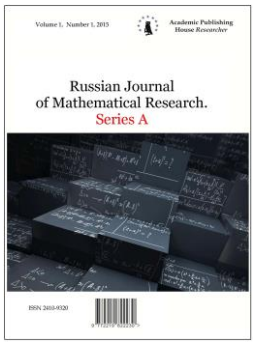

Published in the Slovak Republic
Russian Journal of Mathematical Research. Series A
Has been issued since 2015.
E-ISSN: 2413-7529
2017, 3(2): 49-61

DOI: 10.13187/rjmr.a.2017.2.49
www.ejournal30.com

Information Security in Neural-Networked Queuing Systems

Viktor I. Samarin [a, *], Simon Zh. Simavoryan [a], Arsen R. Simonyan [a], Elena I. Ulitina [a]

[a] Sochi state university, Russian Federation

Abstract

Electronic information systems, used as an operator, regulator, communicator, navigator, tutor and verifier, are introduced into all spheres of human activity. On the basis of target software products of information processing and decision-making, the real-time management of production and technological, financial and banking, scientific and technical, political, energy-producing and distribution, educational and educational, advertising and trading, strategically important communication, military-operational and other processes is carried out.

The issues of improving the functioning of queuing systems as an integral part of the digital economy are considered. The actual tasks to be solved in the field of developing intellectual information protection means are proposed.

Keywords: queuing systems, network traffic safety, information protection, unauthorized access, network attacks, information leakage, the most demanded directions of intelligent systems development for information security.

1. Введение

Электронно-информационные системы, используемые в качестве оператора, регулятора, коммуникатора, навигатора, тьютора и верификатора, внедряется во все сферы деятельности человека. На базе целевых программных продуктов обработки информации и принятия решения осуществляется управление в реальном времени производственно-технологическими, финансово-банковскими, научно-техническими, политическими, энерго- производящими и распределительными, образовательно-просветительными, рекламно-трейдинговыми, стратегически значимыми коммуникационными, военно-оперативными и другими процессами. Поскольку активная экспансия электронной информации происходит во все сферы человеческой деятельности, то уязвимость информации может негативно сказаться на судьбе людей, деструктивно воздействовать на функционирование предприятий, угрожать экономико-политическим устоям государств и даже перспективам глобальной цивилизации. Абсолютно защищенных серверов, к сожалению, не существует, а при утрате контроля над аккаунтом пользователь электронными устройствами может не только потерять возможность пользоваться услугами того или иного сервиса, но и рискует тем, что от его имени могут действовать другие лица, в первую очередь, злоумышленники и кибермошенники. Взломщика систем защиты информации могут интересовать: государственные информационные ресурсы; конфиденциальные персональные (в том числе медико-диагностические и биометрические)

* Corresponding author
E-mail addresses: visamarin@mail.ru (V.I. Samarin), simsim58@mail.ru (S.Zh. Simavoryan), oppm@mail.ru (A.R. Simonyan), elenaulitina@mail.ru (E.I. Ulitina)

данные отдельных частных лиц или всех сотрудников организации и ее клиентов; информация о финансовых ресурсах и потоках; неофициальная переписка; оказываемые физическому лицу сервисные и медицинские услуги; инновационные технологии, инженерно-конструкторские решения, программное обеспечение; еще неопубликованные результаты научно-исследовательских разработок; диагностические методики; используемые формальные и неформальные коммуникационные каналы и т.д.

Работа человеческого мозга – это постоянное принятие решений. Различные схемы и принципы принятия решения приведены в (Самарин, 2000). Развитие кибернетики и нейросетей позволяет принятие хотя бы некоторых решений, в т.ч. управленческих, возложить на автоматизированные системы. Для этого разрабатываются системы искусственного интеллекта, которые на основе самообучения и выполняемых ими логичных аргументированных рассуждений и действий решают задачи аппаратного или программного моделирования эвристической творческой деятельности. В (Люгер, 2005), где детально описываются как теоретические основы искусственного интеллекта, так и примеры построения конкретных прикладных систем, искусственный интеллект определяется как способность автоматизированных систем к познанию, использованию знаний, разумному поведению в проблемных ситуациях. Таким образом, электронные интеллектуальные системы способны выполнять самообучение компьютерных программ (в первую очередь, эвристических) для выполнения экспертных и определенных творческих функций при решении некоторых практических задач, а также осуществляют действия, которые являются следствием обдуманных решений, принимаемых с учетом возможных последствий. Принятие решений интеллектуальной системой в условиях неопределенности на основе вероятностных рассуждений и статистические методы обучения искусственного интеллекта для выработки знаний, обеспечивающих принятие решений, исследованы в (Рассел, Норвиг, 2006).

2. Обсуждение

Предметный анализ

1. Функции СМО

Системы массового обслуживания (СМО) в исключительных случаях представляют замкнутые полностью роботизированные изолированные структуры с локальным программным управлением. В общем случае, СМО – открытая система, предназначенная для удовлетворения поступающих на ее вход требований (заявок, вызовов) и предполагает наличие человеческого фактора при выполнении этих требований, поэтому она достаточно уязвима. Целевыми приоритетами СМО являются бесперебойное функционирование и удовлетворение всех персональных, возможно эксклюзивных, запросов каждого клиента. Для достижения высокого уровня спроса на оказываемые услуги необходимо постоянно повышать качество сервиса. Рыночная экономика предполагает оперативную адаптацию к изменяющимся условиям, формированию или нахождению новых рынков, необходимость расширения сферы услуг путем привлечения инвестиций, перманентного совершенствования технологий и внедрения инновационного операционно-информационного обеспечения. Сервис – многоотраслевой экономический комплекс, он консолидирует деятельность множества секторально хозяйствующих субъектов, например, санаторный комплекс услуг предполагает взаимодействие с сервисным продуктом отелей, транспортных компаний, учреждений здравоохранения, службы безопасности, ресторанного бизнеса, банковского сектора, предприятий рекламной, печатной, фото- и сувенирной продукции, службы жилищно-коммунального хозяйства, строительных организации для реализации инфраструктурных проектов и выполнения текущего ремонта, организаций по благоустройству мест рекреации, центров экскурсионно-туристско-спортивно-оздоровительных мероприятий, службы автоматизации рабочих мест и компьютеризации мониторинговых, маркетинговых, коммуникационных и электронно-коммерческих операций и т.д. На основе наблюдений, свидетельств, анализа фактов, накопленного практического опыта и полученных результатов теоретических исследований, используя абдукцию, необходимо находить эмпирическое обоснование наиболее оптимальным параметрам функционирования СМО и осуществлять совершенствование законодательства в сфере сервиса.

