{01}}\right) a_{13}{}^2 b_{01} \lambda_{20}\lambda_{34} +$

$+2a_{12}{}^2 a_{01}\lambda_{20} + 2a_{13}{}^2 a_{01}\lambda_{34},$

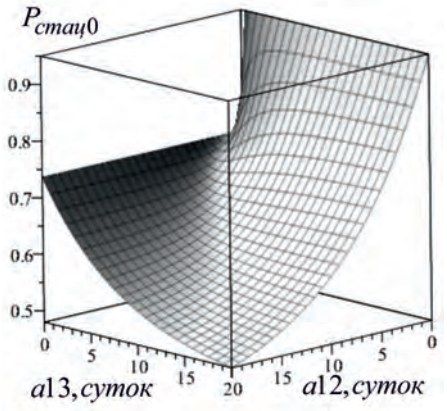
$t_6 = \int_0^\infty \left(\frac{1}{2} - \frac{1}{2} erf\left(\frac{\ln(x) - \mu_{60}}{\sqrt{2}\sigma_{60}}\right)\right) dx.$

Графики зависимостей стационарной вероятности нахождения ИИ в состоянии штатного функционирования от совокупности значений параметров выбранных распределений представлены на рис. 2а-г.

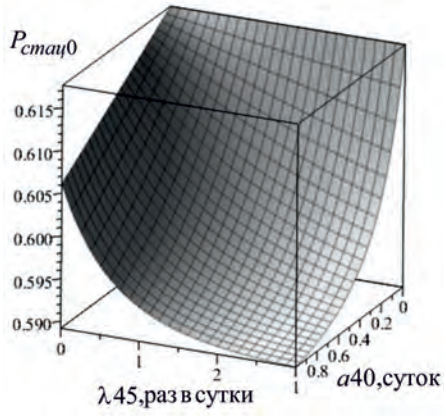
При первом вводе в эксплуатацию ИИ, а также каждый раз при восстановлении ее после отказа, поток появления новых уязвимостей будет снижаться со временем (что соответствует интервалу «приработки»), а наиболее вероятным значением времени появления новой уязвимости будет 60 суток, что соответствует параметрам функции распределения $Q_{01}(t)$: $a_{01} = 0.5$, $b_{01} = 30$. Прогнозируемые наиболее вероятные значения показателей эффективности действий нарушителя следующие: $a_{13} = 10$, $\lambda_{34} = 0.25$, $\lambda_{45} = 0.5$, $\lambda_{56} = 1$.

Прогнозируемые наилучшие значения показателей эффективности ПОИБ при ее противодействии нарушителю следующие: $a_{12\min} = 10$, $\lambda_{20\max} = 1$, $a_{40\min} = 0.5$, $a_{50} = 0.3$. В случае доведения ИИ до состояния отказа, возврат ее к штатному состоянию функционирования возможен не ранее, чем через 2 суток ($\mu_{60} = 1.5$, $\sigma_{60} = 0.9$). Данные значения параметров могут быть отличными от параметров конкретной ИИ и соответствующей ей модели нарушителя.

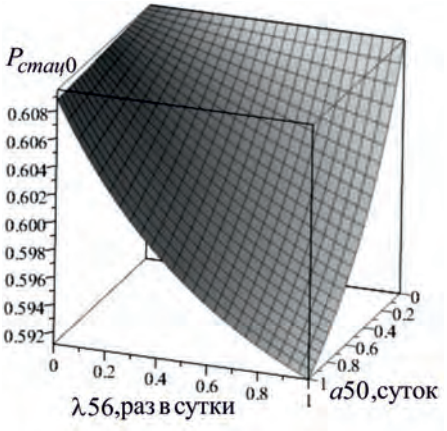
Исходя из этих интервалов значений, возникает задача нахождения множества возможных значений параметров, влияющих на эффективность ПОИБ, которая звучит сле-



