УДК 681.3

О КОНТРОЛЕ ЦЕЛОСТНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ТОРГОВОЙ ОРГАНИЗАЦИИ

И. А. ГУБИН[1]
В.И. СУМИН[2]
В.М. КОЛЫХАЛИН[1]
О.В. ИСАЕВ[2]

[1)] *Воронежский государственный педагогический университет*

[2)] *Воронежский институт ФСИН РФ*

email:
gubin24@yandex.ru
viktorsumin51@yandex.ru
wi@ret.ru
OlegIsaev71@yandex.ru

В данной статье раскрывается современный подход к проектированию систем защиты информации (СЗИ). В частности применительно к информационной системе (ИС) торговой организации. Частично раскрывается суть эталонной модели защищённой автоматизированной системы (ЭМЗАС) как метода построения ИС таким образом, чтобы искоренить угрозы безопасности, имеющие основу в погрешностях самой системной структуры. Предоставляется расположение элементов ИС организации по уровням ЭМЗАС.

Дается описание сервиса контроля целостности (КЦ) как основного элемента СЗИ. Уделяется внимание эффективности функционирования КЦ: приводится несколько различных критериев, которым ставятся в соответствие математические элементы. КЦ рассматривается как сложная система, имеющая цепь состояний с вероятностными переходами. На основе данных заключений делается вывод, что максимально удобным математическим аппаратом анализа такой стохастической модели является теория конечных полумарковских процессов.

Ключевые слова: автоматизированная система обработки данных; агрессивность функционирования; дискреционный доступ; защита информации; информационная система; конечный полумарковский процесс; контроль целостности; несанкционированный доступ; стохастический процесс; торговая организация.

Характерной особенностью любого информационного процесса автоматизированной системы (АС) является определённая политика безопасности (ПБ). ПБ регламентирует методы, процессы, способы работы и функционирования АС таким образом, чтобы поддерживать информационную безопасность на необходимом уровне. В настоящее время специалисты всё чаще прибегают к использованию дискреционной ПБ, а точнее сказать, к её усовершенствованной модели – ролевой ПБ. Тем не менее, всегда присутствует угроза несанкционированного доступа и потери данных за счет несовершенности структуры самой информационной системы (ИС). В связи с этим целесообразно применять концепцию эталонной модели защищённой автоматизированной системы (ЭМЗАС).

ЭМЗАС – метод проектирования ИС таким образом, чтобы обеспечить её максимальную степень защиты за счёт доступа к информации реализованного путем последовательного спуска по уровням детализации ресурсов цепочкой авторизованных доступов компонентов более высокого уровня к ресурсам компонентов более низкого уровня [5, 10].

В качестве примера возьмём ИС компании «Рет». Эта организация занимается реализацией компьютерной и цифровой техники в региональном масштабе.

Административный уровень определяет доступ администратора к ИС. Администратор имеет широкие функциональные обязанности, в частности, предоставляет пользователям полномочия. В результате пользователь становится уполномоченным (авторизованным) пользователем.

Идентификационный уровень определяет доступ уполномоченного пользователя к ИС ООО «Рет» (процедуры идентификации и аутентификации). В результате устанавливается соответствие между уполномоченным пользователем и его идентификатором.

Интеграционный уровень осуществляет доступ виртуального пользователя, авторизованного уполномоченным пользователем, к ресурсам ИС посредством создания интегрированной индивидуальной пользовательской рабочей среды интегратором ИС (доступ виртуального пользователя к интегратору ИС).

Диспетчерский уровень предназначен для доступа интегратора ИС ООО «Рет», авторизованного некоторым образом, к ресурсам ИС посредством управления запуском прикладных программ, осуществляемого диспетчером программ ИС (доступ интегратора ИС к диспетчеру программ ИС).

Навигационный уровень определяет доступ диспетчера программ, авторизованного некоторым образом, к средствам навигации ИС. Предполагается, что при функционировании ИС, как для работы прикладных программ, так и непосредственно для пользователя, возникает потребность в различных данных.

