УДК 004.021

Д. В. Мишин, М. Ю. Монахов

ОБ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ИНФРАСТРУКТУРЫ АСУП

Предлагаются средства автоматизации процессов администрирования информационно-технологической инфраструктуры автоматизированной системы управления предприятием, используемых в поисковых и восстановительных работах при деструктивных воздействиях на ее компоненты.

Ключевые слова: *администрирование корпоративной сети передачи данных, автоматизированная система администрирования, администратор.*

Введение. Под ИТ-инфраструктурой автоматизированной системы управления предприятием (АСУП) будем понимать композицию следующих компонентов: вычислительная техника (компьютеры пользователей, корпоративные серверы и т.д.) и периферийное оборудование (сетевые принтеры, факсы и т.д.), телекоммуникационное оборудование (коммутаторы, маршрутизаторы, аппаратные межсетевые экраны и т.д.) и кабельные системы, системное (операционная система, утилиты) и прикладное программное обеспечение (ПО), объединенных понятием „корпоративная сеть передачи данных“ (КСПД).

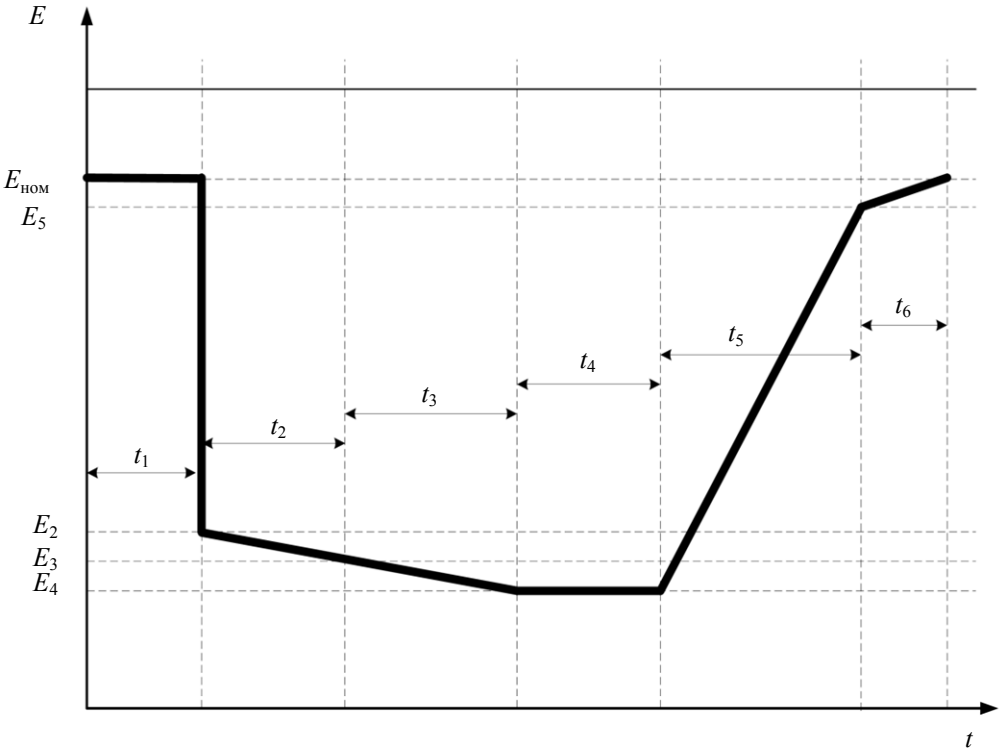
Понятие „функциональная устойчивость“ [1] КСПД включает свойства надежности, живучести и безопасности, отражает способность сохранения и/или восстановления возможности выполнения возложенных на КСПД функций, при деструктивных воздействиях (поражающих факторов, ПФ) на ее компоненты. Одной из характеристик функциональной устойчивости КСПД является время восстановления работоспособности. Все этапы технологического цикла восстановления работоспособности [2] КСПД современных предприятий реализуются, как правило, в рамках процессов администрирования [3] — операционного управления, направленного на обеспечение надежного, стабильного и безопасного функционирования КСПД на протяжении всего ее жизненного цикла сети с качеством, требуемым АСУП. Реализация процессов администрирования КСПД осуществляется службой технической поддержки (СТП) предприятия (в составе ИТ-отдела), основным звеном которой являются администраторы КСПД (будем называть их так вне зависимости от квалификации и функциональной специализации).

