УДК 65.012.8

А.М.БЛИНОВ, *канд. экон. наук, доцент, (812)328-82-56*
Санкт-Петербургский государственный горный университет

A.M.BLINOV, *PhD in ec. sc., associate professor, (812)328-82-56*
Saint Petersburg State Mining University

НЕКОТОРЫЕ АСПЕКТЫ АВТОМАТИЗАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ПРЕДПРИЯТИЙ С УЧЕТОМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья посвящена вопросам классификации информационных систем, а также актуальной проблеме обеспечения информационной безопасности в корпоративных информационных системах. Построение различных функциональных подсистем должно быть рассмотрено в сочетании с возможностью использования подсистем защиты.

***Ключевые слова*:** информационные системы, информационная безопасность.

SOME PROBLEMS OF AUTOMATION OF TECHNOLOGICAL PROCESSES OF THE ENTERPRISES WITH USING OF INFORMATION SECURITY

The article is devoted to the problem of information systems classification as well as to such an urgent issue as providing information security in corporate information systems. The problem of various functional subsystems creation has to be considered along with the study of the possibility of guarding subsystems use.

***Key words*:** information systems, information security.

В современных экономических условиях предприятие должно быть готово к оперативному и точному реагированию на любое изменение ситуации на рынке. На крупных предприятиях циркулируют большие и зачастую весьма запутанные потоки информации. Предприятия и, особенно корпорации, представляющие собой многопрофильные территориально распределенные структуры с распределенным управлением, более других нуждаются в создании единого информационного пространства, устраняющего барьеры между подразделениями. Это и понятно – чем крупнее предприятие, тем дороже обходится неэффективное управление. Единственный способ сделать корпорацию реально и эффективно управляемой – охватить ее информационной системой (ИС).

Информационные системы высокого уровня, позволяющие компании выдвинуться в лидеры в своей области деятельности, должны удовлетворять двум непреложным требованиям: разрабатываться достаточно быстро и быть легко адаптируемыми к постоянно меняющимся требованиям формирующегося рынка.

Потребность в защите данных, циркулирующих в информационных и вычислительных системах, от несанкционированного, случайного или злоумышленного использования, модификации или уничтожения особенно остро проявилась в последнее время в связи с резким ростом количества сетей ЭВМ, предназначенных для работы в режиме разделения ресурсов (времени, данных) между большим числом пользовате-

Основные признаки классов ИС

Параметры	Классы		
	Малые ИС	Средние ИС	Крупные ИС
Жизненный цикл	Непродолжительный	Длительный	Длительный
Массовость использования	Массовое	Сотни	Десятки
Стоимость	Низкая	Средняя	Высокая
Аналитическая обработка данных	Нет	Есть	Высокая
Возможность модификации	Только разработчики	Совместно	Совместно
СУБД	Настольные СУБД (FoxPro, Clipper, Paradox, Access)	ORACLE, dBase	–
Наличие дополнительного программного обеспечения	Нет	Возможность обмена данными	Много
Требования к оборудованию	Невысокое	В зависимости от поставленной задачи	Высокое (жизненный цикл оборудования меньше, чем у системы)
Требование к обслуживающему персоналу	Нет	Для функций администрирования	Администрирование Сопровождение Разработка
Обеспечение безопасности	Нет	Есть	Разнообразное
Предметные области	1	Несколько	Десятки
Решаемые задачи	Узконаправленная	Объединение нескольких параллельных задач	Масштабные и сложные
Распределенность	Локальная	1-5 офисов	Территориальная

лей, т.е. соответственно с ростом числа корпораций (предприятий).

