УДК 004.89 DOI: 10.17587/it.26.185-191

Е. А. Басыня, канд. техн. наук, доц.[1], директор[2], e-mail: director@nii-ikt.ru,
[1]Новосибирский государственный технический университет,
[2]Научно-исследовательский институт информационно-коммуникационных технологий, г. Новосибирск

Метод интеллектуально-адаптивного управления информационной инфраструктурой предприятия

Предлагается новый метод интеллектуально-адаптивного управления информационной инфраструктурой предприятия, позволяющий обеспечить исправное и отказоустойчивое функционирование технических систем и объектов со снижением загрузки канала связи. Выбор рациональной стратегии реагирования на различные типы воздействий осуществляется их интеллектуальной обработкой с прогнозированием реакции сервисов на изолированных модельных объектах.

Ключевые слова: *системный анализ, интеллектуально-адаптивное управление, обработка, сетевой трафик, локальные информационные процессы, нештатные воздействия, информационная безопасность, TCP/IP, угрозы, атаки*

Введение

Развитие информационных технологий является глобальным трансграничным процессом, затрагивающим все сферы деятельности общества. Повышение эффективности, надежности, отказоустойчивости и качества различных технических систем являются приоритетными задачами научного сообщества и бизнеса. Их успешное решение позволяет оптимизировать информационные и рабочие процессы хозяйствующих субъектов, повысить рентабельность их функционирования. На сегодняшний день практически любой вид экономической деятельности использует сетевое взаимодействие на основе стека протоколов TCP/IP (англ. Transmission Control Protocol/ Internet Protocol). Технические отрасли не составляют исключение, невозможно представить современную автоматизацию любого производственного процесса без использования информационных технологий.

Важно отметить, что задачи системного анализа, управления и обработки информационных потоков и процессов являются приоритетными, смещается вектор их развития в сторону программных и аппаратно-программных решений. Уровень информационной безопасности предприятия становится следствием эффективности решения данных задач.

Разработкой методов управления информационными потоками и процессами занимаются российские и зарубежные ученые: О. Б. Калугина, С. М. Трошина, Н. В. Штуллер, L. Sung-Ho, P. Jun-Sang, J. Woo-Suk, P. Jun-Sang и др. [1—4]. Предлагаемые подходы обеспечивают надежную и отказоустойчивую работу информационных систем посредством использования сигнатурной обработки трафика. Другой интересный подход излагается в работах Р. Р. Файзулина, А. Я. Инсарова, L. He, Y. Cuibo, G. Xuerong, H. Jieying, J. Z. Zhang, L. Lishi и заключается в идентификации автомодельности сетевых потоков [5—8].

К сожалению, данные методы не выполняют поиск рациональной стратегии реагирования на несанкционированные внутренние и внешние воздействия различного уровня риска. Осуществляется лишь сигнатурная обработка инцидентов или идентификация автомодельности трафика, которые в случае отсутствия корректных начальных условий не могут быть выполнены. В качестве простого примера стоит упомянуть шифрование информацион-

ных потоков и использование виртуальных защищенных каналов связи.

Под рациональной стратегией реагирования подразумевается комплекс мер, позволяющий максимально снизить загрузку канала связи в сравнении с альтернативными решениями, но без негативных воздействий на штатные информационные потоки и процессы, а также на уровень безопасности информационно-коммуникационного сектора предприятия. При этом важно отметить, что производители программных и аппаратно-программных сетевых решений могут иметь различные правила обработки идентичных инцидентов.

Соответственно, возрастает актуальность разработки проблемно-ориентированных методов управления сетевым трафиком и локальными информационными процессами, позволяющих в автоматическом режиме проводить поиск и применение рациональной стратегии реагирования.

1. Цель работы

Целью данной работы являлась разработка нового метода интеллектуально-адаптивного управления информационной инфраструктурой предприятия. Необходимо было обеспечить исправное и отказоустойчивое функционирование технических систем и объектов со снижением загрузки каналов связи при разнообразных внутренних и внешних воздействиях различного уровня риска.

Следовало минимизировать риск перехода информационных систем в режим недоступности. Требовалось обеспечить высокий уровень безопасности информационной инфраструктуры предприятия без ущерба штатным информационным потокам, которые могли бы проводиться и с применением технологий анонимизации.

Ставилась задача разработки концепции автоматического поиска и применения рациональной стратегии реагирования на различные типы возмущений с возможностью самообучения и самоорганизации правил и модулей управления.

2. Предлагаемое решение

Целевое и практическое назначение предлагаемого метода — обеспечение функционирования авторской программной системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия (далее именуемой "Система" или "СИАУ ИИП"). Ее разработка, проектирование, программная реализация и исследование будут представлены в следующей статье.