Централизованный оперативный контроль, управление и координация процессов администрирования (диспетчеризация) осуществляются специальным сотрудником СТП (лицом, принимающим решения, ЛПР) — диспетчером, аналитиком, главным администратором или начальником СТП — на основании личного опыта, имеющейся оперативной информации о текущих характеристиках КСПД, нормативной документации и информации об имеющихся ресурсах.

Настоящая работа посвящена исследованию методов и средств автоматизации процессов администрирования КСПД интегрированных АСУ промышленных предприятий, позволяющих снижать время восстановления работоспособности элементов КСПД и как следствие — обеспечивать ее функциональную устойчивость.

Технологический цикл восстановления КСПД. Рассмотрим технологический цикл устранения инцидента КСПД в рамках процессов администрирования при однократном воздействии ПФ на типовую КСПД (см. рисунок).

Этап 1. Штатный режим. КСПД функционирует в штатном режиме с требуемой (номинальной) эффективностью $E_{\text{ном}}$. Данный этап сопровождается итеративным контролем значений параметров элементов сети и процедурами периодического обслуживания (не приводящими к снижению $E_{\text{ном}}$), осуществляемыми администраторами с использованием специальных средств — сканеров сети, программ инвентаризации аппаратных компонентов и программного обеспечения узлов КСПД и т.д. Этап завершается при возникновении (мгновенном) инцидента (воздействии ПФ). При этом эффективность АСУП может достигнуть нуля (выход из строя системы) или некоторого значения E_2, в зависимости от типа и мощности ПФ ($0 \le E_2 < E_{\text{ном}}$).



Этап 2. Обнаружение инцидента. На этом этапе происходит обнаружение воздействия ПФ, поиск отказавших элементов КСПД, сбор информации об инциденте и его последствиях, т.е. формально — производится поиск отказавших элементов КСПД и их отклонения от заданных (эталонных) значений. В течение этапа эффективность АСУП может продолжать снижаться вследствие вторичных отказов ($0 \le E_3 \le E_2$).

Автоматизация этапа обнаружения инцидента предусматривает несколько направлений:

— создание специальной базы профилей, содержащих значения эталонных состояний элементов КСПД, и программного инструментария для получения этих значений;

— внедрение системы *Service Desk*, позволяющей пользователям оперативно информировать СТП о возникающих инцидентах;

— внедрение интеллектуальных средств анализа средств защиты информации КСПД по журналам событий — систем обнаружения вторжений, систем межсетевого экранирования, антивирусных комплексов и т.д.

Этап 3. Идентификация инцидента. Производится анализ собранной информации об инциденте (идентификация инцидента и его классификация), анализ возможных решений инцидента. Выбирается подходящее (возможно, оперативное (временное), обеспечивающее частичное повышение эффективности) решение инцидента. В течение этапа эффективность КСПД может продолжать снижаться ($0 \le E_4 \le E_3$).

Задача автоматизации этапа идентификации инцидента может решаться внедрением специальной системы поддержки принятия решения (СППР), содержащей идентификационные

признаки (базу знаний, БЗ) инцидентов КСПД, статистические сведения о динамике их возникновения, систему прогнозирования и т.д. В случае ошибки/отказа автоматизированной идентификации (неизвестный инцидент) предусматривается пополнение БЗ СППР новыми сигнатурами по результатам исследования инцидента специальной экспертной группой.

Этап 4. Формирование программы решения. Происходит выработка последовательности функций администрирования (ФА) на основе выбранного варианта решения инцидента — программы решения. ФА предлагается рассматривать как элементарные управляющие воздействия, предназначенные для получения или изменения состояний элементов КСПД — настройки конфигурационного параметра программы, замены аппаратного модуля автоматизированного рабочего места, добавления учетной записи, смены пароля пользователя, установки ПО и т.д. Из множества альтернатив выбирается „подходящий“ администратор для выполнения первой/очередной ФА. Основной участник этапа — ЛПР, целевой задачей которого является выработка наиболее эффективной (в конкретной оперативной обстановке) стратегии администрирования.

Программу решения предлагается формировать по результатам имитационного моделирования процесса функционирования СТП [4, 5]. Формальная модель администратора КСПД и алгоритмов формирования программы (выбора исполнителя ФА) представлена в работах [6, 7].

Этап 5. Исполнение ФА администратором — замена или ремонт вышедших из строя элементов, реконфигурация оборудования и программного обеспечения. Формируется отчет о выполнении. В случае отказа ФА происходит возврат к этапу 3, иначе — к 4.