Серверный уровень осуществляет доступ средства навигации ИС, авторизованного некоторым образом, к серверам ИС: индивидуальный сервер филиала организации и общий сервер организации. В результате определенный сервер предоставляет свои услуги средству навигации в интересах пользователя, авторизующего доступ.

Прикладной уровень определяет доступ сервера ИС ООО «Рет», авторизованного некоторым образом, к подчиненным ему прикладным компонентам. Для сервера филиала организации это модуль доступа к объектам, а для общего сервера организации – модуль доступа к данным и аналитический модуль.

Менеджерский уровень регламентирует доступ прикладного компонента сервера ИС, авторизованного некоторым образом, к менеджерам ресурсов данного сервера.

Информационный уровень определяет доступ менеджера ресурсов сервера ИС, авторизованного некоторым образом, к данным, хранящимся на сервере.

Описав функциональные характеристики уровней ЭМЗАС, можно схематично расположить компоненты базы данных (БД) ООО «Рет» согласно каждому уровню. Так же необходимо указать связи компонентов между отдельными уровнями и внутри уровня (рис. 1).

Для поддержки принятия администратором в рамках защиты информации (ЗИ) решений по выбору временной последовательности запусков сервиса контроля целостности (КЦ) рабочей среды в составе используемой в ИС ООО «Рет» типовой системы защиты информации (СЗИ) от несанкционированного доступа (НСД) предлагается использовать новую подсистему – подсистему автоматизированного управления КЦ рабочей среды ООО «Рет». Исходными данными для нее являются следующие:

1. Статистические данные о выполнении СЗИ НСД своих сервисных задач в ИС ООО «Рет», а также реализации конкретных функций ЗИ от НСД при выполнении этих сервисных задач. Эти данные предоставляются подсистемой регистрации и учета по окончании каждой контрольной проверки.

2. Параметры, задающие требования к управлению КЦ рабочей среды «Рет» как в плане обеспечения ЗИ от НСД, так и в плане обеспечения функционирования ИС по целевому назначению. Эти данные задаются администратором ЗИ в соответствии с разделом «Требования к подсистеме ЗИ от НСД» эксплуатационной документации на ООО «Рет».

В эталонной автоматизированной системе обработки данных (АСОД) ИС ООО «Рет» в смысле ЭМЗАС контроль целостности информации осуществляется достаточно специфическим образом, в силу чего специфично и управление этим процессом.

Однако цель такого управления едина для любых АСОД – обеспечение разумного компромисса между удовлетворением требований к АСОД по аспекту целостности интегрального свойства защищенности информации и удовлетворением требований к АСОД по ее прямому назначению. Основной фактор противоречивости этих требований заключается в большой требовательности сервисов контроля целостности информации к временному ресурсу [2].

Специфика эталонной АСОД при управлении контролем целостности информации проявляется, в частности, в том, что моменты времени запуска необходимых контрольных процедур и контролируемые объекты жестко связаны с процессами доступа к информации, и, следовательно, их выбор не может входить в круг управленческих решений. Остается только возможность варьирования длительностью проведения процедур контроля целостности информации за счет варьирования степени полноты контроля.