Рассмотрим метод интеллектуально-адаптивного управления информационной инфраструктурой предприятия на примере работы СИАУ ИИП (рис. 1, см. четвертую сторону обложки).

Система осуществляет управление всеми объектами информационной инфраструктуры предприятия: пользовательскими электронно-вычислительными машинами, выделенными и виртуальными серверами, управляемым сетевым оборудованием (коммутаторами, маршрутизаторами и другими объектами), авторскими наукоемкими системами и сервисами, техническими объектами и системами промышленности (в том числе компонентами автоматизированных систем управления технологическим процессом), функционирующими на основе стека протоколов TCP/IP.

Повышение надежности, отказоустойчивости и качества технических систем достигается комплексным управлением трафиком и информационными процессами на всех уровнях взаимодействия.

2.1. Задача управления информационными потоками и процессами

Задача управления трафиком вычислительной сети может быть решена различными способами. Оценка эффективности вариантов решения сводится к сравнению загрузки канала связи при условии сохранения штатного режима обработки легитимных информационных потоков и процессов (рис. 2, см. четвертую сторону обложки). На программном уровне проводится ряд наблюдений за изменением загрузки канала связи в определенный интервал времени. Осуществляется оценка быстродействия принятия решений с мониторингом уровня безопасности информационно-коммуникационного сектора предприятия.

Сетевое оборудование (маршрутизаторы, межсетевые экраны) имеют несколько сетевых интерфейсов, организующих разные каналы связи в рамках локальных или глобальных сетевых взаимодействий. Соответственно, для каждого из них в параллельном режиме может осуществляться поиск рациональной стратегии обработки различных типов сетевых воздействий.

В качестве математической абстракции описания данного подхода может быть введен безразмерный критерий рациональности J, представляющий суммарный критерий снижения загрузки линии связи J_1 и быстродействия J_2:

$$J = J_1 + J_2 = F(u, h, t) + \frac{kr}{d}T, \qquad (1)$$

где $F(u, h, t)$ — функция загрузки канала, в связи с отсутствием возможности представления в математическом виде рассматриваемая как нелинейная, псевдослучайная, описывающая изменение пропускной способности вычислительной сети во времени t; h — нежелательные возмущения; $u \in \Omega_u$ — управляющее воздействие (набор команд модулям системы согласно стратегии реагирования), Ω_u — рабочая область управляющих воздействий; T — время принятия решений по управлению; k — стоимостной коэффициент, определяемый новизной управляющего воздействия (чем "новее" решение, тем меньше коэффициент; тем самым предоставляется небольшое окно по времени поиска новых решений, а не использованию старых; базовый интервал начальных значений: [0,5; 1], автономно корректируются системой для различных типов активности); d — коэффициент достоверности определения типа возмущения, $d \in [0; 1]$; r — коэффициент риска, который назначен системой определенному виду нештатных воздействий, $r \in [0, \infty)$. Бесконечность подразумевает, что решение не может быть принято ни при каких условиях, так как несет риски информационной безопасности, сопровождающие его принятие.

Под внешними воздействиями понимаются информационные потоки трафика вычислительной сети, предназначенные непосредственно Системе или объектам информационной инфраструктуры предприятия, которыми она управляет. Это могут быть штатные информационные взаимодействия, несанкционированные внешние или внутренние возмущения, способные нанести существенный вред нормальному функционированию технических объектов. Природа последних запросов может быть обусловлена как аппаратно-программными неполадками, так и злоумышленными намерениями сторонних лиц или сотрудников из числа доверенных пользователей.

Существующие системы управления не являются комплексными продуктами, включают атомарный функционал и используют "жесткую" логику поведения, не проводящую сравнительного анализа и поиска рационального решения (снижающего загрузку канала связи и обеспечивающего исправное, надежное, отказоустойчивое и безопасное функционирование технических систем и объектов). Это позволяет хакерам однозначно идентифицировать продукт защиты атакуемого объекта посредством инструментов активного и пассивного анализа трафика и информационных ресурсов (сканеров/зондеров, инструментов пентеста и др.) с последующей эксплуатацией уязвимости для нарушения работоспособности узлов/сети.

2.2. Блок генетической алгоритмизации и нечеткой логики

В целях нивелирования описанных рисков было решено спроектировать и реализовать методы, обладающие интеллектуально-адаптивными свойствами. Важно отметить, что в рассматриваемой задаче поиска рационального решения в управлении информационными потоками существует значительный недостаток априорной информации о структуре всех объектов и систем, а также о характерах возмущений. Для получения устойчивых решений в данной ситуации было сделано заключение о применении генетической алгоритмизации (ГА), обладающей гибкостью функционирования, возможностью выхода из локальных на глобальные экстремумы, возможностью эффективного распараллеливания вычислений, высокой скоростью поиска решений на нелинейных функциях и другими преимуществами.