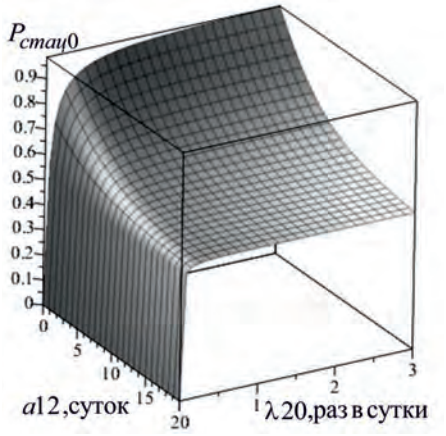
а) зависимость от наиболее вероятных значений времени обнаружения уязвимости ПОИБ a_{12} и нарушителем a_{13} при следующих значениях остальных параметров: $a_{01}=3$, $b_{01}=22.6$, $\lambda_{20}=0.95$, $\lambda_{34}=0.15$, $a_{40}=0.3$, $\lambda_{45}=0.17$, $a_{50}=0.3$, $\lambda_{56}=0.16$, $\mu_{60}=3.75$, $\sigma_{60}=0.55$



б) зависимость от наиболее вероятного значения времени обнаружения признаков компьютерной атаки и ее блокирования a_{40} и от интенсивности проведения атаки нарушителем λ_{45} при следующих значениях остальных параметров: $a_{01}=3$, $b_{01}=22.6$, $a_{12}=10$, $a_{13}=10$, $\lambda_{20}=0.95$, $\lambda_{34}=0.15$, $a_{50}=0.3$, $\lambda_{56}=0.16$, $\mu_{60}=3.75$, $\sigma_{60}=0.55$



в) зависимость от наиболее вероятного значения времени обнаружения признаков деградации ИИ a_{50} и от интенсивности доведения ее до состояния отказа λ_{56} при следующих значениях остальных параметров: $a_{01}=3$, $b_{01}=22.6$, $a_{12}=10$, $a_{13}=10$, $\lambda_{20}=0.95$, $\lambda_{34}=0.15$, $a_{40}=0.3$, $\lambda_{45}=0.17$, $\mu_{60}=3.75$, $\sigma_{60}=0.55$

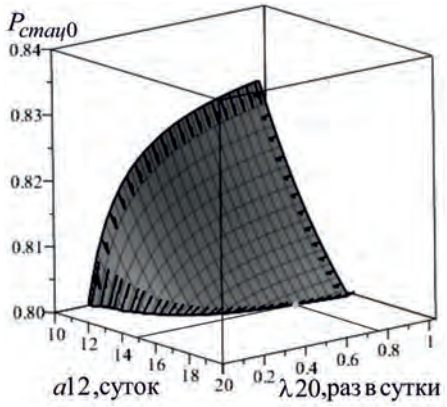


г) зависимость от наиболее вероятных значений времени обнаружения уязвимости ПОИБ a_{12} и интенсивности применения обновления для ее закрытия λ_{20} при следующих значениях остальных параметров: $a_{01}=3$, $b_{01}=22.6$, $a_{13}=10$, $\lambda_{34}=0.15$, $a_{40}=0.3$, $\lambda_{45}=0.17$, $a_{50}=0.3$, $\lambda_{56}=0.16$, $\mu_{60}=3.75$, $\sigma_{60}=0.55$

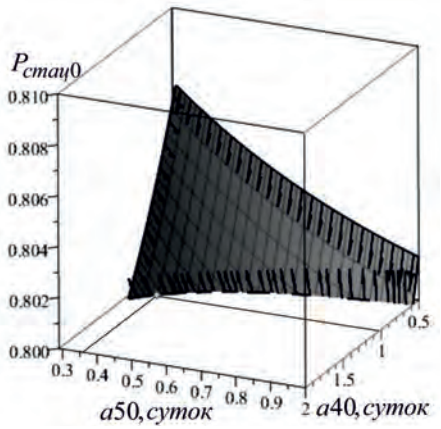
Рис. 2. Графики стационарной вероятности нахождения ИИ в состоянии штатного функционирования

дующим образом: найти области допустимых значений технических показателей ПОИБ, обеспечивающих конфликтную устойчивость ИИ и удовлетворяющих условию (5), при заданных наиболее вероятных значениях технических показателей действий нарушителя и существующих ограничениях на построение ПОИБ ИИ.