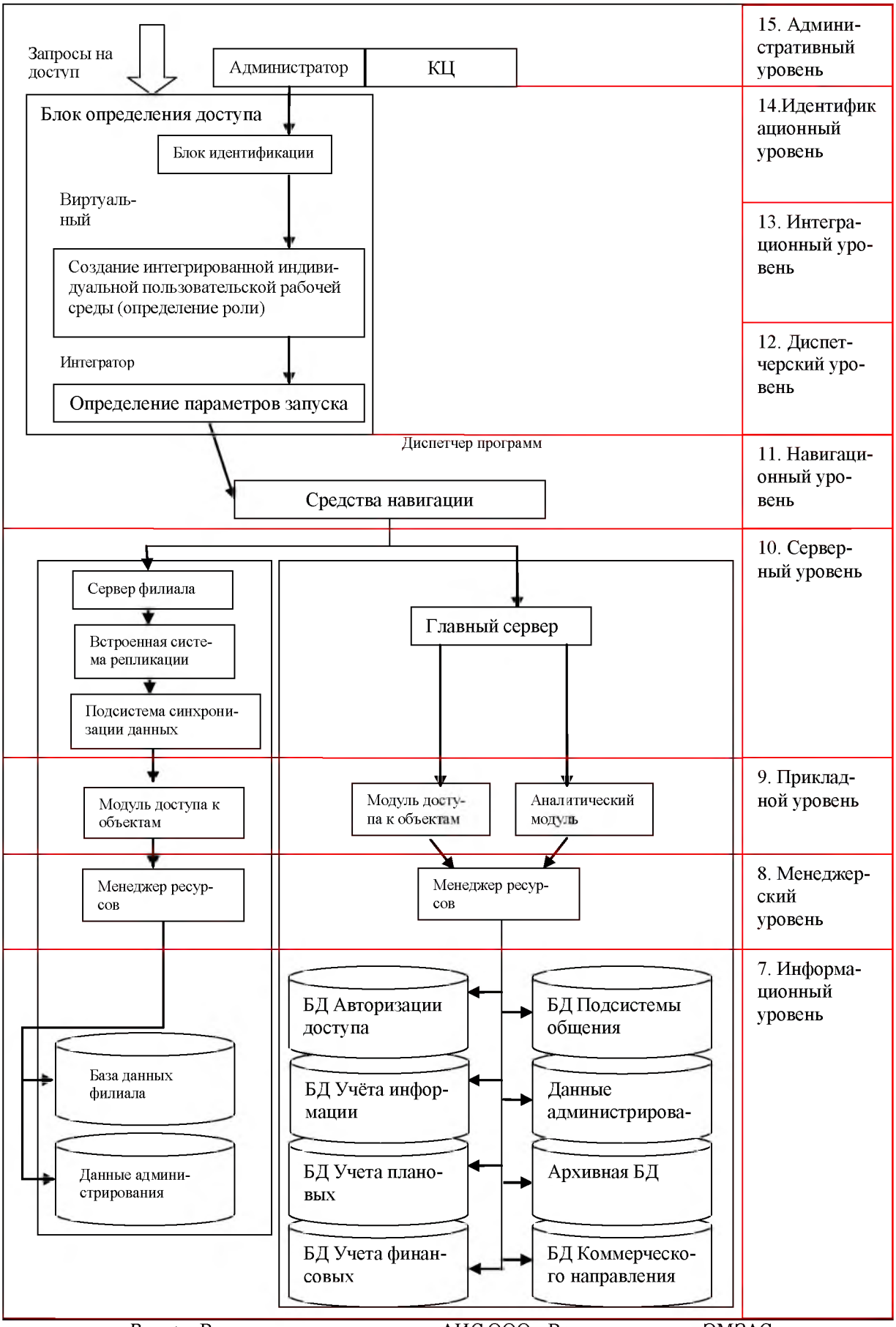

Рис. 1. «Распределение элементов АИС ООО «Рет» по уровням ЭМЗАС»

В идеале, контроль целостности объекта представляет собой контроль его неизменности [8]. При этом проверяется полное тождество контролируемого объекта и образца

(объекта, хранящего исходное состояние контролируемого объекта, которое принимается за эталонное), что обеспечивает полностью достоверный контроль (с нулевой вероятностью ошибки). В этом случае эталонный объект должен быть как минимум одинаковой длины с контролируемым, что приводит к максимальной длительности проведения процедуры контроля неизменности.

Сокращение длительности проведения подобной процедуры достигается за счет использования в качестве эталонного объекта вычисляемого с использованием хэш-функций хэш-значения, отличающегося меньшей по сравнению с проверяемым объектом длиной. Процесс установления неизменности объекта становится вероятностным, и в этом случае говорят уже не о контроле неизменности объекта, а о контроле его целостности [4, 5]. Таким образом, контроль неизменности объекта представляет собой предельный случай контроля его целостности, наилучший по защищенности и наихудший по использованию временного ресурса. Сравнивать по использованию временного ресурса реальный контроль целостности с предельным (контролем неизменности) естественно по соотношению длительностей проведения соответствующих процедур, но сравнение по защищенности неоднозначно.