Сервис должен быть доступным, удобным, оперативно предоставляемым потребителю,

все вопросы затребованного сервиса должны решаться с минимальными временными и ресурсными затратами как для организации, так и для потребителя. Этому должно способствовать широкое внедрение электронно-цифровых технологий оказания услуг.

2. Математическое обеспечение функционирования СМО

Уже на стадии обоснования целесообразности и эффективности сервиса необходимо изучение рынка спроса, получение стоимостной оценки предоставляемых услуг, установление срока окупаемости всех требуемых затрат, учесть возможные риски, неопределенности, турбулентности состояний системы, обстоятельств форс-мажора, выявить доминирующие факторы, определяющие устойчивость и доходность и, в целом, конкурентоспособность данного вида сервиса. Моделирование полного множества очевидных и латентных факторов в их «синергетическом» взаимодействии, влияющих на успешность и эффективность сервисной деятельности, относится к числу трудно формализуемых проблем (Samarin, 2013). Это обусловлено разноплановостью организационно-структурного и функционального назначения объектов сервиса, вариативным характером и неоднородностью состава клиентов, осуществлением деятельности в определенном правовом поле, требованием высокой степени ответственности работников сервиса за безопасность оказываемых услуг и т.д.

Для организации и мониторинга работы СМО используется разнообразный математический аппарат, применение которого могут реализовать электронные интеллектуальные системы:

- инструментарий математической статистики по обработке и кластеризации выборочных данных с учетом их нечеткости для вероятностных оценок возможных экстраординарных ситуаций и соответствующих доверительных интервалов этих оценок с целью подготовки к принятию необходимых упреждающих действий;
- факторный анализ – для выявления латентных факторов, определяющих функционирование систем в проблемных условиях;
- дисперсионный анализ – для установления реакции показателей динамической системы на контролируемые автономные или совместные внешние или внутренние воздействия;
- корреляционно-регрессионный анализ – для установления тесноты корреляционной связи случайных переменных и прогнозирования изменения усредненных значений одних случайных переменных при изменении величин других переменных;
- имитационное моделирование – для тестирования и диагностики поведения модели системы при воспроизведении различных эксплуатационных режимов, в том числе экстремальных;
- моделирование временных рядов – для определения тренда развития реализуемых процессов;
- использование методов теории графов – для оптимизации структур сетевых моделей сервисного комплекса, составления сетевых графиков и календарных планов;
- моделирование марковских процессов принятия решений – для реализации неопределенных рассуждений и принятия решений в условиях нечетких знаний;
- реализация алгоритмов динамического программирования – для оптимизации действий при принятии многошаговых решений в процессе радикальных изменений в сетевом трафике коммуникационной системы;
- осуществление математического программирования – для оптимизации управления критично ограниченными ресурсами на базе всего разнообразия известных алгоритмов, включая и предложенный в (Samarin, 2014a);
- использование прикладных моделей теории игр как инструментария эвристического поиска (Люгер, 2005) – для выработки оптимальных стратегий в условиях неопределенности и риска, а также учета фактора конкуренции на рынке услуг;
- анализ принятия решения на основе теории нечетких множеств – для формализации функционирования систем в условиях неполной информации и «расплывчатости» управляющих команд;
- использование нечеткой комбинаторики – как инструментария, например, для управления кадрами (расстановка кадров, обучение, повышение квалификации, перепрофилизация и т.д.) (Samarin, 2015);

- использование алгоритмов нечеткой или вероятностной модели задачи транспортного типа (Samarin, 2014b) – как одного из подходов к оптимизации распределения ограниченных ресурсов в условиях неопределенности;
- моделирование бифуркационных явлений на фоне синергетических переходов количественных изменений в качественные и наоборот;
- использование балансовой модели Леонтьева для учета **межотраслевых связей, пропорций и структур сервисного сектора экономики и другие разделы математики**.

Следует отметить, что для математического анализа реальных СМО часто приходится иметь дело с ее функционированием в неустановившемся режиме, поскольку реальные потоки заявок в СМО многоукладны, нечетки с эффектами турбулентности и, следовательно, отличаются от простейших.

3. Использование нейронных сетей в СМО

В условиях «цифровой экономики» в СМО все чаще внедряются интеллектуальные нейросетевые системы для:

– формирования и регуляции очередей – распределения и эшелонирования поступающих на вход системы заявок по очередям с учетом приоритетов, а также с учетом не только длины очередей, но и скорости их продвижения; с учетом возможности бесконфликтного восстановления в очереди ранее убывшей из этой очереди заявки; с учетом законодательных и этических норм, включая, при необходимости, экстренное изменение приоритета заявки/вызова и изыскание возможности безотлагательного обслуживания, предполагающего поиск свободных каналов, а в случае их отсутствия, прерывание в одном или нескольких каналах таких обслуживаний, которые не предусматривают неотложности; с учетом возможности перенаправления заявки от одного канала к другому при корректировке необходимой услуги или при настоятельном требовании клиента по персонификации обслуживания и т.д.;

– коммуникации при общении с клиентами в интерактивно-диалоговом режиме для уточнения индивидуальных запросов и предпочтений по каталогу и опциям сервиса до выполнения сервисных услуг, а также учету мнения клиента о качестве обслуживания при выходе из системы, его претензий и предложений по повышению качества сервиса после завершения сервиса;

– имплементации обратной связи с клиентом для оповещения о его фактическом положении в очереди, организации превентивных мер оперативного исключения простоев в работе системы по получению информации о задержке клиента, или его просьбы отложить предусмотренные сервисные процедуры на указываемый срок, или заявления об аннулировании сделанной ранее заявки;

– вывода на информационное табло сведений о длине очереди к каждому каналу, индикации занятости канала и его освобождении, отображения номера вызываемой заявки и выделяемого канала для ее обслуживания и т.д.;

– отслеживания заявок не по профилю сервисной организации, и направления отказа для таких заявок;

– управления режимом функционирования каналов, в частности, группировки или разгруппировки каналов с соответствующей функциональной дифференциацией в зависимости от характера и интенсивности требований на соответствующий сервис; задействование одного канала на облуживание в течение некоторого интервала времени нескольких заявок, например, в случае возможного режима частичного или полного самообслуживания; поиск резервного канала для замены вышедшего из строя;

– мониторинга времени обслуживания каждым каналом, фактического времени работы каждого работника сервиса и его производительности труда;

– получения информации о незагруженности каналов обслуживания и решения вопроса о соответствующем сокращении числа функционирующих каналов;

