УДК 004.89 DOI: 10.17587/it.26.283-289

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

Система интеллектуально-адаптивного управления информационной инфраструктурой предприятия

Предлагается новая система интеллектуально-адаптивного управления информационной инфраструктурой предприятия, функционирующая на основе ранее представленного [10] одноименного метода. Ее назначение заключается в осуществлении системного анализа, обработки информации и управления сложными системами информационной инфраструктуры предприятия в целях повышения их эффективности и отказоустойчивости даже в нештатных режимах работы. Предоставляется возможность противодействия несанкционированным исследованиям технических объектов и систем с исключением возможности компрометации управляющих воздействий.

Ключевые слова: *интеллектуально-адаптивное управление, нештатные воздействия, самообучение, сетевой трафик, локальные информационные процессы, TCP/IP, информационная безопасность, маскировка, профилирование источников, ловушки*

Введение

Динамическое развитие информационно-коммуникационных технологий является катализатором роста мировой экономики. Вопросы информационной безопасности приобретают первостепенное значение для любого хозяйствующего субъекта. Уровень защищенности информации любой компании является следствием эффективности подходов к системному анализу, управлению и обработке информации.

Значительный вклад в разработку методов управления потоками и процессами информационной инфраструктуры предприятия в контексте обеспечения надежного и отказоустойчивого функционирования внесли Y. Lan, Y. Sun, S. Liu, Z. Ma, L. Nie, C. Xin, L. Juhao и др. [1—3]. Однако данные исследования не принимают в расчет незадекларированные воздействия, в том числе инсайдерские угрозы.

Исследованиями в области теории управления информационными потоками на основе идентификации аномальной активности занимаются K. Vengatesan, K. Abhishek, N. Radhakrishana, K. Verma, Y. Qing, G. Xiaowei, Y. Gao и др. [4—6]. Другое интересное направление заключается в построении и работе с математическими моделями сетевого трафика и представлено в работах А. В. Черниговского, М. В. Кривова, А. П. Буслаева, Д. А. Кучелева, М. В. Яшина [7—9].

К сожалению, данные подходы не дают однозначного результата в реальных сетевых инфраструктурах, где функционируют различные криптоустойчивые алгоритмы и протоколы шифрования, технологии виртуальных защищенных каналов связи.

Соответственно возрастает актуальность разработки проблемно-ориентированных систем управления информационными потоками и процессами, позволяющих в автоматическом режиме осуществлять противодействие несанкционированным воздействиям, в том числе исследованию технических объектов и систем.

1. Цель работы и постановка задач

Целью данной работы являлась разработка системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия. Назначением системы является проведение системного анализа, обработки информации и управления сложными систе-

мами информационной инфраструктуры предприятия в целях повышения их эффективности, надежности и отказоустойчивости даже в нештатных режимах работы.

Ставилась задача автоматического противодействия несанкционированным внутренним и внешним исследованиям технических объектов и систем. Следовало исключить возможность первичного сбора информации о компонентах информационной инфраструктуры предприятия злоумышленником, использующим инструменты активного и пассивного анализа информационных систем и вычислительных сетей.

Требовалось создать возможность разграничения хакеров с осуществлением их дезинформации по разным сценариям. Было необходимо расширить функции самообучения системы с учетом анализа вредоносных действий подозрительных субъектов взаимодействия.

Было необходимо исключить даже потенциальную вероятность компрометации управляющих воздействий.

2. Предлагаемое решение

Система интеллектуально-адаптивного управления информационной инфраструктурой предприятия (далее Система или СИАУ ИИП) функционирует на основе ранее представленного одноименного метода [10]. Рассмотрим ее работу поэтапно.

В первую очередь выполняется сбор, обработка и системный анализ информационных потоков, процессов и ресурсов всех объектов корпоративной инфраструктуры предприятия. Достигается данная цель посредством использования инструментов активного и пассивного сетевого анализа трафика и информационных ресурсов, интеграции с модифицированным блокчейн-хранилищем и системой управления доверием к регистрируемой информации, анализом информационных процессов через взаимодействие с авторскими клиентскими модулями на хостах и управляемом сетевом оборудовании.