Ключевой составляющей процесса организационно-технологического управления КЦ рабочей среды АСОД ООО «Рет» является принятие решений, реализуемое соответствующей подсистемой принятия решений. Управляющее воздействие на сервис КЦ, соответствующее принятому решению, производится подсистемой управляющих воздействий. Процессы контроля качества функционирования сервиса КЦ, осуществляемые соответствующей подсистемой, реализуют функцию обратной связи управления КЦ рабочей среды ООО «Рет». Принятие решения по оперативному планированию очередного запуска сервиса КЦ осуществляется после реализации непосредственно предшествующего ему запуска на основе следующих данных:

– анализа условий функционирования ООО «Рет» как с точки зрения ЗИ от НСД, так и с точки зрения требований к ООО «Рет» в плане функционирования по целевому назначению;

– результатов контроля качества функционирования сервиса КЦ как объекта управления.

Принятие решения осуществляется на основе комплексной оценки качества функционирования сервиса КЦ как объекта управления с учетом результатов его контроля, реализующего функцию обратной связи управления, для обеспечения и поддержания разумного компромисса между уровнем целостности информации в АСОД ООО «Рет» и её эффективностью функционирования по целевому назначению. Комплексная оценка качества функционирования сервиса КЦ как объекта управления производится по комплексу критериев качества функционирования сервиса КЦ как объекта организационно-технологического управления КЦ рабочей среды ИС. В результате управленческого решения выбирается такой набор значений управляемых параметров функционирования сервиса КЦ, который обеспечивает наилучшее качество его функционирования как объекта управления [9]. При этом выбранный набор значений управляемых параметров используется подсистемой управляющих воздействий для определения конкретного момента времени начала очередной контрольной проверки, но так, чтобы пользователи не могли прогнозировать этот момент времени.

Оценка результатов принятия решения при организационно-технологическом управлении сервисом КЦ производится по оценивающему качество его функционирования комплексу критериев, определяющих количественные значения для соответствующих подхарактеристик (рисунок 2). Комплекс критериев качества функционирования сервиса КЦ как объекта управления – это совокупность критериев, в полной мере количественно выражающая его пригодность при заданных в данной ситуации параметрах функционирования в данной ИС удовлетворять предъявляемым требованиям [6].

Стохастическое варьирование несколько сложнее детерминированного по своей реализации, но зато не дает возможности злоумышленнику прогнозировать степень полноты проверки. Поэтому в качестве предпочтительного способа варьирования выберем для дальнейшего моделирования стохастический, осуществляемый взаимно независимо на всех уровнях ЭМЗАС.

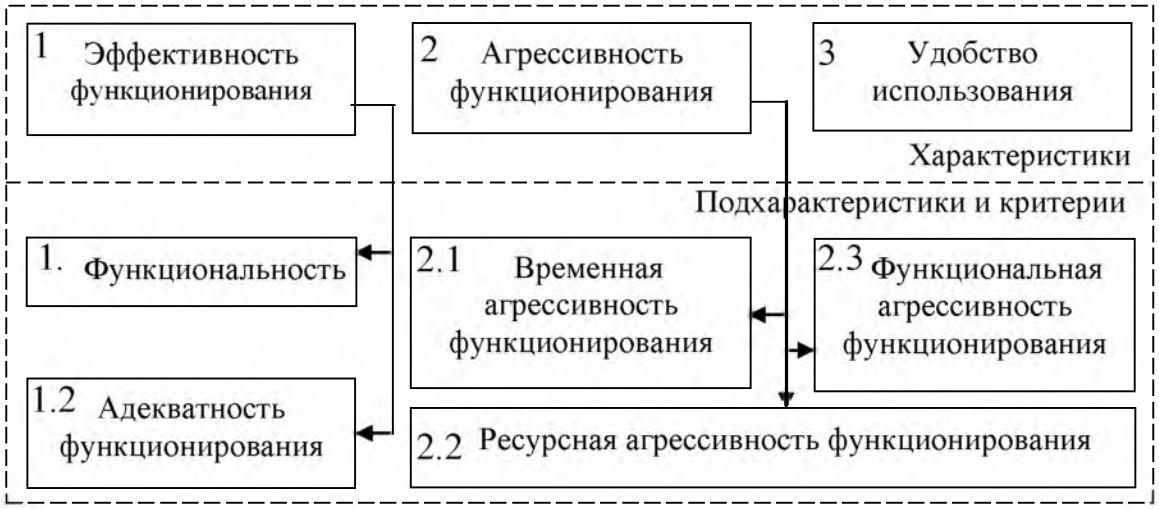

Рис. 2. Структурная схема комплексной оценки качества функционирования сервиса КЦ как объекта управления