– определения интенсивности потоков поступающих заявок «онлайн» с учетом сегментации и сезонности предпочтений в сервисе и выработки рекомендаций изменения ценовой политики (вопросы сегментации и сезонности на примере туристского рынка рассмотрены, например, в (Балабанов, Балабанов, 2003));

– проверки и выработки консультационных предложений по соблюдению

государственного законодательства в области сервисной деятельности (Самарина, 2009);

– обеспечения математического моделирования для оптимизации и повышения качества сервиса при имеющихся ресурсах;

– учета использованных и еще имеющихся в резерве расходных материалов, своевременное оформление заказа на их пополнение;

– фиксация степени морального и физического износа оборудования и экономической целесообразности модернизации и диверсификации;

– осуществления объемно-предметного моделирования для изготовления необходимых заказчику изделий на 3D-принтере;

– управления автоматизированными рабочими местами, в том числе, осуществляющими прецизионное дозирование и выполнение метрологических (операционно-поверочных) измерений объемов жидкости (Ладария и др., 1988a; Ладария и др., 1988b);

– сигнализации о попытке информационного взлома системы или нарушения ее функционирования;

– контроля результатов управления на каждом этапе процесса функционирования системы;

– отслеживания информации о конкурентах, поиска возможных партнеров и выработки форм координации, консолидации, кооперации с ними;

– научно обоснованного прогнозирования состояния системы в локальные и интервальные значения времени и др.

Помимо общих функциональных операций возможны специфические, связанные с конкретным видом сервиса.

Так, при выполнении дистанционных образовательных услуг необходимо предусмотреть идентификацию личности, которой оказывается услуга, осуществлять видеоконтроль выполнения тестовых заданий и самостоятельной работы по академическим дисциплинам, фиксировать уровень освоения соответствующих дисциплин и т.д.

При выполнении медицинских услуг – организация очереди с учетом некоторых требований по направлению к персонифицируемому специалисту; компьютерная диагностика заболеваний с одновременным самообучением на основе обработки накапливаемых статистических данных; назначение процедур и дозировки, а также соблюдение последовательности введения в организм лекарственных препаратов; мониторинг динамики лечения; сопровождение эксплуатации робототехнических манипуляторов при выполнении или ассистировании ими хирургических операций и т.д.

В авиадиспетчерских – опознание «свой» - «чужой», слежение за трафиком авиаперелетов, оперативное выделение резервных взлетно-посадочных полос аэропорта при аварийных ситуациях, предупреждение экипажей о возможном опасном сближении бортов в воздухе, дистанционное управление самолетами в случае неработоспособности летного экипажа, отсечение из эфира шумовых сигналов, например, возникающих при ряде атмосферных явлений, от крупных птиц или стаи птиц и т.д.

При почтовых услугах – прослеживание в реальном времени траектории движения писем, посылок, финансовых переводов и др. от момента отправления до завершения услуги.

В рекламной деятельности – контроль над осуществлением непрерывной рекламы на стендах и дискретного повторения необходимое число раз на мониторах и телевизионных каналах с возможным различным временным интервалом при серии выводимых в эфир реклам в отводимое рекламное время.

В торговой сфере – сопровождение продукции от фактического региона производства до получателя с фиксацией пересечения всех логистических географических границ с учетом процедур перезагрузки с одного вида транспорта на другой, таможенного оформления и растаможивания.

Если при мониторинге системы массового обслуживания нейросетью моменты сбоев в системе из-за неопознанной инновационной злонамеренной атаки на СМО будут иметь пуассоновское распределение, а время бесперебойной работы будет подчинено показательному закону распределения, то вероятность безотказной работы в любой промежуток времени $[t_1; t_2]$ следующий за предыдущим временным интервалом

бесперебойной работы согласно характеристическому свойству показательного закона надежности работы системы будет определяться по формуле:

$$p = \exp[-\lambda(t_2 - t_1)], \quad (1)$$

где λ – нечеткое усредненное число сбоев, вызванных соответствующими атаками в единицу времени. Если же требуется определить вероятность сбоя, вызываемого такой атакой, в заданном интервале $[t_1; t_2]$, то следует использовать формулу интервальной вероятности:

$$p_{сб} = \exp(-\lambda t_1) - \exp(-\lambda t_2). \quad (2)$$

Вероятность того, что в СМО произойдет m сбоев в интервале времени $[t_1; t_2]$, вызванных серией злонамеренных атак, рассчитывается по формуле:

$$p_m(t_1, t_2) = \frac{\lambda^m \cdot (t_2 - t_1)^m}{m!} \cdot e^{-\lambda \cdot (t_2 - t_1)} \quad (3)$$

4. Защита безопасности функционирования СМО

Наибольшую опасность для жизни людей представляют СМО с одновременным массовым выполнением идентичных требований (массовые зрелищные, спортивные, развлекательные, процедурно-оздоровительные, маркетинговые, просветительно-выставочные и т.п. мероприятия, транспортные перевозки большого числа пассажиров, в первую очередь, в самолетах, поездах, на морских судах), когда возрастают последствия возможных терактов и катастроф. Поэтому особенно важны электронные формы защиты, включающие интеллектуальные средства наблюдения, поиска, слежения, сличения, обнаружения, опознания, проверки, регистрации, сигнализации, оповещения и т.д. Это, в свою очередь, требует обеспечения гарантированной защиты соответствующих электронных устройств и сетей от несанкционированного проникновения. В (Samarin et al., 2017) рассмотрены возможные последствия несанкционированного доступа к электронной информации, а также некоторые функции нейронных сетей, позволяющие в той или иной степени противодействовать несанкционированному доступу к электронной информации.

С точки зрения защиты информации и безопасности функционирования СМО нейросеть:

– обеспечивает сохранность базы данных клиентов системы массового обслуживая;

– отслеживает «фейковые» (ложные, искаженные, тенденциозно отфильтрованные) информационные сбросы о качестве обслуживания в соответствующей системе;

– оперативно фиксирует хакерские программы, позволяющие формировать поток вызовов на выбранные «кустовым способом» адреса систем массового обслуживания;

– осуществляет пресечение взлома коммуникационных каналов связи и проникновения в операционные комплексы с целью трансформации компьютерных программ, дезорганизации работы системы, вымогательства;

– зондирует и локализует доменные адреса источников злонамеренных атак на систему;

– идентифицирует дистанционные устройства лже-вызова и способы доставки вредоносных программ, в том числе вирусов-шифровальщиков;

– исключает или снижает вероятность ошибочной блокировки всей системы при локальных сбоях в ее работе;

– информирует о возникновении угрозы возникновения режима бесконечного среднего времени ожидания ($\theta \geq 1$, где θ – интенсивность нагрузки на каждый канал) и востребованности открытия нового канала обслуживания;

– осуществляет поиск неисправней в системе и их оперативное устранение, повышая отказоустойчивость СМО;

– при выполнении функций мессенджера реализует мгновенный обмен информацией с клиентами СМО с высокой степенью безопасности и конфиденциальности;

– при печати на 3D-принтерах предотвращает использование соответствующих технологий для производства социально опасных изделий, конструкций и веществ.