Необходимость принятия решений в условиях приближенных рассуждений аргументировало применение связки генетической алгоритмизации с нечеткой логикой (англ. fuzzy logic). Технологии нейронных, гибридных и других сетей являются избыточным инструментом в срезе исследуемой задачи.

Поскольку в задачах снижения загрузки канала связи и обеспечения исправного, надежного, отказоустойчивого и безопасного функционирования технических систем и объектов некоторые экземпляры решений недопустимы (могут нарушить штатное функционирование инфраструктуры предприятия), а также в связи с необходимостью реализовать механизмы подмены и прогнозирования реакций на модельных объектах (МО) разрабатываемой Системы была проведена модернизация блока генетической алгоритмизации. Введен контур функционирования нечеткой логики с блоками прогнозирования на модельных объектах СИУА ИИП,

обработки результатов прогнозирования с дополнительной множественной фильтрацией после создания поколений (рис. 3). Под модельными объектами понимается эталонная копия актуального состояния системы и реальных корпоративных серверных решений и сервисов.

Для более качественного распознавания неблагоприятных сетевых воздействий и предотвращения возможных побочных эффектов от принятых решений система формирует аддитивный фоновый тестовый сетевой трафик для модельных объектов. Удостоверившись, что экземпляр решения уменьшает нагрузку на систему в целом и одновременно с этим не препятствует прохождению полезного трафика, фильтр системы может признать решение допустимым.

С использованием модельных объектов СИАУ ИИП осуществляет прогнозирование реакции системы/объектов, по обратной связи корректируется начальная выборка (новые поколения). Идентичная подстройка фильтра с использованием нечеткой логики позволяет выбирать из правильных решений рациональное, что приводит к снижению загрузки канала связи. Осуществляется нивелирование негативных воздействий от потенциально подозрительных возмущений различного уровня риска с обеспечением исправного обслуживания штатных воздействий.

Концепция генетической алгоритмизации заключается в организации эволюционного процесса и наследует идеи природы. Популяцией особей выступает конечное множество альтернативных решений. Хромосомы выражают составляющие действия в решении (стратегии реагирования) и являются упорядоченными последовательностями генов, описывающих параметры задачи. В качестве оценки приспособленности предлагается использовать стоимостную функцию

$$\omega_i(\Delta T) = \sum_{n\in[0,\,N-1]} |traffic(n) - \overline{traffic}| = N \cdot \overline{traffic} + \frac{}{2}, \quad (2)$$

n — отсчеты в рассматриваемом интервале времени ΔT; N — число измерений загрузки канала связи в данном интервале; $\overline{traffic}$ — среднее арифметическое значение загрузки канала за этот интервал времени; $traffic(n)$ — значения загрузки канала для каждого отсчета времени.

Правое слагаемое представляет собой интегральное выражение (площадь) всплесков трафика выше среднего арифметического значения за рассматриваемый период.

Для повышения быстродействия системы проводится распараллеливание анализа генерируемых решений СИАУ ИИП перенаправлением идентичных информационных потоков на модельные объекты, подключенные к альтернативному каналу связи. Для каждого из этих решений на соответствующем МО высчитывается функция приспособленности. Расчет условия остановки алгоритма выполняется в условиях приближенных рассуждений. Соответственно, здесь задействуется блок нечеткой логики. Для оценки эффективности решения используется функция приспособленности:

$$F_i = \frac{\omega(\Delta T_0) - \omega_i(\Delta T)}{\omega(\Delta T_0)} \cdot 100\,\% = \frac{\Delta\omega_i(\Delta T)}{\omega(\Delta T_0)} \cdot 100\,\%. \quad (3)$$

Она отображает процентное соотношение снижения значения стоимостной функции $\Delta\omega_i(\Delta T)$ к значению стоимостной функции в момент до принятия решения $\omega(\Delta T_0)$. Данный показатель рассчитывается для каждой изучаемой особи (хромосомы, экземпляра решения, стратегии реагирования) на модельных объектах.

