как ступенчатая модель. В качестве карбюризатора в нашем случае используется керосин.

Разработан методический подход, с помощью которого производится цементация деталей. Ниже предложена модель (рис.1), по которой будет происходить автоматизированный процесс насыщения деталей углеродом.

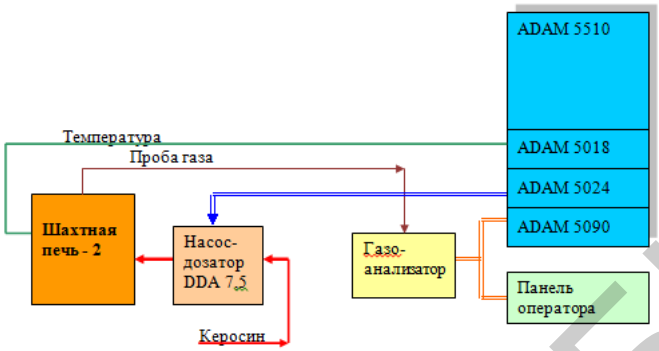

Рисунок 1. Структурная схема системы управления процессом насыщения деталей углеродом.

Система управления может работать в двух режимах:

1. Ручной режим. Здесь управление насос-дозатором отсутствует, расход керосина задается вручную.
2. Режим управления. При температуре в печи менее 870 ^{0}C керосин не подается в печь, а при достижении 920 ^{0}C происходит автоматическая подача жидкого карбюризатора. Далее с газоанализатора через модуль интерфейсов ADAM-5090 получаем информацию о содержании газовых компонентов CO и CO_2 и одновременно определяется температура газа в печи. По полученным результатам рассчитывается текущее значение углеродного потенциала печной атмосферы. Исходя из полученных результатов, через модуль ADAM-5024 происходит команда на регулирование подачи керосина в печь.

Полученные данные каждого из режимов отображаются на операторской панели в реальном времени.

УДК 004.418

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Мордасова Е.В.
Научный руководитель – Гутич И.И., старший преподаватель

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы

эффективность защиты информации росла вместе со сложностью архитектуры хранения данных.

Наглядными примерами, иллюстрирующими необходимость защиты информации и обеспечения информационной безопасности, являются участившиеся сообщения о компьютерных "взломах" банков, росте компьютерного пиратства, распространении компьютерных вирусов.

Так постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации; действуют законы о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации. Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах. Другими словами, вопросы защиты информации и защиты информации в информационных системах решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения. Под информационной безопасностью понимается защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена.

На практике важнейшими являются три аспекта информационной безопасности:

Доступность - возможность за разумное время получить требуемую информационную услугу.

Целостность - ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность - защита от несанкционированного прочтения.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления - производством, транспортом. Менее драматичные, но также весьма неприятные последствия - и материальные, и моральные - может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей, например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет. Доступность - это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др. Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными. Таким образом, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности. Целостность - гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность - самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить

представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы. Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность - гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Методы и системы защиты информации, опирающиеся на управление доступом, включают в себя следующие функции защиты информации в локальных сетях информационных систем: идентификация пользователей, ресурсов и персонала системы информационной безопасности сети; опознание и установление подлинности пользователя по вводимым учетным данным (на данном принципе работает большинство моделей информационной безопасности); допуск к определенным условиям работы согласно регламенту, предписанному каждому отдельному пользователю, что определяется средствами защиты информации и является основой информационной безопасности большинства типовых моделей информационных систем; протоколирование обращений пользователей к ресурсам, информационная безопасность которых защищает ресурсы от несанкционированного доступа и отслеживает некорректное поведение пользователей системы.

Информационная безопасность банков и экономическая информационная безопасность и других систем должна обеспечивать своевременное реагирование на попытки несанкционированного доступа к данным посредством сигнализации, отказов и задержке в работе.

Литература

1. http://www.natahaus.ru/.
2. http://www.bibliotekar.ru/deyatelnost-predpriyatiya-2/84. htm.