В (Ефремова, 2016) рассмотрены преимущества и особенности обучения нейронных сетей для обеспечения информационной безопасности и их применение на практике. В (Нестерук, Нестерук, 2008) отмечено, что применение нейронных сетей для решения

задач защиты информации связано, в первую очередь, с интеллектуальным анализом временных рядов (например, динамики трафика защищаемой локальной сети) и на его основе прогнозированием, а также поиском скрытых закономерностей в массивах первичных данных.

Выделим следующие достоинства нейронных сетей при обеспечении информационной безопасности СМО:

- автоматическое отслеживание и кластеризация злонамеренных проникновений в систему и в силу этого обеспечение оперативности их идентификации;
- иерархическое выстраивание многоуровневой экспертизы программного обеспечения и расследования инцидентов угрозы информационной безопасности;
- возможность самообучения по результатам обработки информации некоторой последовательности кибератак, выявления скрытых закономерностей и на их основе обновления программного обеспечения защиты, и, как следствие, адаптации сети к распознаванию инновационных разновидностей вредоносного программного продукта и автоматического обеспечения СМО более мощной электронной защитой;
- автоматическое осуществление копирования возникающих новых массивов данных и их безопасное хранение на резервных носителях информации;
- благодаря нелинейности по своей сути нейросеть способна обнаруживать атаки, которые могут оказаться незамеченными неинтеллектуальными средствами защиты;
- благодаря формируемой ассоциативной памяти нейросеть способна обнаруживать кибератаки по нечетким (неполным и даже частично недостоверным) данным, поступающим на вход СМО;
- благодаря возможности реализации в нейросети определенных обратных связей достигается функциональная устойчивость сети в процессах обнаружения атак базы данных сигнатур и правил, с помощью которых анализируются признаки входных сигналов.

Процесс защиты безопасности системы нейросетью осуществляется в 2 этапа: сначала на иммунный этапе – из нечеткого набора признаков атаки формируется нечеткий выходной вектор угроз информационной безопасности; затем на рецепторном этапе, исходя из компонент нечеткого вектора угроз, активизируются соответствующие механизмы информационной защиты системы.

Особое внимание следует уделять программному обеспечению кибернетических устройств, предназначенных для оказания сервиса при непосредственном контакте с заказчиком. Безопасное функционирование компьютерных систем не ограничивается лишь обеспечением надежности работоспособности автоматизированных средств и сохранности конфиденциальной информации, но в настоящее время выходит на новый уровень гарантий – обеспечение безопасности человека, представляя угрозу для цивилизации в целом. Франс Холле, создатель искусственной нейронной сети The Verge предупреждает: «Пожалуй, самая большая угроза – массовый контроль над населением посредством таргетинга сообщений и пропагандистских бот-армий». Генеральный директор Tesla и SpaceX Элон Макс заявил, что работы в области искусственного интеллекта нуждаются в государственном регулировании. Он привел в пример случаи внедрения технологий искусственного интеллекта в интернет: «Роботы могут начать войну, выпуская «фейковые» новости и подделывая учетные записи электронной почты и пресс-релизы, манипулируя информацией». Физик-теоретик Макс Тегмарк из Массачусетского технологического института (США) отмечает, что исследование искусственного интеллекта зачастую игнорирует проблему сознания, в частности, различие между сознательной и бессознательной системами обработки информации, характерными для живой и неживой природы, что представляет риск для будущего человечества.

В силу этого необходимы разработки и внедрение «профилактических прививок» – «антивирусов» и «антидотов» для интеллектуальных систем, позволяющих таким системам мгновенно распознавать и нейтрализовать опасные злонамеренные чужеродные программные продукты, а в случае затруднений искусственный интеллект должен самоблокироваться, чтобы исключить возможную агрессивность интеллектуальных манипуляторов по отношению к человеку.

Несанкционированный доступ к информации, включая вирусную атаку на серверы, может привести к сбою в локальной сети СМО; к нарушению каналов связи с внешними партнерами во внешней сети; к уничтожению или блокированию программного обеспечения

и базы данных; к похищению персональных данных персонала и клиентуры СМО.

Для электронной защиты информации от компьютерных вирусов, программ-шпионов и других киберпреступлений, требуется создавать такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму. Для реализации такой защиты используются, в первую очередь, криптографические методы кодирования для преобразования этой информации. В настоящее время на практике наиболее распространены блочные шифры. Эти методы базируются на дискретной математике, вероятностных закономерностях, статистических наблюдениях и математических методах обработки выборочных данных, математической логике и теории алгоритмов.

Основные модели СМО приведены, например, в (Вентцель, 1972; Даниелян, Симонян, 2005). Подробно изучены траектории основных характеристик моделей M|G|1|∞ и GI|G|s|∞ при разных ограничениях на загрузку систем и доказаны теоремы в виде классических предельных теорем теории вероятностей в (Simonyan, Ulitina, 2004; Simonyan, 2015; Simonyan, Ulitina, 2015).

Задачей функциональной логистики является управление всеми информационными, материальными и сервисными потоками СМО. Приведем основные схемы потоков в различных обобщенных моделях *n*-канальных СМО (рис. 1-5).

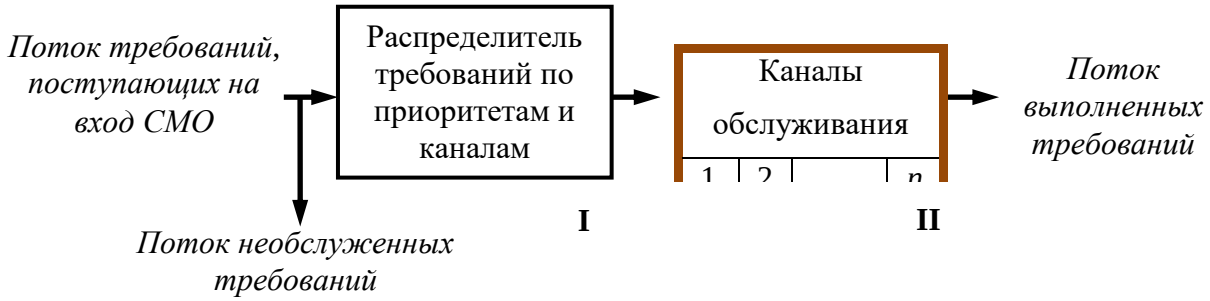

Рис. 1. Схема потоков в СМО с отказами (потерями)