Система анализирует текущие и статистические значения функций приспособленности (F_i) всей популяции особей. Вычисляя средние значения и среднеквадратичные отклонения (СКО) для их множеств, блок нечеткой логики может принять одно из следующих решений (процентные соотношения могут динамически изменяться):

1) если текущее среднее значение лучше статистического более

Рис. 3. Блок-схема модернизированного генетического алгоритма поиска рационального решения задачи управления трафиком вычислительной сети

чем на 7 %, то выбрать лучшую особь, применить к реальной системе, не останавливать работу генетического алгоритма (ГА);

2) если число итераций < 3, то не останавливать работу ГА;

3) если число итераций ⩾ 3, все решения хуже статистических, то остановить работу ГА;

4) если число итераций ⩾ 3, текущее среднее значение лучше статистического не более чем на 7 %, и СКО ⩽ 7 %, то выбрать лучшую особь, применить к реальной системе, остановить работу ГА;

5) если число итераций ⩾ 3, значение для лучшей особи превосходит статистическое не более чем на 7 %, и СКО ⩽ 40 %, то выбрать лучшую особь, применить к реальной системе, перезапустить работу ГА;

6) если число итераций ⩾ 3, значение для лучшей особи превосходит статистическое не более чем на 7 %, и СКО > 40 %, то выбрать лучшую особь, применить к реальной системе, перезапустить работу ГА с дополнительными параметрами фильтра.

С первого по шестой пункты динамически подстраиваются параметры фильтра. В случае идентификации крайне отрицательного решения, подтвержденного статистикой к различным типам воздействий, особь исключается из допустимой выборки начальной популяции. Временные интервалы исследования решений и условия выбора корректируются блоком нечеткой логики. В случае отключения информационных потоков, направленных на модельные объекты (например, источники прекратили взаимодействие), СИАУ ИИП перенаправляет очередную порцию клиентов на данный объект. Действие выполняется для обеспечения равномерного распределения нагрузки на линии связи, предоставляемые модельным объектам.

Система содержит звено аналитики, которое ведет статистику по объектам, классам и группам объектов. Разграничиваются воздействия, риски и решения. Процентное соотношение генетических рулеток адаптивно изменяется в зависимости от статистики звена аналитики. Однако для повышения эффективности работы генетической алгоритмизации элитарное доминирование пресекается контуром нечеткой логики.

2.3. Обработка воздействий различного уровня риска

Существующие системы управления информационными потоками и процессами (в том числе маршрутизаторы, межсетевые экраны и другие единицы управляемого сетевого оборудования) в общем случае работают по схеме, показанной на рис. 4.

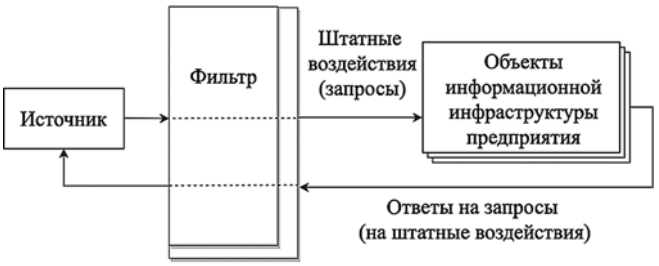

Рис. 4. Общая схема обработки внешних воздействий

Важно отметить, что легитимные запросы с применением технологий анонимизации нередко сразу блокируются существующими решениями. Не предоставляется доступ к объектам сетевой инфраструктуры источникам, обеспечивающим свою конфиденциальность.

Рассматриваемый метод интеллектуально-адаптивного управления информационной инфраструктурой предприятия вводит множественную фильтрацию, изменяет стандартную логику обработки воздействий в зависимости от их уровня риска (рис. 5, см. четвертую сторону обложки). Задействуются новые компоненты: блок прогнозирования с модельными объектами, блок фальсификации с имитированными объектами в изолированной среде, модули множественной фильтрации.

Данным комплексом выполняется идентификация и классификация внешних возмущений в зависимости от рисков негативных воздействий как на саму Систему, так и на объекты информационной инфраструктуры предприятия [9, 10]. Далее, в зависимости от типа воздействия и оценки потенциальных последствий, выявленных в результате анализа, информационные потоки перенаправляются от источников возмущений на блок прогнозирования либо блок фальсификации.

Первый блок задействуется в случае потенциальных подозрительных возмущений низкого риска. На нем проводится поиск рациональной стратегии реагирования через ранее описанный блок генетической алгоритмизации и нечеткой логики.

Второй блок подключается для обработки потенциальных подозрительных возмущений среднего и высокого риска. На нем проводится не только поиск рациональной стратегии реагирования через механизмы "информацион-

ных ловушек", но и автоматическая идентификация недостатков системы с декларированием и последующей нейтрализацией.

Результаты из блоков прогнозирования и фальсификации через обратную связь передаются системе управления с множественной фильтрацией, которая динамически перестраивается и самообучается таким образом. Затем выполняются управляющие воздействия на источники возмущений или их информационые потоки, нивелируются потенциальные риски и снижается загрузка каналов связи.