Следующие программные продукты используются как модули системы (каждый из них представляет собой объект интеллектуальной собственности: получены свидетельства о государственной регистрации программы для ЭВМ):

- автоматизированная система сетевого и системного администрирования операционных систем семейства Windows и Linux. Расширяет функционал Help и Service Desk систем обработкой инцидентов в атематическом режиме;
- распределенная система сбора, обработки и анализа событий информационной безопасности информационной инфраструктуры предприятия. Позволяет однозначно идентифицировать сложные локальные инциденты с последующим автоматическим исправлением ошибок на основе базы знаний. Самообучение реализовано оригинальным сигнатурным, корреляционным и статистическим подходом к итерационному тестированию и имитации известных сетевых и локальных воздействий с отслеживанием реакции операционных систем и приложений в изолированной среде [11];
- система обнаружения и предотвращения вторжений и фальсификации реестра событий на основе децентрализованного подхода. Расширяет функционал IDS/IPS и SIEM. Позволяет повысить отказоустойчивость и надежность функционирования информационной инфраструктуры предприятия даже в случае технических сбоев в работе отдельных объектов и систем. Исключает ошибки идентификации инцидентов/технических проблем за счет формирования объективного и информативного децентрализованного реестра событий на основе модифицированного блокчейн-хранилища с оригинальной системой управления доверием к регистрируемым событиям;
- система самоорганизующегося виртуального защищенного канала связи на основе стохастического многослойного шифрования и оверлейных технологий. Позволяет повысить надежность и отказоустойчивость сетевого взаимодействия хостов с исключением глобальной наблюдаемости и анализа коммуникаций. Нивелирует риск потенциальной эксплуатации даже неизвестных уязвимостей и ошибок используемых технологий. Применяется авторская технология маскировки трафика с автономным составлением секретной последовательности действий на стороне клиента и сервера для последующего удаленного доступа [12];
- комплексное обеспечение управляемого сетевого оборудования ARK-Gateway. Представляет собой прошивки коммутаторов, маршрутизаторов, шлюзов и другого управляемого сетевого оборудования, имеющих возможность стекирования и объединения в единую экосистему;

- система интеллектуально-адаптивного управления трафиком вычислительной сети. Позволяет комплексно анализировать сетевой трафик на всех уровнях стека протоколов TCP/IP с возможностью идентификации новых типов возмущений и выработкой оптимальной стратегии их обработки;
- система автоматического управления информационными потоками корпоративных вычислительных сетей. Позволяет обрабатывать метаинформацию сетевого трафика и локальных файлов, осуществлять управление информационными потоками на ее основе;
- система автоматического противодействия инструментам несанкционированного активного и пассивного анализа информационных систем и вычислительных сетей. Позволяет использовать инструменты ловушек, маскировки и фальсификации различных операционных систем и функционирующих на них сервисов и служб;
- комплексная система управления сетевой информационной безопасностью предприятия. Сочетает функционал систем защиты на всех уровнях стека протоколов TCP/IP с полноценным покрытием информационной инфраструктуры предприятия и проведением корреляционного анализа инцидентов;
- система мониторинга работы пользователей персональных компьютеров. Осуществляет учет рабочего времени пользователя и всех его локальных и сетевых действий в рамках правового поля, определенного законодательством РФ;
- система интеллектуального контроля и управления доступом к информационным ресурсам персонального компьютера. Пресекается несанкционированный доступ к данным даже при разблокированной операционной системе. Задействуются алгоритмы профилирования доступа средствами BIOS/UEFI (от проверки целостности конфигурации аппаратно-программной части до парольной защиты), модифицированная технология инкапсулированного шифрования с сокрытием основной операционной системы и фальсификации ОС-ловушки. Применяются методики мониторинга подключаемых сетей и оборудования, наличия связанных устройств в зоне видимости. Задействуется поведенческий анализ действий пользователя и семантический анализ посещаемых Интернет-ресурсов в сочетании с технологией глубокого анализа содержимого дейтаграмм, а также методы анализа биометрических данных (клавиатурного почерка, голоса, лица).

Блок-схема общего принципа функционирования Системы представлена на рис. 1, который отражает фоновые процессы в штатном режиме работы, выполняемые параллельно.