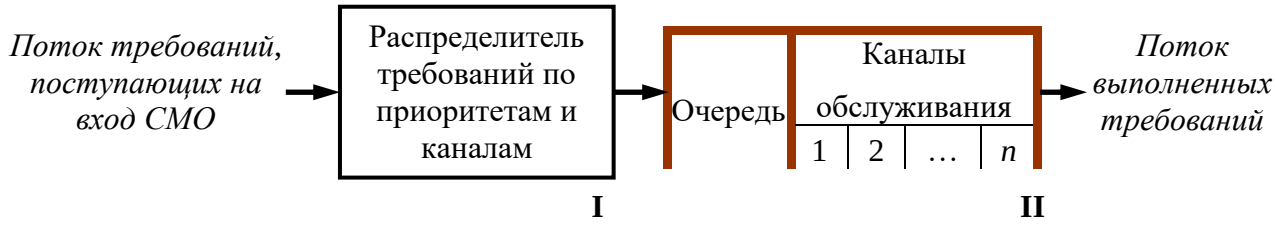

Рис. 2. Схема потоков в СМО с неограниченным временем ожиданием

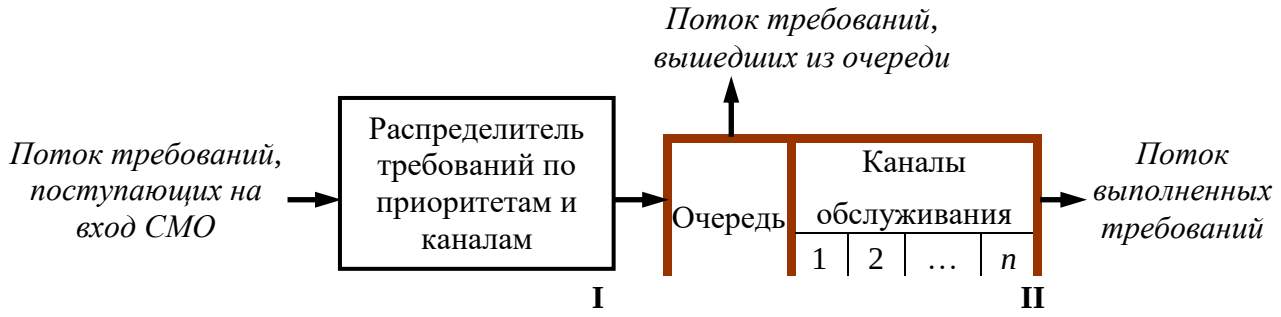

Рис. 3. Схема потоков в СМО с ограниченным временем ожиданием

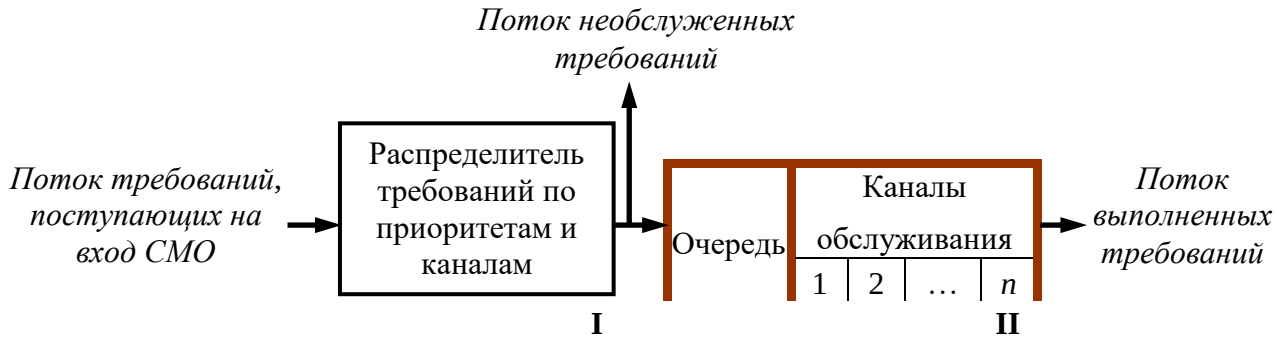

Рис. 4. Схема потоков в СМО с ограниченной очередью

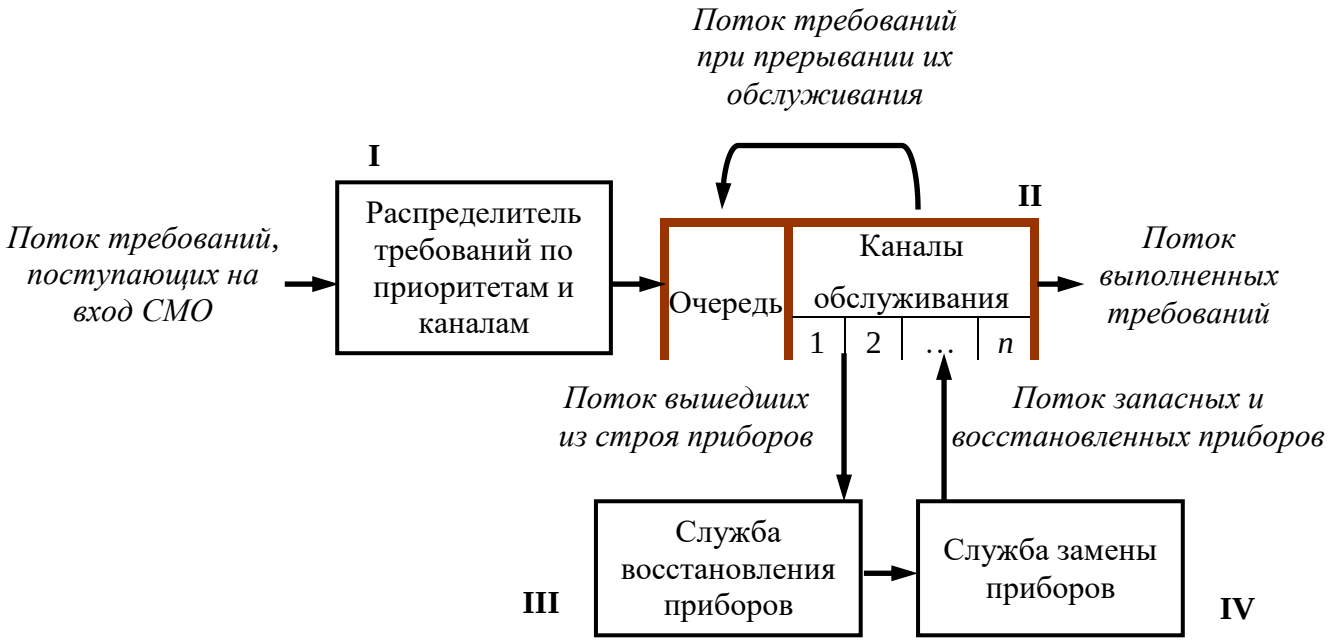

Рис. 5. Схема потоков в СМО с восстанавливаемыми каналами (приборами) обслуживания при неограниченной очереди