Описанный метод разрешает анонимным источникам получать доступ к ресурсам информационной инфраструктуры при отсутствии злоумышленных возмущений. Дополнительно реализована интеллектуальная поддержка принятия решений через блок прогнозирования и накопленную статистику. Если технический специалист хочет апробировать определенные действия или осуществить интеграцию новых модулей, то Система может предложить проведение итерационного исследования на модельных объектах с привнесением штатных тестовых сигналов и отслеживанием реакции. Детализированный отчет с оценкой рисков и рекомендациями будет предоставлен системному администратору.

Заключение

Был разработан новый метод интеллектуально-адаптивного управления информационной инфраструктурой предприятия, позволяющий обеспечить исправное и отказоустойчивое функционирование технических систем и объектов со снижением загрузки канала связи при разнообразных воздействиях различного уровня риска.

Автоматический поиск и применение рациональной стратегии реагирования на различные типы воздействий осуществляется путем их интеллектуальной обработки с прогнозированием реакции сервисов на изолированных модельных объектах. Для достижения данной цели применяется блок генетической алгоритмизации и нечеткой логики с самоорганизацией правил и модулей управления.

Минимизирован риск перехода информационных систем в режим недоступности, обеспечен высокий уровень безопасности информационной инфраструктуры предприятия без ущерба штатным информационным потокам, которые могли бы выполняться с применением технологий анонимизации.

Разработка, проектирование, программная реализация и исследование системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия будут представлены в следующей статье.

Список литературы

1. **Кудрявцев М. Е., Калугина О. Б.** Сигнатуры систем обнаружения вторжений: основы IDS сигнатур // Актуальные проблемы современной науки, техники и образования. 2019. Т. 10, № 1. С. 80—83.

2. **Трошина С. М., Штуллер Н. В.** Система обнаружения атак // Вестник Уральского финансово-юридического института. 2016. № 4 (6). С. 109—112.

3. **Sung-Ho L., Jun-Sang P., Sung-Ho Y., Myung-Sup K.** High performance payload signature-based Internet traffic classification system // Proceedings of the 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), Busan, South Korea. 2015. P. 491—494.

4. **Woo-Suk J., Jun-Sang P., Myung-Sup K., Jae-Hyun H.** Efficient payload signature structure for performance improvement of traffic identification // Proceedings of the 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), Busan, South Korea. 2015. P. 180—185.

5. **He L., Cuibo Y., Xuerong G.** Analysis of traffic model and self-similarity for QQ in 3G mobile networks // Proceedings of the International Conference on Advanced Intelligence and Awareness Internet (AIAI), Shenzhen, China. 2011. P. 131—135.

6. **Faizullin R. R., Yaushev S. T., Insarov A. Y.** Modeling and Self-Similarity Analysis of Non-Poissonian Traffic Represented by Multimodal Non-Typical Pascal and Rice Distributions // Proceedings of the International Conference on Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia. 2019. P. 1—4.

7. **Jieying H., Zhang J. Z.** Network traffic anomaly detection using weighted self-similarity based on EMD // Proceedings of the IEEE Southeastcon, Jacksonville, FL, USA. 2013. P. 1—5.

8. **Ye T., Dongqi H., Lishi L., Yu F.** A self-similar traffic generation model based on time // Proceedings of the 7th IEEE International Symposium on Microwave, Antenna, Propagation, and EMC Technologies (MAPE), Xi'an, China. 2017. P. 160—163.

9. **Французова Г. А., Гунько А. В., Басыня Е. А.** Самоорганизующаяся система управления трафиком вычислительной сети: метод противодействия сетевым угрозам // Программная инженерия. 2014. № 3. С. 16—20.

10. **Басыня Е. А.** Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия // Безопасность информационных технологий. 2018. Т. 25, № 4. С. 43—52.

E. A. Basinya, Ph. D., Professor[1], Director[2], e-mail: director@nii-ikt.ru,
[1]Novosibirsk State Technical University,
[2]Research Institute of Information and Communication Technologies, Novosibirsk, Russian Federation

Method of Intellectually-Adaptive Management of the Enterprise Information Infrastructure

The aim of this work was to develop a new method of intellectually adaptive management of the enterprise information infrastructure. It was necessary to ensure the serviceable and fault-tolerant functioning of technical systems and facilities with reducing communication channel load under various internal and external influences of a different risk level. The task was also to develop the concept of automatic search and apply a rational response strategy to various types of disturbances. A rational response strategy implied as a set of measures that would minimize the load on the communication channel in comparison with alternative solutions, without adversely affecting regular information flows and processes, as well as the level of security of the enterprise's information and communication sector. As a result, a new method of intelligent adaptive management of the enterprise information infrastructure is proposed. The choice of a rational response strategy to various types of influences is carried out by their intellectual processing with prediction of the response of services on isolated model objects. To achieve this goal, a block of genetic algorithmization and fuzzy logic is applied with self-organization of rules and control modules. The risk of information systems switching to unavailability mode is minimized, a high level of security of the enterprise information infrastructure is ensured. Complex traffic and information processes management at all levels of interaction achieve improving the reliability, fault tolerance and quality of technical systems.