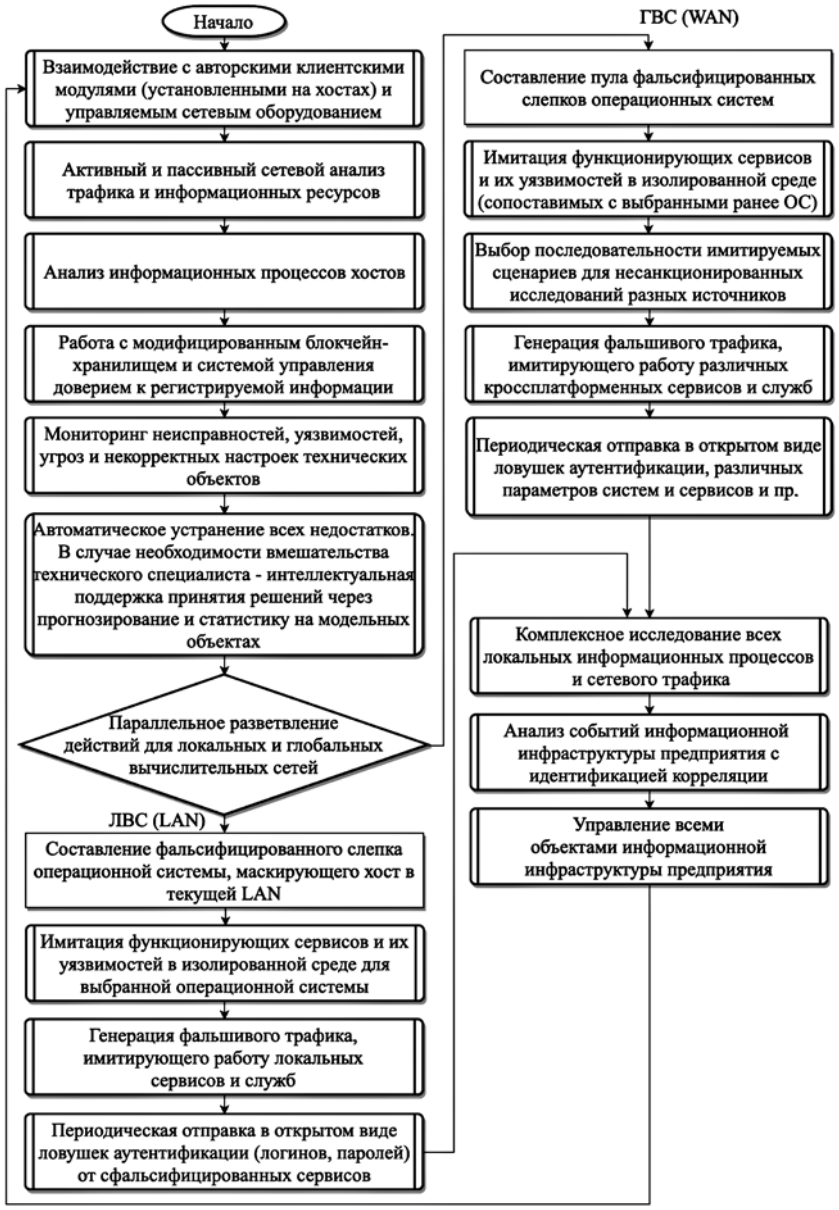

Рис. 1. Блок-схема общего принципа функционирования СИАУ ИИП

СИАУ ИИП осуществляет непрерывный мониторинг неисправностей, уязвимостей, угроз и некорректных настроек технических объектов с последующим их устранением в автоматическом режиме. В случае необходимости вмешательства технического специалиста Система предоставляет интеллектуальную поддержку принятия решений, описанную ранее.

В целях упреждающего воздействия на негативные последствия подозрительных возмущений различного уровня риска, в том числе несанкционированного исследования объектов, Система применяет широкий спектр методов фальсификации информации об информационной инфраструктуре и ее объектах: формируются ложные слепки операционных систем и сервисов с различными уязвимостями, выполняется генерация фальшивого трафика в целях имитации функционирования сервисов и служб, осуществляется периодическая отправка в открытом виде ловушек аутентификации, различных параметров сфальсифицированных системных сервисов.

Важно отметить, что СИАУ ИИП действует параллельно в сегменте локальных (ЛВС) и глобальных вычислительных сетей (ГВС) с применением соответствующей специфики.

Цель мероприятий в локальном сегменте — корректная маскировка Системы в рабочей области узлов с последующей идентификацией инсайдеров, злоумышленников из числа доверенных лиц.