Будем рассматривать динамические критерии для эталонной АСОД ООО «Рет» применительно к функционированию сервиса КЦ при реализации конкретного дискреционного доступа. При этом положим известными величины:

$V_{(di)}$ – объем контролируемой на целостность информации в течении всего дискреционного доступа,

$v_{(di)}$ – случайная величина объема информации проверяемой на неизменность в течение всего дискреционного доступа,

c – скорость проверки на неизменность информации.

Для определения динамических критериев введем следующие величины:

$\tau_{(di)} = v_{(di)} / c$, $K_{(di)} = v_{(di)} / V_{(di)} = c \cdot \tau_{(di)} / V_{(di)}$ – случайные величины времени протекания КЦ и его коэффициента в течение всего дискреционного доступа;

$\tau_{\min аф}$, $\tau_{\max ва}$, $K_{(di)}\min$, $K_{(di)}\max$ – их минимально и максимально допустимые границы (экспоненциально распределены со средним $\tau_{маф}$, $\tau_{ива}$, $\overline{K}_{(di)}\min$, $\overline{K}_{(di)}\max$);

Примем

$$c = V_{(di)} = V_{(di)} / c = 1,$$

то есть будем измерять время и количество информации в относительных единицах. Тогда

$$v_{(di)} = K_{(di)} = \tau_{(di)},\ \overline{K}_{(di)}\min = \tau_{\min аф},\ \overline{K}_{(di)}\max = \tau_{\max ва}.$$

Введем вспомогательный критерий $E(\tau_m)$, который назовем критерием динамической эффективности функционирования сервиса КЦ:

$$E(\tau_m) = P\left(\tau_{(di)} \le \tau_{\max}(\tau_m)\right),$$

Определим динамические критерии для эталонной АСОД ООО «Рет» равенствами:

$$E_{аф} = P\left(K_{(di)} > K_{(di)}\min\right) = 1 - P\left(\tau_{(di)} \le \tau_{\min аф}\right) = 1 - E\left(\tau_{маф}\right), \qquad (1)$$

$$E_{ва} = P\left(K_{(di)} \le K_{(di)\max}\right) = P\left(\tau_{(di)} \le \tau_{\max ва}\right) = E\left(\tau_{тва}\right). \quad (2)$$