Keywords: *system analysis, intelligent adaptive management, processing, network traffic, local information processes, abnormal impacts, information security, TCP/IP, threats, attacks*

DOI: 10.17587/it.26.185-191

References

1. **Kudryavcev M. E., Kalugina O. B.** Intrusion Detection Signatures: IDS Signature Basics, *Aktual'ny'e Problemy' Sovremennoj Nauki, Texniki i Obrazovaniya*, 2019, vol. 10, no. 1, pp. 80—83 (in Russian).

2. **Troshina S. M., Shtuller N. V.** Attack detection system, *Vestnik Ural'skogo finansovo-yuridicheskogo instituta*, 2016, no. 4 (6), pp. 109—112 (in Russian).

3. **Sung-Ho L., Jun-Sang P., Sung-Ho Y., Myung-Sup K.** High performance payload signature-based Internet traffic classification system, *Proceedings of the 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Busan, South Korea, 2015, pp. 491—494.

4. **Woo-Suk J., Jun-Sang P., Myung-Sup K., Jae-Hyun H.** Efficient payload signature structure for performance improvement of traffic identification, *Proceedings of the 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Busan, South Korea, 2015, pp. 180—185.

5. **He L., Cuibo Y., Xuerong G.** Analysis of traffic model and self-similarity for QQ in 3G mobile networks, *Proceedings of the International Conference on Advanced Intelligence and Awareness Internet (AIAI)*, Shenzhen, China, 2011, pp. 131—135.

6. **Faizullin R. R., Yaushev S. T., Insarov A. Y.** Modeling and Self-Similarity Analysis of Non-Poissonian Traffic Represented by Multimodal Non-Typical Pascal and Rice Distributions, *Proceedings of the International Conference on Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, Russia, 2019, pp. 1—4.

7. **Jieying H., Zhang J. Z.** Network traffic anomaly detection using weighted self-similarity based on EMD, *Proceedings of the IEEE Southeastcon*, Jacksonville, FL, USA, 2013, pp. 1—5.

8. **Ye T., Dongqi H., Lishi L., Yu F.** A self-similar traffic generation model based on time, *Proceedings of the 7th IEEE International Symposium on Microwave, Antenna, Propagation, and EMC Technologies (MAPE)*, Xi'an, China, 2017, pp. 160—163.

9. **Franczuzova G. A., Gunko A. V., Basinya E. A.** Self-organizing computer network traffic management system: a method to counteract network threats, *Programmnaya inzheneriya*, 2014, no. 3, pp. 16—20 (in Russian).

10. **Basinya E. A.** Distributed system of collecting, processing and analysis of security information events of the enterprise network infrastructure, *Bezopasnost' informacionny'x texnologij*, 2018, vol. 25, no. 4, pp. 43—52 (in Russian).

Рисунки к статье Е. А. Басыни

«МЕТОД ИНТЕЛЛЕКТУАЛЬНО-АДАПТИВНОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРОЙ ПРЕДПРИЯТИЯ»