Установка в глобальном сетевом сегменте нацелена на идентификацию, профилирование и обработку подозрительных воздействий с пресечением потенциальной возможности сбора информации об информационной инфраструктуре. В отличие от стратегии в ЛВС задействуется генерация широкого спектра обманных элементов с последующей дезинформацией источника возмущений даже в случае маскировки запросов средствами анонимизации.

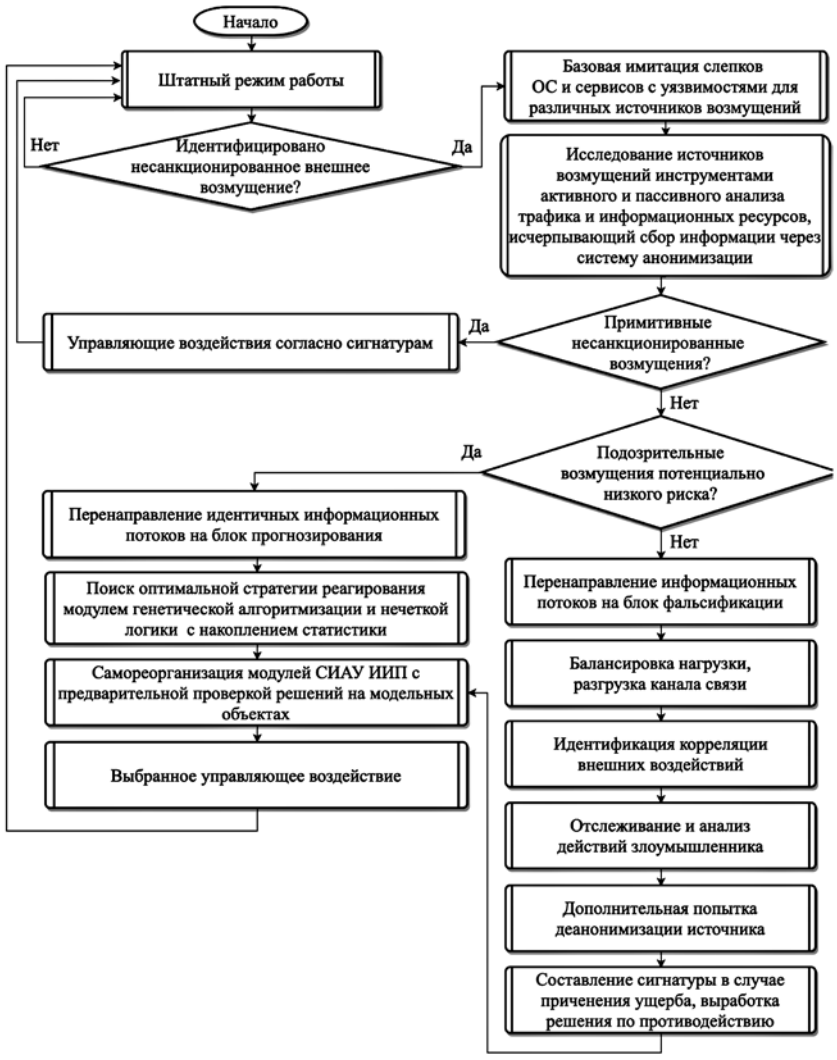

Рис. 2. Блок-схема обработки несанкционированных внешних возмущений СИАУ ИИП

Результатом описанных действий является пресечение несанкционированного исследования узлов и сетей, осуществление объективного мониторинга и эффективного комплексного управления объектами информационной инфраструктуры предприятия посредством выбора оптимальных стратегий реагирования.

Фоновые процессы Системы в случае идентификации несанкционированных внешних возмущений представлены на рис. 2.

Проводится классификация уровня риска. Для всех категорий воздействий осуществляется базовая имитация слепков операционной системы и сервисов с уязвимостями. Все источники возмущений исследуются средствами активного и пассивного анализа трафика и информационных ресурсов, выполняется исчерпывающий сбор информации через системы анонимизации (оверлейные технологии и сети, VPN-сервисы и прочие средства).