В результате проведенного расчета получены области допустимых значений техни-



а) область значений времени обнаружения уязвимости ПОИБ a_{12} и интенсивности применения обновления для ее закрытия λ_{20}



б) область значений времени обнаружения признаков деградации ИИ a_{50} и времени обнаружения признаков компьютерной атаки и ее блокирования a_{40}

Рис. 3. Графики областей допустимых значений технических параметров ПОИБ, для которых выполняется условие $P_{стац0} \geq 0.8$

ческих показателей ПОИБ, изображенные на рисунках 3а, 3б, при которых обеспечивается конфликтная устойчивость ИИ. Яркая точка на рисунках 3а и 3б обозначает лишь одно из множества значений технических показателей ПОИБ – $a_{12} = 14.92$, $a_{40} = 1.02$, $a_{50} = 0.36$, $\lambda_{20} = 0.77$, для которых выполняется условие (5).

Таким образом, разработана полумарковская модель функционирования ИИ в условиях конфликта нарушителя и ПОИБ, позволяющая при заданной вероятности штатного функционирования ИИ обосновывать ограниченные снизу значения технических показателей ПОИБ. Полученные зависимости технических характеристик ПОИБ могут стать основой при обосновании тактико-технических требований к перспективным подсистемам.

СПИСОК ЛИТЕРАТУРЫ

1. *Язов Ю. К., Соловьев С. В.* Защита информации в информационных системах от несанкционированного доступа. – Воронеж : Кварта, 2015. – 440 с.

2. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. – СПб. : Наука и Техника, 2004. – 384 с.

3. *Макаренко С. И., Михайлов Р. Л.* Информационные конфликты – анализ работ и методологии исследования // Системы управления, связи и безопасности. – 2016. – № 3.

4. *Радько Н. М., Скобелев И. О.* Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – М. : РадиоСофт, 2010. – 232 с.

5. *Вялых А. С., Вялых С. А., Сирота А .А.* Оценка уязвимости информационной системы на основе ситуационной модели динамики конфликта // Информационные технологии. – 2012. – № 9. – С. 16–21.

6. *Вялых А. С., Вялых С. А.* Динамика уязвимостей в современных защищенных информационных системах // Вестник Воронеж. гос. ун-та. Сер. Системный анализ и информационные технологии. – 2011. – № 2.

7. *Сирота А. А.* Компьютерное моделирование и оценка эффективности сложных систем. – М. : Техносфера, 2006. – 280 с.

8. Модели информационного конфликта средств поиска и обнаружения. Монография / Под. Ред. Ю. Л. Козирацкого. – М. : Радиотехника, 2013. – 232 с.

9. *Vandana Gupta, Dharmaraja S.* Semi-Markov modeling of dependability of VoIP network in the presence of resource degradation and security attacks // Reliability Engineering and System Safety 96. – 2011. – Pp. 1627–1636.

10. *Гнеденко Б. В., Коваленко И. Н.* Введение в теорию массового обслуживания. Изд. 4-е, испр. – М. : Издательство ЛКИ, 2007. – 400 с.

11. *Тихонов В. И. Миронов М. А.* Марковские процессы. –М. : «Сов. радио». – 1977. – 488 с.

12. *Журавлев В. И.* Поиск и синхронизация в широкополосных системах. – М. : Радио и связь, 1986.

Андреещев Иван Алексеевич – адъюнкт, ВУНЦ ВВС «Военно-воздушная академия им. проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж).
E-mail: Ivan241@inbox.ru

Будников Сергей Алексеевич – д-р техн. наук, доцент, начальник кафедры, ВУНЦ ВВС «Военно-воздушная академия им. проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж).
E-mail: buser@bk.ru

Гладков Антон Валерьевич – курсант, ВУНЦ ВВС «Военно-воздушная академия им. проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж).
E-mail: gladkov.av@mail.ru

Andreeshchev Ivan A. – adjunct, Military Educational and Scientific Center «Zhukovsky–Gagarin Air Force Academy» (Voronezh).
E-mail: Ivan241@inbox.ru

Budnikov Sergey A. – Dr. Sc. (Eng.), Associate Professor, Head of Department, Military Educational and Scientific Center «Zhukovsky–Gagarin Air Force Academy» (Voronezh).
E-mail: buser@bk.ru

Gladkov Anton V. – cadet, Military Educational and Scientific Center «Zhukovsky–Gagarin Air Force Academy» (Voronezh).
E-mail: gladkov.av@mail.ru