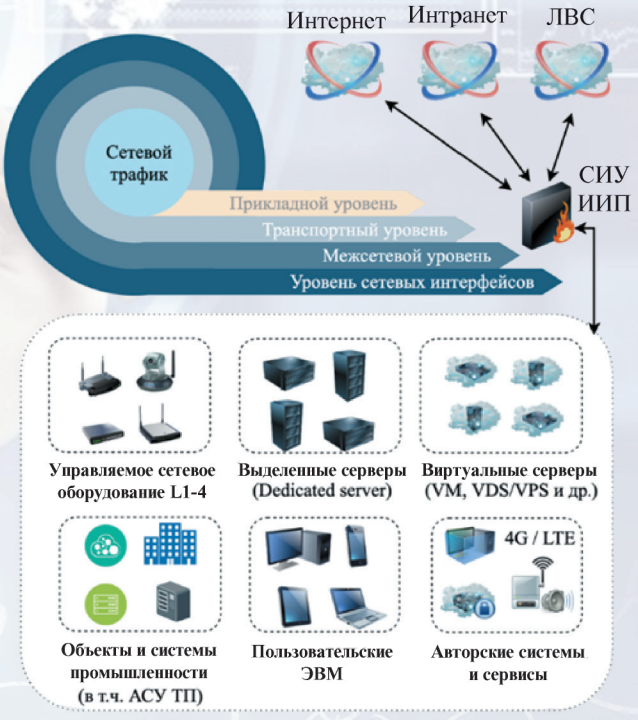

Рис. 1. Объекты управления СИУА ИИП

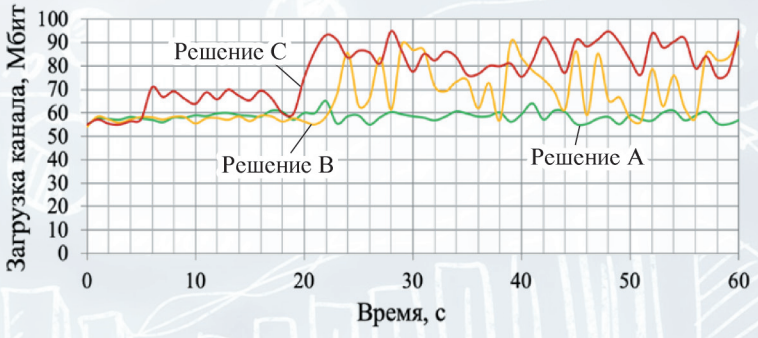

Рис. 2. Диаграмма загрузки канала связи при различных решениях по обработке трафика

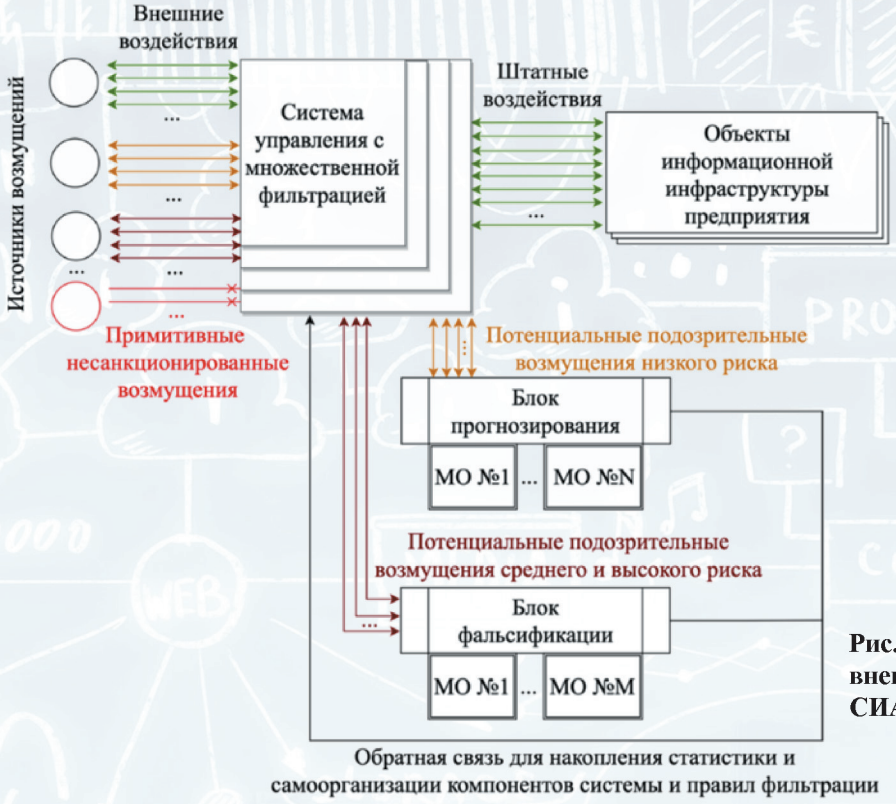

Рис. 5. Общая схема обработки внешних воздействий СИАУ ИИП

ISSN 1684-6400. Информационные технологии. 2020. Том 26. № 3. 129–192. Индекс: 72656 (Объединенный каталог «Пресса России»)

Рисунки к статье Е. А. Басыни

«МЕТОД ИНТЕЛЛЕКТУАЛЬНО-АДАПТИВНОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРОЙ ПРЕДПРИЯТИЯ»