Примитивные нештатные возмущения обрабатываются согласно сигнатурам. Подозрительные воз-

действия потенциально низкого риска могут включать легитимный сигнал. Соответственно, осуществляется перенаправление идентичных информационных потоков на блок прогнозирования. Далее выполняется поиск оптимальной стратегии реагирования на модельных объектах с использованием ранее описанного модуля генетической алгоритмизации и нечеткой логики. Система накапливает и анализирует статистику с дополнительной проверкой выработанных действий на модельных объектах. При необходимости осуществляется реконфигурация правил и модулей фильтрации с самореогранизацией компонентов Системы. Затем осуществляется управляющее воздействие, Система переходит в штатный режим работы после успешной оптимизации загрузки канала связи.

В случае идентификации подозрительных возмущений среднего и высокого рисков выполняется перенаправление информационных потоков на блок фальсификации, в рамках которого подготовлены виртуальные машины с различными операционными системами (как пользовательскими, так и серверными версиями ОС семейства Windows, Linux, Mac OS) и функционирующими на них сервисами. Данные объекты изолированы от рабочей информационной инфраструктуры многоуровневой инкапсулированной виртуализацией и сегментацией виртуального сетевого трафика.

Перенаправление информационных потоков на требуемые объекты фальсификации осуществляется в соответствии с ранее имитированными слепками ОС и сервисов с уязвимостями для конкретных источников. Важно отметить, что даже в случае осуществления внешних воздействий через сервисы анонимизации Система разграничивает источники с высоким уровнем достоверности и фальсифицирует нужный объект, не вызывая подозрений у сторонних субъектов взаимодействия.

Проводятся отслеживание и комплексный анализ действий злоумышленника клиентским программным обеспечением, интегрированным в объект фальсификации. При условии нарушения штатного режима работы последнего Система автоматически создает сигнатуру сбоя и генерирует комплекс мер, устраняющих потенциальную возможность повторения данной проблемы с исключением из выборки решений с данной уязвимостью. Параллельно осуществляется идентификация корреляций внешних воздействий с балансировкой нагрузки и разгрузкой канала связи. Используются механизмы "информационных ловушек": от имитации состояния зависания до скрытого перенаправления, что помогает установить круг соучастников и расширить "черные" списки.

В автоматическом режиме реализуется дополнительная попытка деаномизации источника не только инструментами активного и пассивного анализа трафика и информационных ресурсов, но и различными скриптами в смоделированных веб-ресурсах, вредоносными замаскированными исполняемыми файлами, оставленными на объекте фальсификации как дезинформация с выполнением кода, приводящая к исчерпывающему сбору информации об источнике.

Заключительным этапом выступает самореогранизация модулей СИАУ ИИП с предварительной проверкой выработанных решений на модельных объектах с аддитивным фоновым тестовым сетевым трафиком. После проведения управляющего воздействия и нейтрализации проблемных возмущений система переходит в штатный режим работы.

Таким образом, СИАУ ИИП динамически самообучается и самореорганизуется, идентифицируя и обрабатывая без риска даже ранее неизвестные типы воздействий.

Важно отметить, что предлагаемая система предоставляет возможность централизованного конфигурирования и мониторинга всех объектов через веб-интерфейс панели администрирования (включая все сетевое оборудование), а также выступает единым центром автоматического управления всей инфраструктуры предприятия, не лишая узлы самостоятельности в выполнении их целевых функций и обработке примитивных нештатных воздействий.

Стоит рассмотреть простой пример. В случае технического сбоя сетевого адаптера электронно-вычислительного устройства может появиться шум в канале связи, который не может однозначно идентифицировать коммутатор. Система предпринимает попытки через клиентский модуль проблемного устройства программно устранить неполадку в автоматическом режиме.

Если проблема является аппаратной, то техническому специалисту поддержки отправляется уведомление с отчетом и рекомендациями заменить заменить/отремонтировать сетевой адаптер. Информирование осуществляется через электронную почту и push-уведомления мобильного приложения. Параллельно из центра управления коммутатору поступает указание с проведением действий по фильтрации трафика с блокировкой потоков по соответствующему

MAC-адресу поврежденного адаптера во избежание негативных последствий в сетевом сегменте.

Подобный централизованный подход к управлению является гибким, функциональным и надежным. Однако не исключена вероятность компрометации управляющих воздействий. В целях нивелирования подобных рисков был разработан оригинальный алгоритм дополнительной проверки подлинности и правомерности не только субъекта взаимодействия, но и его действий. Для этого в сетевую инфраструктуру интегрирован авторский децентрализованный реестр событий на основе модифицированного блокчейн-хранилища с системой управления доверием к регистрируемой информации.