При отказе прибора выполнявшаяся операция обслуживания прерывается. Т.о., отказ прибора равносилен появлению требования, обладающего абсолютным приоритетом перед остальными требованиями, находящимися в очереди. Для сохранения стабильной работоспособности СМО с ненадежными обслуживающими приборами необходимо иметь некоторый резерв исправной аппаратуры для срочной замены приборов, в работе которых произошел сбой.

Одноканальные СМО являются частным случаем приведенных моделей ($n = 1$). Замкнутая СМО рассмотрена, например, в (Вентцель, 1972; Samarin, 2016). Простейшие модели СМО с приоритетом анализировались, например, в (Самарин, 2008).

Обеспечение безопасности и гарантированной работоспособности электронных средств СМО достигается предотвращением искажений в информации о потоках, входящих в систему или в ее составные блоки. Взлом системы и возможное влияние человеческого фактора внутри системы могут привести к сбою информационно-функциональных процессов в СМО, к блокировке доступа к имеющимся в системе электронным информационным ресурсам. Наиболее опасным является проникновение злонамеренного сигнала, в том числе в виде законспирированного требования, с потоком требований на вход СМО. При этом могут выйти из строя как отдельные блоки системы, так и вся система в целом в силу существующих взаимосвязей и взаимодействий всех структурных элементов

системы. При сбое в **I** блоке возможны нарушения в очередности требований, в наибольшей степени, если очередь электронная. При этом может возникнуть подача требований на уже занятый канал, путаница в приоритетах, прерывание приема новых требований при наличии свободных каналов и т.д. При сбое во **II** блоке возможны отказы в работе каналов, блокировка входа в каналы, прерывание сигнала об освобождении канала, нереагирование системы на вышедшие из строя приборы, запирание требования в СМО и т.п. При сбое в **III** блоке возможны прекращение восстановления вышедших из строя приборов, приостановка передачи восстановленных приборов в **IV** блок и т.д. При сбое в **IV** блоке возможно прекращение замены вышедших из строя приборов на резервные или восстановленные.

Следует отметить, что ко всем перечисленным потокам необходимо добавить общий информационный поток системы, формируемый в результате слияния входящего в систему потока с внутрисистемными потоками. В свою очередь, одна часть информационного потока системы циркулирует внутри этой системы, а другая – передается во внешнюю информационную сеть (рис. 6).

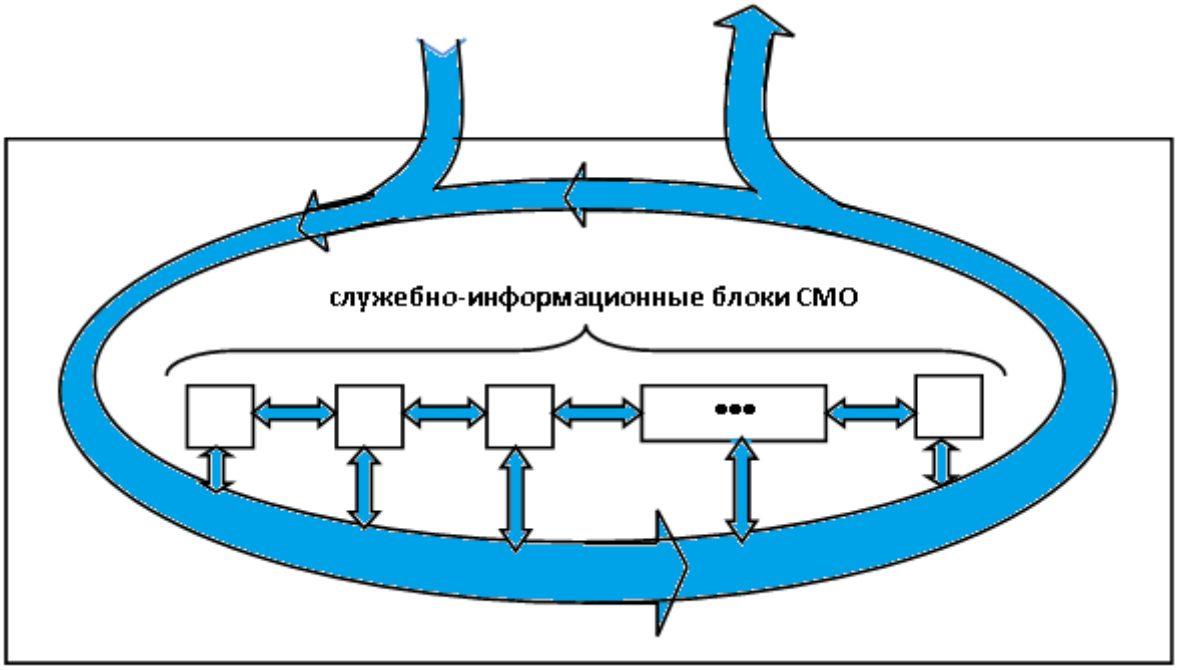

Рис. 6. Схема информационных потоков в СМО

В результате с увеличением в системе числа служебных блоков возрастает уязвимость ее информационной безопасности. Поэтому отслеживание, предотвращение, нейтрализация соответствующих злонамеренных проникновений в операционные комплексы должны гарантировать интеллектуальные средства защиты аппаратных и программных электронных средств, обеспечивая бесперебойное функционирование систем массового обслуживания. В (Симаворян и др., 2015) рассмотрены основные задачи оперативно-диспетчерского управления защитой информации в автоматизированных системах обработки данных и проанализированы возможности использования методов искусственного интеллекта. В (Симаворян и др., 2014) рассмотрены вопросы наделения систем защиты информации возможностями интеллектуальности.

3. Заключение

Рассмотренные задачи в области совершенствования функционирования систем массового обслуживания как составной части цифровой экономики и разработки интеллектуальных средств защиты информации позволят структурировать первоочередные разработки для достижения соответствующих целей в условиях риска и неопределенности.

4. Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 16-01-00527 и 15-01-99482.