Автоматизация данного этапа возможна средствами документированного обеспечения администрирования (ДОА), позволяющими администратору использовать данные информационно-технической (паспорта элементов КСПД), информационно-графической (карты и диаграммы различных уровней и детализации КСПД) и организационно-правовой (регламенты обслуживания, инструкции, положения, журналы) документации [8]. Кроме того, данный этап предусматривает создание системы регистрации в журнале деятельности администраторов — их производительности, надежности выполнения ФА, трудозатрат и т.д.

Этап 6. Завершение инцидента. Производится контроль значений параметров КСПД. Освобождаются ресурсы администрирования. По завершении этапа переходим к этапу 1, реализуя цикл процесса восстановления КСПД. На данном этапе эффективность сети должна достигнуть значения $E_{\text{ном}}$.

Восстанавливаемость КСПД определяется временем обработки ее элементов и может выражаться через сумму следующих показателей (см. рисунок): время обнаружения инцидента — t_2; время идентификации инцидента — t_3; время формирования программы решения — t_4; время выполнения программы (сумма по времени всех ФА) — t_5; время завершения инцидента — t_6. Предложенные решения по автоматизации позволяют уменьшить время реализации рассматриваемого цикла.

Особенности и рекомендации по внедрению

1. Этап 2, на наш взгляд, самый сложный. Авторы неоднократно сталкивались с такой ситуацией, когда показатели функциональных элементов „в норме“, система обнаружения вторжений с сетевым экраном не отражает подозрительной активности, а производительность КСПД падает. В таких случаях рекомендуется выделить определенное время на поиск источника инцидента (самым квалифицированным администратором), после чего (случай необнаружения) требуется делать „начальную установку“ (перезагрузку) всей КСПД.

2. В современных АСУП часто используется уникальное ПО, устанавливаемое и обслуживаемое сторонними организациями. В случае возникновения инцидента, связанного с данными элементами, приходится приглашать стороннего специалиста, т.е. увеличивается t_3, t_4, t_5. Частично преодолеть эту ситуацию возможно за счет удаленного администрирования (*freelance* и *outsourcing*).

3. Некоторые виды инцидентов в КСПД возникают регулярно, другие — редко. Необходимо поддерживать способность быстрого реагирования на возникающие события администраторов. С этой целью авторы рекомендуют создавать постоянно действующую в КСПД автоматизированную систему тренинга, моделирующую инциденты и оценивающую качество их устранения администраторами.

СПИСОК ЛИТЕРАТУРЫ

1. *Бородакий Ю. В., Тарасов А. А.* О функциональной устойчивости информационно-вычислительных систем // Информационное противодействие угрозам терроризма. Таганрог: ЮФУ, 2006. № 6. С. 79—93.

2. *Додонов А. Г., Флейтман Д. В.* Корпоративные информационные системы: обеспечение живучести // Математические машины и системы. 2005. № 4. С. 118—130.

3. ГОСТ Р ИСО/МЭК 7498-4-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 4. Основы административного управления.

4. *Мишин Д. В.* О применении среды моделирования AnyLogic в исследовании эффективности алгоритмов выбора администраторов корпоративной сети передачи данных // Тр. 5-й Всерос. науч.-практич. конф. „Имитационное моделирование. Теория и практика“ ИММОД-2011. СПб, 2011. Т. 1. 448 с.

5. *Мишин Д. В., Монахова М. М.* Имитационное исследование алгоритмов оптимизации административных ресурсов КСПД // Проблеми інформатики і моделювання. Тез. 11-і міжнар. наук.-техн. конф. Харків-Ялта: НТУ „ХПІ“, 2011. 84 с.

6. *Мишин Д. В., Монахова М. М.* О модели администратора автоматизированной системы администрирования корпоративной сети передачи данных // „Перспективные технологии в средствах передачи информации“. Матер. 9-й Междунар. науч.-технич. конф. Владимир: ВлГУ, 2011. Т. 1. 272 с.

7. *Мишин Д. В., Монахова М. М.* Алгоритм выбора администраторов корпоративной сети передачи данных // „Информационные системы и технологии ИСТ-2011“. Матер. XVII Междунар. науч.-технич. конф. Н. Новгород, 2011. С. 147—148.

8. *Мишин Д. В., Монахова М. М.* Система документированного обеспечения администрирования корпоративной сети передачи данных // Вестн. Костромского гос. ун-та им. Н. А. Некрасова. Сер. Технические и естественные науки „Системный анализ. Теория и практика“. 2010. Т. 16, № 1. С. 70—72.

Сведения об авторах

Денис Вячеславович Мишин — аспирант; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: mishin.izi@gmail.com

Михаил Юрьевич Монахов — д-р техн. наук, профессор; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; заведующий кафедрой; E-mail: mmonakhov@vlsu.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.