Когда объект критический информационной инфраструктуры получает от головной системы управляющее воздействие, к нему прилагается список событий, повлекших за собой данное решение. Хост-исполнитель обращается к децентрализованному реестру событий и проверяет факт их существования, а также рейтинг доверия к этим данным. Далее сопоставляет их с общедоступной базой знаний реагирования. После успешной проверки выполняет требуемые действия.

Важно отметить, что сетевое взаимодействие хостов осуществляется безопасно на базе самоорганизующегося виртуального защищенного канала связи на основе стохастического многослойного шифрования и оверлейных технологий.

Достигается проверка подлинности и правомерности управляющих воздействий. Дополнительным интересным авторским решением является децентрализованное распределение трафика с многослойным шифрованием внутри корпоративной сети при подозрительной активности межсетевых хостов на основе рейтинга доверия к ним.

Таким образом, последовательно решены все ранее поставленные задачи.

Заключение

Была разработана система интеллектуально-адаптивного управления информационной инфраструктурой предприятия, целевым назначением которой выступает проведение системного анализа, обработки информации и управления сложными системами информационной инфраструктуры предприятия в целях повышения их эффективности, надежности и отказоустойчивости даже в нештатных режимах работы.

Научная новизна предлагаемого решения заключается в интеллектуальной обработке нештатных внутренних и внешних возмущений на изолированных модельных объектах посредством применения генетической алгоритмизации и нечеткой логики. Адаптивное управление информационными потоками и процессами достигается прогнозированием реакции сервисов/хостов на модельных объектах с самоорганизацией правил и модулей системы через обратную связь. Другим аспектом научной новизны выступает централизованное управление критическими объектами информационной инфраструктуры с проверкой хостами-исполнителями аргументации требуемых от них действий через объективный и информативный децентрализованный реестр событий на основе модифицированного блокчейн-хранилища с системой управления доверием к регистрируемой информации. Оригинальным функционалом выступает интеллектуальная поддержка при принятии управленческих решений в технических системах для широкого спектра специалистов: от инженеров информационной безопасности до системных и сетевых администраторов.

Проектирование, программная реализация и исследование системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия будут представлены в следующих работах.

Список литературы

1. **Lan Y., Sun Y., Liu S., Ma Z.** A real-time network traffic analysis and QoS management platform // Proceedings of the IEEE 9th International Conference on Communication Software and Networks (ICCSN), Guangzhou, China. 2017. P. 266—270.

2. **Nie L.** Traffic matrix estimation approach based on partial direct measurements in large-scale IP backbone networks // Proceedings of the IEEE 5th International Conference on Electronics Information and Emergency Communication, Beijing, China. 2015. P. 178—181.

3. **Xin C., Juhao L., Paikun Z., Ruizhi T.** and oth. Fragmentation-aware routing and spectrum allocation scheme based on distribution of traffic bandwidth in elastic optical networks // IEEE/OSA Journal of Optical Communications and Networking. 2015. Vol. 7, Iss. 11. P. 1064—1074.

4. **Vengatesan K., Abhishek K., Radhakrishana N., Verma K.** Anomaly Based Novel Intrusion Detection System For Network Traffic Reduction // Proceedings of the 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Palladam, India. 2018. P. 688—690.

5. **Qing Y., Xiaowei G.** Network Traffic Anomaly Detection Based on Dynamic Programming // Proceedings of the International Conference on Computing Intelligence and Information System (CIIS), Nanjing, China. 2017. P. 62—65.

6. **Gao Y.** Network Anomaly Traffic Detection Method Based on Support Vector Machine // Proceedings of the International Conference on Smart City and Systems Engineering (ICSCSE), Hunan, China. 2016. P. 3—6.

7. **Черниговский А. В., Кривов М. В.** Подбор математической модели сетевого трафика // Современные технологии и научно-технический прогресс. 2018. Т. 1. С. 90—91.

8. **Буслаев А. П., Кучелев Д. А., Яшина М. В.** Динамические системы и математические модели трафика информации // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12, № 3. С. 22—38.

9. **Черниговский А. В., Кривов М. В.** Основные модели сетевого трафика // Вестник Ангарского государственного технического университета. 2017. № 11. С. 137—143.