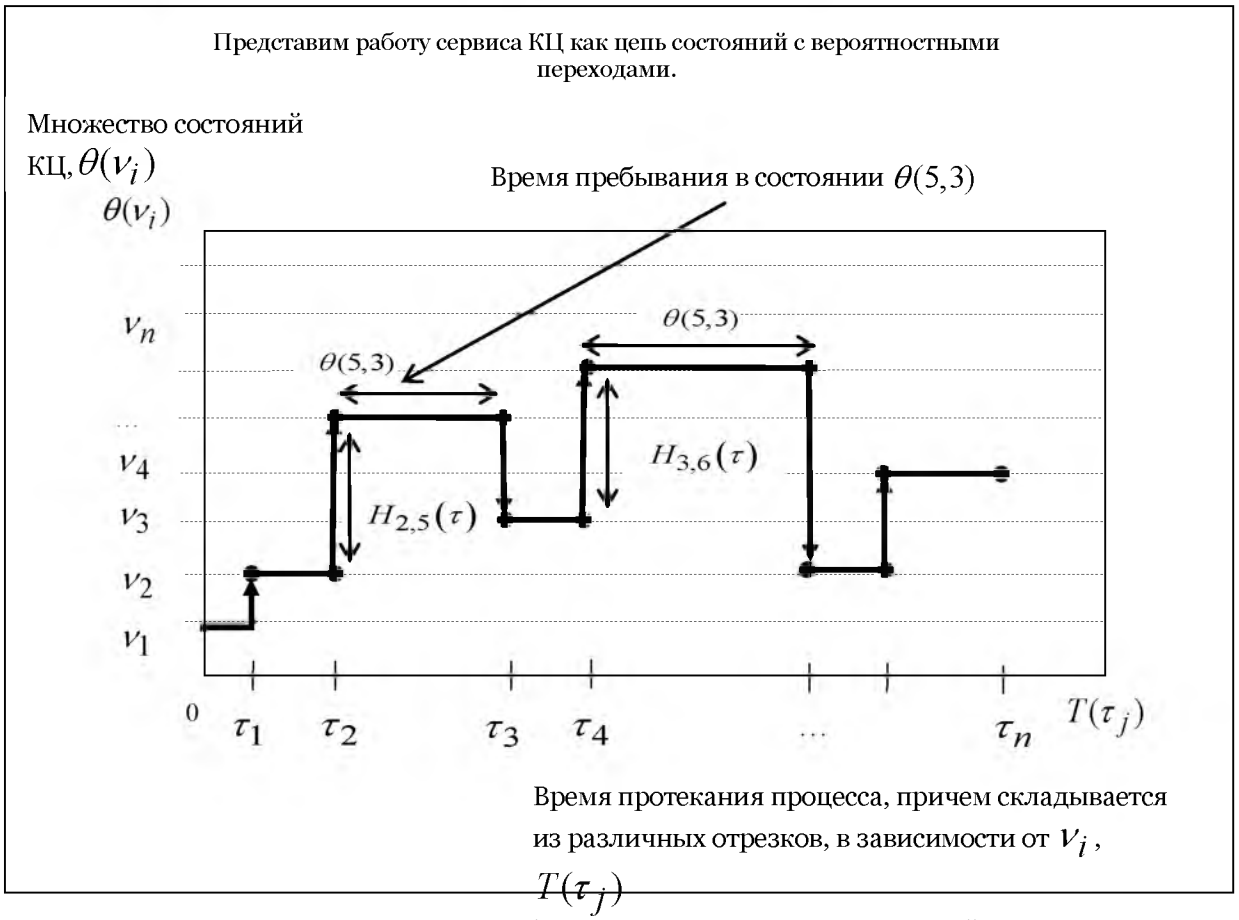

Рис. 3. Схематичное изображение стохастических состояний КЦ

Для оценки и анализа по формулам (1)-(2) динамических критериев качества функционирования сервиса КЦ как объекта управления в АСОД ООО «Рет» нужна подходящая стохастическая модель динамики функционирования сервиса КЦ в ИС. Она описываться матрицей $\left\|H_{ij}(\tau)\right\|$, произвольный элемент которой $H_{ij}(\tau)$ есть вероятность того, что моделируемый процесс, оказавшись в состоянии i, перейдет из него в состояние j в результате срабатывания соответствующего перехода сети, причем за время, меньшее τ (Рис. 3). Адекватным математическим аппаратом анализа такой стохастической модели является теория конечных полумарковских процессов (КПП) [3, 4]. Тогда сама модель представляет собой поглощающий КПП, характеризующийся полумарковской матрицей $H = \left\|H_{ij}(\tau)\right\|$ [3, 4], что позволяет учитывать произвольность закона распределения пребывания процесса в любом состоянии.

При использовании таких полумарковских моделей оценка любого динамического критерия сводится к оценке вероятности своевременного поглощения соответствующего КПП. Своевременность поглощения КПП означает, что время достижения некоторого конечного его состояния, являющегося поглощающим, из определенного начального состояния (время жизни КПП) не превышает некоторой максимально допустимой границы, являющейся экспоненциально распределенной случайной величиной с заданным средним значением. Выбор экспоненциального закона распределения обусловлен широкой сферой его использования для аппроксимации максимально допустимого времени выполнения сложными системами своих функциональных задач [1, 7]. Какие именно состояния являются начальными или конечными, зависит от того, какой конкретно динамический критерий рассматривается. Обозначим через n число состояний КПП, отдельные состояния нумеруются натуральными числами от 1 (начальное) до n (конечное). Тогда время жизни КПП есть промежуток времени от

момента времени входа КПП в начальное (первое) состояние до момента времени входа КПП в конечное (n-ое) состояние.