Литература

Балабанов, Балабанов, 2003 – *Балабанов И.Т., Балабанов А.И.* (2003). Экономика туризма. М: Финансы и статистика. 176 с.

Вентцель, 1972 – *Вентцель Е.С.* (1972). Исследование операций. М.: Советское радио. 552 с.

Даниелян, Симонян, 2005 – *Даниелян Э.А., Симонян А.Р.* Введение в теорию очередей. Ереван: РАУ. 2005, 196 с.

Ефремова, 2016 – *Ефремова Е.В.* Нейронные сети в информационной безопасности. *Научный альманах*, 2016, № 2-1(16). С. 154-156.

Ладария и др., 1988a – *Ладария Г.Г., Акопов В.А., Самарин В.И., Фараджян В.С.* Устройство для определения масштабного номера шкалы жиромера // Бюллетень Госкомитета СССР по делам изобретений и открытий «Открытия, изобретения, промышленные образцы, товарные знаки», № 14. Авторское свидетельство № 1388727, 1998.

Ладария и др., 1988b – *Ладария Г.Г., Акопов В.А., Самарин В.И., Фараджян В.С.* Программно-управляемый функциональный модуль воспроизведения вместимости // *Научно-технический реферативный сб. «Метрологическая служба в СССР»*, вып. 8. С. 37-44.

Люгер, 2005 – *Люгер Дж.Ф.* Искусственный интеллект: стратегии и методы решения сложных проблем. 2005. М.: Вильямс. 864 с.

Нестерук, Нестерук, 2008 – *Нестерук Г.Ф., Нестерук Ф.Г.* Применение нейронных сетей для интеллектуального анализа данных при решении задач защиты информации: Методические указания. 2008. СПб.: СПбГУ ИТМО. 32 с.

Рассел, Норвиг, 2006 – *Рассел С., Норвиг П.* Искусственный интеллект: Современный подход. М.: Издательский дом «Вильямс». 2006, 1408 с.

Самарин, 2000 – *Самарин В.И.* Общая постановка задачи о принятии решения: методология математического обоснования // *Труды Сочинского государственного университета туризма и курортного дела*, вып. 1. Сочи: РИЦ СГУТиКД. 2000. С. 220-238.

Самарин, 2008 – *Самарин В.И.* Простейшие модели СМО с приоритетом. // Материалы IV Всероссийской научно-практической конференции «Актуальные задачи математического моделирования и информационных технологий» (13-18 мая 2008 г., гор. Сочи). Сочи: СГУТиКД. 164 с.

Samarin, 2013 – *Samarin V.I.* (2013). Constituents of Service Activity Systems Analysis // *European Researcher*, vol. (48), № 5-1. pp. 1110-1113.

Samarin, 2014a – *Samarin V.I.* Composite Principal-Dual Simplex Method for Linear Programming Solving // *Modeling of Artificial Intelligence*, 2014, vol. (3), № 3. pp. 126-132.

Samarin, 2014b – *Samarin V.I.* Transportation Model with Stochastic Restrictions on Cargo Supply Solution // *Modeling of Artificial Intelligence*, 2014, vol. (1), № 1. pp. 22-28.

Samarin, 2015 – *Samarin V.I.* Fuzzy Combinatorics // *Russian Journal of Mathematical Research, Series A*, 2015, vol. (2), Is. 2. pp. 45-57.

Samarin, 2016 – *Samarin V.I.* Linear Programming in a Closed Loop Queuing System // *Russian Journal of Mathematical Research. Series A*, 2016, vol. (4), Is. 2. pp. 56-63.

Samarin et al., 2017 – *Samarin V.I., Simavoryan S.Zh., Simonyan A.R., Ulitina E.I.* Neural Networks as Intelligent Units Prospects for Information Protection // *American Scientific Journal*, 2017, vol. 1, № (15). pp. 19-25.

Самарина, 2009 – *Самарина Т.В.* Организационные и правовые основы государственного управления курортным делом: первая половина XVIII века – начало XXI века. М.: Изд-во Современного гуманитарного университета. 2009, 199 с.

Simavoryan et al., 2014 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A.* About one Approach to a Question of Classification of Intellectual Systems of Information Security // *Modeling of Artificial Intelligence*, 2014, vol. (1), № 1. pp. 29-44.

Simavoryan et al., 2015 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A.* Research of the Intellectual Antagonism of Malefactors and Service of Information Security in the

ADPS // *Modeling of Artificial Intelligence*, 2015, vol. (5), Is. 1. pp. 33-41.

Simonyan, 2015 – *Simonyan A.R.* Around the Model GI|G|s|∞ // *Russian Journal of Mathematical Research, Series A*, 2004. vol. (2), Is. 2. pp. 58-61.

Simonyan, Ulitina, 2004 – *Simonyan A.R., Ulitina E.I.* A Theorem on the Convergence to a Stable Law in the M|G|1|∞ Model // *Russian Mathematical Surveys*, 2004, vol. 59. № 3. pp. 589-590.

Simonyan, Ulitina, 2015 – *Simonyan A.R., Ulitina E.I.* (2015). Properties of the Trajectories of Waiting Times and Downtime in Single-channel Models with Expectation // *Russian Journal of Mathematical Research, Series A*, vol. (2), Is. 2. pp. 62-72.

References

Balabanov, Balabanov, 2003 – *Balabanov I.T., Balabanov A.I.* (2003). Ekonomika turizma [Tourism Economics]. M: Finansy i statistika. 176 p. [in Russian]

Venttsel', 1972 – *Venttsel' E.S.* (1972). Issledovanie operatsii [Operations research]. M.: Sovetskoe radio. 552 s.

Danielyan, Simonyan, 2005 – *Danielyan E.A., Simonyan A.R.* (2005). Vvedenie v teoriyu ocheredei [Introduction to the theory of queuing]. Erevan: RAU. 196 p. [in Russian]

Efremova, 2016 – *Efremova E.V.* (2016). Neironnye seti v informatsionnoi bezopasnosti [Neural networks in information security]. *Nauchnyi al'manakh*, № 2-1(16). pp. 154-156. [in Russian]

Ladariya i dr., 1988a – *Ladariya G.G., Akopov V.A., Samarin V.I., Faradzhyan V.S.* (1988). Ustroistvo dlya opredeleniya masshtabnogo nomera shkaly zhiromera [The device for determining the scale number of the scale of the zhiromer]. Byulleten' Goskomiteta SSSR po delam izobretenii i otkrytii «Otkrytiya, izobreteniya, promyshlennye obraztsy, tovarnye znaki», № 14. Avtorskoe svidetel'stvo № 1388727. [in Russian]