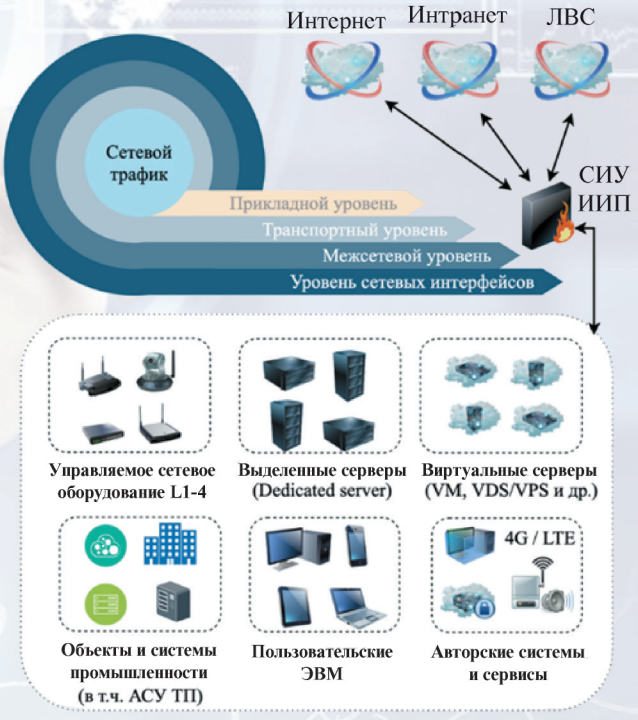

Рис. 1. Объекты управления СИУА ИИП

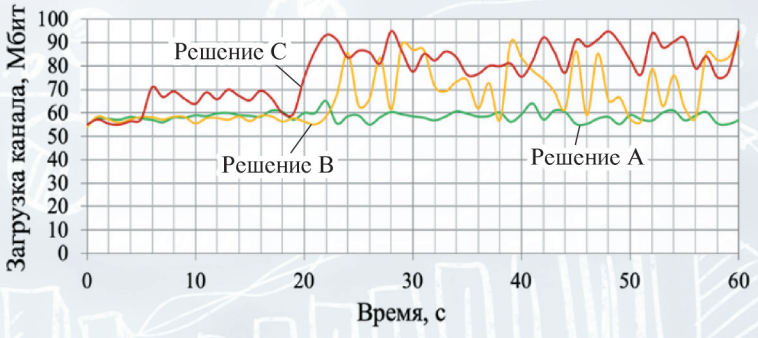

Рис. 2. Диаграмма загрузки канала связи при различных решениях по обработке трафика

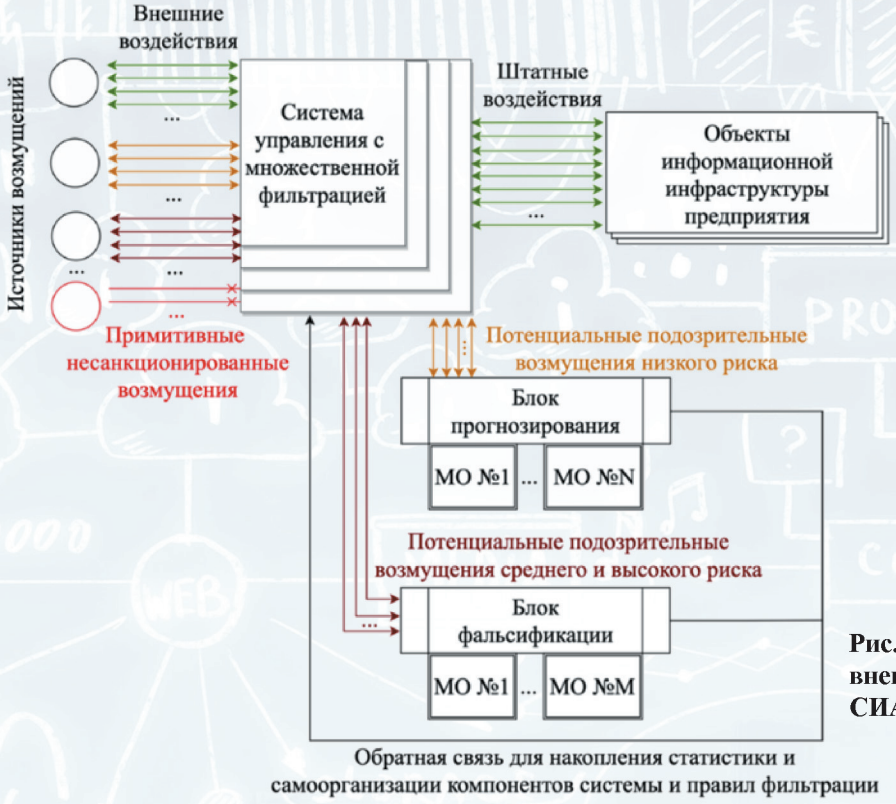

Рис. 5. Общая схема обработки внешних воздействий СИАУ ИИП

ISSN 1684-6400. Информационные технологии. 2020. Том 26. № 3. 129–192. Индекс: 72656 (Объединенный каталог «Пресса России»)