Список литературы

1. Антонюк, Б. Д. Информационные системы в управлении [Текст] / Б. Д. Антонюк. – М. : Радио и связь, 1986. 240 с 11

2. Багаев, М. А. Методы и средства автоматизированной оценки и анализа качества функционирования программных систем защиты информации [Текст] : монография / М. А. Багаев, А. С. Дубровин, И. И. Застрожнов, О. Ю. Макаров, Е. А. Рогозин, В. И. Сумин. – Воронеж : Воронеж. гос. техн. ун-т, 2004. 181 с.

3. Девянин, П. Н. Теоретические основы компьютерной безопасности [Текст] : учеб. пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и [др.]. – М. : Радио и связь, 2000. 192 с.

4. Дейт, К. Дж. Введение в системы баз данных [Текст] / К. Дж. Дейт; перевод с англ. – 8-е изд. – М. : Издательский дом «Вильямс», 2005. 1328 с.

5. Дубровин, А. С. Оценка защищенности автоматизированных систем на основе сравнения с эталонной моделью защищенной автоматизированной системы [Текст] / А. С. Дубровин, М. В. Коротков, В. И. Сумин // Всероссийская науч.-практическая конф. «Современные проблемы борьбы с преступностью» : сб. материалов (радиотехнические науки). – Воронеж : Воронеж. ин-т МВД России, 2004. С. 58–59.

6. Дубровин, А. С. Модели и алгоритмы автоматизированного управления подсистемой контроля целостности в системах защиты информации [Текст]: дис. ... канд. тех. наук / А. С. Дубровин; Воронежский институт МВД России. – Воронеж, 2003. 137 с.

7. Жиляков, Е.Г. Компьютерная кластеризация совокупности аддитивных математических моделей взаимосвязанных процессов/ Е.Г. Жиляков, В.И. Ломазова, В.А. Ломазов //Вопросы радиоэлектроники. – 2011. – № 1. С. 115-119.

8. Жиляков, Е.Г. Селекция аддитивных функциональных моделей сложных систем/Е.Г. Жиляков, В.И. Ломазова, В.А. Ломазов //Информационные системы и технологии. 2010. – № 6. С. 66-70.

9. Жиляков Е.Г. Адаптивное определение относительных важностей объектов на основе качественных парных сравнений. // Экономика и математические методы, – Том 42, №2, 2006г

10. Сумин, В. И. Построение модели рационального выбора систем принятия решения/ В. И. Сумин, А. В. Ильницкий // Научные ведомости БелГУ. 2012. № 19 (138). Вып.24/1. С. 158-160.

ABOUT CONTROL INTEGRITY OF INFORMATION PROCESSES IN AUTOMATED SYSTEM TRADE ORGANIZATION

I.A. GUBIN[1]
V.I. SUMIN[2]
V.M. KOLYHALIN[1]
O.V. ISAEV[2]

[1)] ***Voronezh State Pedagogical University***

[2)] ***Voronezh Institute of the Federal Penitentiary Service of the Russian Federation***

email:
wi@ret.ru
OlegIsaev71@yandex.ru
viktorsumin51@yandex.ru
gubin24@yandex.ru

This article deals with the modern approach to the design of security systems (GIS). In particular with regard to information system (IS) of the trade organization. Partially reveals the essence of the reference model secure automated system (RMPAS) as a method of constructing the IP so as to eliminate security threats that have a basis in the very errors of systemic structure. Given layout IS organization by levels RMPAS.

A description of the service integrity (CC) as a key part of GIS. Attention is paid to the efficiency of the CC: is a number of different criteria, which are mapped to mathematical elements. KC seen as a complex system, which has a chain of states with probabilistic transitions. Conclusions based on the data it is concluded that the most convenient mathematical tool to analyze the stochastic model is the theory of finite semi-Markov processes.

Keywords: automatic data processing system; aggressiveness functioning; discretionary access; protection of information; the information system; the final semi-Markov process; integrity control; unauthorized access; stochastic process; trade organization.