10. **Басыня Е. А.** Метод интеллектуально-адаптивного управления информационной инфраструктурой предприятия // Информационные технологии. 2020. Т. 26, № 3. С. 185—191.

11. **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.

12. **Басыня Е. А.** Система самоорганизующегося виртуального защищенного канала связи // Защита информации. Инсайд. 2018. № 5 (83). С. 10—15.

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

System for Intellectually Adaptive Management of the Enterprise Information Infrastructure

The aim of this work was to develop a system for intellectually adaptive management of the enterprise information infrastructure. The purpose of the System was to perform a system analysis, information processing and management of complex systems of an enterprise's information infrastructure in order to increase their efficiency, reliability and fault tolerance even in abnormal operating modes. As a result, a system was developed that operates on the basis of the previously presented eponymous method and addresses the preset tasks. The possibility of automatic counteraction to unauthorized internal and external research of technical objects and systems has been implemented. A mechanism for distinguishing between hackers and their misinformation according to different scenarios has been carried out. The self-learning functions of the system are expanded taking into account the analysis of the malicious actions of suspicious interaction subjects. The possibility of the initial collection of information about the components of the information infrastructure of the enterprise by an attacker using tools of active and passive analysis of information systems and computer networks is excluded. The scientific novelty of the proposed solution lies in the intellectual processing of abnormal internal and external disturbances on isolated model objects through the use of genetic algorithmization and fuzzy logic. Adaptive management of information flows and processes is achieved by predicting the response of services / hosts on model objects with the self-organization of rules and system modules through feedback.

Keywords: *intelligent and adaptive management, abnormal impacts, self-training, network traffic, local information processes, TCP/IP, information security, masking, source profiling, traps*

DOI: 10.17587/it.26.283-289

References

1. **Lan Y., Sun Y., Liu S., Ma Z.** A real-time network traffic analysis and QoS management platform, *Proceedings of the IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, Guangzhou, China, 2017, pp. 266—270.

2. **Nie L.** Traffic matrix estimation approach based on partial direct measurements in large-scale IP backbone networks, *Proceedings of the IEEE 5th International Conference on Electronics Information and Emergency Communication*, Beijing, China, 2015, pp. 178—181.

3. **Xin C., Juhao L., Paikun Z., Ruizhi T.** and oth. Fragmentation-aware routing and spectrum allocation scheme based on distribution of traffic bandwidth in elastic optical networks, *IEEE/OSA Journal of Optical Communications and Networking*, 2015, vol.7, iss.11, pp. 1064—1074.

4. **Vengatesan K., Abhishek K., Radhakrishana N., Verma K.** Anomaly Based Novel Intrusion Detection System For Network Traffic Reduction, *Proceedings of the 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Palladam, India, 2018, pp. 688—690.

5. **Qing Y., Xiaowei G.** Network Traffic Anomaly Detection Based on Dynamic Programming, *Proceedings of the International Conference on Computing Intelligence and Information System (CIIS)*, Nanjing, China, 2017, pp. 62—65.

6. **Gao Y.** Network Anomaly Traffic Detection Method Based on Support Vector Machine, *Proceedings of the International Conference on Smart City and Systems Engineering (ICSCSE)*, Hunan, China, 2016, pp. 3—6.

7. **Chernigovskij A. V., Krivov M. V.** The selection of a mathematical model of network traffic, *Sovremenny'E Texnologii i Nauchno-Texnicheskij Progress*, 2018, vol. 1, pp. 90—91 (in Russian).

8. **Buslaev A. P., Kuchelev D. A., Yashina M. V.** Dynamic systems and mathematical models of information traffic, *T-Comm: Telekommunikacii i Transport*, 2018, vol. 12, no. 3, pp. 22—38 (in Russian).

9. **Chernigovskij A. V., Krivov M. V.** The main models of network traffic, *Vestnik Angarskogo Gosudarstvennogo Texnicheskogo Universiteta*, 2017, no. 11, pp. 137—143 (in Russian).

10. **Basinya E. A.** The method of intellectually-adaptive management of the enterprise information infrastructure, *Informacionnye Tehnologii,* 2020, vol. 26, no. 3, pp. 185—191 (in Russian).

11. **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).

12. **Basinya E. A.** The System of Self-Organizing Virtual Secure Communication Channel, *Zashhita Informacii. Insajd*, 2018, no. 5 (83), pp. 10—15 (in Russian).