Ladariya i dr., 1988b – *Ladariya G.G., Akopov V.A., Samarin V.I., Faradzhyan V.S.* (1988). Programmno-upravlyaemyi funktsional'nyi modul' vosproizvedeniya vmestimosti [Program-driven function module for reproducing capacity]. *Nauchno-tekhnicheskii referativnyi sb. «Metrologicheskaya sluzhba v SSSR»*, vyp. 8. pp. 37-44. [in Russian]

Lyuger, 2005 – *Lyuger Dzh.F.* (2005). Iskusstvennyi intellekt: strategii i metody resheniya slozhnykh problem [Artificial intelligence: strategies and methods for solving complex problems]. M.: Vil'yams. 864 p. [in Russian]

Nesteruk, Nesteruk, 2008 – *Nesteruk G.F., Nesteruk F.G.* (2008) Primenenie neironnykh setei dlya intellektual'nogo analiza dannykh pri reshenii zadach zashchity informatsii [Application of neural networks for intellectual analysis of data in solving problems of information protection]: Metodicheskie ukazaniya. SPb.: SPbGU ITMO. 32 p. [in Russian]

Rassel, Norvig, 2006 – *Rassel S., Norvig P.* (2006). Iskusstvennyi intellekt: Sovremennyi podkhod [Artificial intelligence: the modern approach]. M.: Izdatel'skii dom «Vil'yams». 1408 p. [in Russian]

Samarin, 2000 – *Samarin V.I.* (2000). Obshchaya postanovka zadachi o prinyatii resheniya: metodologiya matematicheskogo obosnovaniya [General formulation of the problem of decision-making: the methodology of mathematical justification]. *Trudy Sochinskogo gosudarstvennogo universiteta turizma i kurortnogo dela*, vyp.1. Sochi: RITs SGUTiKD. pp. 220-238. [in Russian]

Samarin, 2008 – *Samarin V.I.* (2008). Prosteishie modeli SMO s prioritetom [The simplest CMO models with priority]. Materialy IV Vserossiiskoi nauchno-prakticheskoi konferentsii «Aktual'nye zadachi matematicheskogo modelirovaniya i informatsionnykh tekhnologii» (13-18 maya 2008 g., gor. Sochi). Sochi: SGUTiKD. 164 p. [in Russian]

Samarin, 2013 – *Samarin V.I.* (2013). Constituents of Service Activity Systems Analysis. *European Researcher*, vol. (48), № 5-1. pp. 1110-1113.

Samarin, 2014a – *Samarin V.I.* (2014). Composite Principal-Dual Simplex Method for Linear Programming Solving. *Modeling of Artificial Intelligence*, vol. (3), № 3. pp. 126-132.

Samarin, 2014b – *Samarin V.I.* (2014). Transportation Model with Stochastic Restrictions on Cargo Supply Solution. *Modeling of Artificial Intelligence*, vol. (1), № 1. pp. 22-28.

Samarin, 2015 – *Samarin V.I.* (2015). Fuzzy Combinatorics. *Russian Journal of Mathematical Research, Series A*, vol. (2), Is. 2. pp. 45-57.

Samarin, 2016 – Samarin V.I. (2016). Linear Programming in a Closed Loop Queuing

System. *Russian Journal of Mathematical Research. Series A*, vol. (4), Is. 2. pp. 56-63.

Samarin et al., 2017 – *Samarin V.I., Simavoryan S.Zh., Simonyan A.R., Ulitina E.I.* Neural Networks as Intelligent Units Prospects for Information Protection. *American Scientific Journal*, vol. 1, № (15). pp. 19-25.

Samarina, 2009 – *Samarina T.V.* (2009). Organizatsionnye i pravovye osnovy gosudarstvennogo upravleniya kurortnym delom: pervaya polovina XVIII veka – nachalo XXI veka [Organizational and legal foundations of state management of the resort business: the first half of the XVIII century – the beginning of the XXI century]. M.: Izd-vo Sovremennogo gumanitarnogo universiteta. 199 p. [in Russian]

Simavoryan et al., 2014 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A.* About one Approach to a Question of Classification of Intellectual Systems of Information Security. *Modeling of Artificial Intelligence*, vol. (1), № 1. pp. 29-44.

Simavoryan et al., 2015 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A.* Research of the Intellectual Antagonism of Malefactors and Service of Information Security in the ADPS. *Modeling of Artificial Intelligence*, vol. (5), Is. 1. pp. 33-41.

Simonyan, 2015 – *Simonyan A.R.* (2015). Around the Model GI|G|s|∞. *Russian Journal of Mathematical Research, Series A*, vol. (2), Is. 2. pp. 58-61.

Simonyan, Ulitina, 2004 – *Simonyan A.R., Ulitina E.I.* (2004). A Theorem on the Convergence to a Stable Law in the M|G|1|∞ Model. *Russian Mathematical Surveys*, vol. 59. № 3. pp. 589-590.

Simonyan, Ulitina, 2015 – *Simonyan A.R., Ulitina E.I.* (2015). Properties of the Trajectories of Waiting Times and Downtime in Single-channel Models with Expectation. *Russian Journal of Mathematical Research, Series A,* vol. (2), Is. 2. pp. 62-72.

Защита информации в нейросетевых системах массового обслуживания

Виктор Иванович Самарин [a, *], Симон Жоржевич Симаворян [a], Арсен Рафикович Симонян [a], Елена Ивановна Улитина [a]

[a] Сочинский государственный университет, Российская Федерация

Аннотация. Электронно-информационные системы, используемые в качестве оператора, регулятора, коммуникатора, навигатора, тьютора и верификатора, внедряется во все сферы деятельности человека. На базе целевых программных продуктов обработки информации и принятия решения осуществляется управление в реальном времени производственно-технологическими, финансово-банковскими, научно-техническими, политическими, энерго- производящими и распределительными, образовательно-просветительными, рекламно-трейдинговыми, стратегически значимыми коммуникационными, военно-оперативными и другими процессами.

Рассмотрены вопросы совершенствования функционирования систем массового обслуживания как неотъемлемой части цифровой экономики. Предложены актуальные задачи, подлежащие решению в области разработки интеллектуальных средств защиты информации

Ключевые слова: системы массового обслуживания, безопасность сетевых трафиков, защита информации, несанкционированный доступ, сетевые атаки, утечка информации, наиболее востребованные направления развития интеллектуальных систем для обеспечения информационной безопасности.

[*] Корреспондирующий автор

Адреса электронной почты: visamarin@mail.ru (В.И. Самарин), simsim58@mail.ru (С.Ж. Симаворян), oppm@mail.ru (А.Р. Симонян), elenaulitina@mail.ru (Е.И. Улитина)