Каждое предприятие по-своему уникально, однако несколько общих принципов, отражающих базовые требования к гибкости и надежности архитектуры создаваемой ИС на нем все-таки можно сформулировать:

• предоставление легкого, прозрачного и защищенного доступа к данным;

• поддержка быстрой разработки (rapid application development-RAD) и инсталляции новых приложений в системе;

• возможность оперативной модификации существующих приложений в системе;

• обеспечение легкой интеграции новых и прежних приложений в системе;

• максимальное сохранение уже сделанных финансовых вложений в компьютеры, сетевую инфраструктуру, разработанные приложения и в квалификацию персонала;

• поддержка существующих технологий и стандартов и возможность легкой модернизации под новые стандарты и технологии;

• максимальное поощрение накопления и повторного использования различных утилит (время, когда каждая задача писалась с нуля, безвозвратно прошло);

• возможность динамической переконфигурации системы или сетевого окружения без потери работоспособности информационной системы. Простой информационной системы может вызвать огромные потери;

• наличие таких свойств, как адаптируемость, переносимость, сопрягаемость с другими системами, управляемость, защищенность информационного наполнения, распределенность, надежность, доступность для удаленных пользователей.

Специфика решаемых с помощью ИС задач, различная сложность их создания, модификации, сопровождения, интеграции с другими ИС и т.п. позволяют разделить информационные системы на классы: малые, средние и крупные (корпоративные) информационные системы (см. таблицу).

Корпоративные информационные системы (КИС) – это, в первую очередь, интегрированные многоплатформенные системы

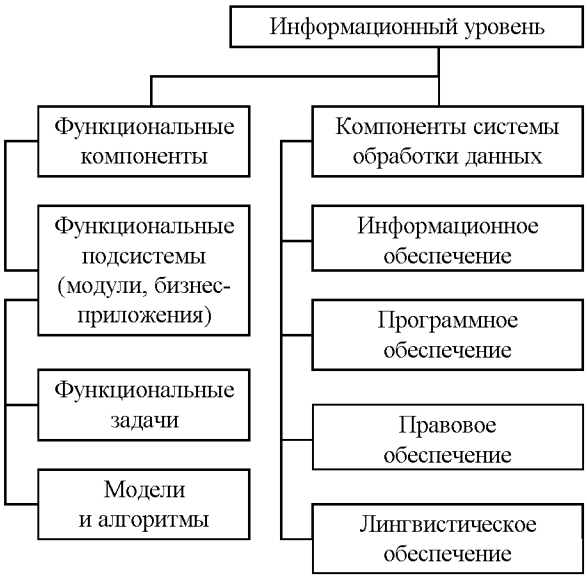


Рис.1. Структура информационного уровня

на функционально и территориально распределенном предприятии, основанные на углубленном анализе потоков данных и бизнес-процессов, на построении систем поддержки и принятия решений, электронном документообороте и делопроизводстве. КИС призваны объединять бизнес-стратегию предприятия и передовые информационные технологии.

Прежде всего КИС должна охватывать как весь документооборот корпорации с учетом территориальной распределенности, так и обеспечивать внешние связи предприятия при работе с клиентами и партнерами. При этом система должна быть удобна для пользователя, обеспечивать необходимый уровень скорости работы, безопасности и надежности.

В любой КИС можно выделить два уровня: информационный и технологический

Из них ключевое значение для корпоративного управления имеет информационный уровень КИС (рис.1), а технологический уровень является обеспечивающим.

Технологический уровень состоит из следующих компонентов:

• структурированной кабельной системы (розетки, пожарная сигнализация, мониторинг и видеонаблюдение, вентиляция и кондиционирование, вспомогательное оборудование, АТС, системы жизнеобеспечения здания);

• активного оборудования (шлюзы, маршрутизаторы, концентраторы);

• серверов;

• рабочих станций.

Основной для работоспособности КИС является производственная база данных и документооборот. Согласно этому определяются остальные компоненты информационного уровня, например операционная система и доступ к internet. Исходя из всей информационной составляющей, формируется технологический уровень. На сегодняшний день существует и обратная зависимость: производственную базу данных выбирают в зависимости от стоимости модернизации аппаратного обеспечения и технологический уровень становится первичным.

С другой стороны, КИС можно рассмотреть как набор технического, программного, человеческого и информационного компонентов (объектов).

Рассмотрим безопасность объектов КИС. Концепция построения системы защиты с точки зрения функции управления представлена на рис.2.

Обеспечение безопасности информационных технологий зависит от полноты исследований, характерных особенностей тех изменений в объекте защиты, который вносит научно-технический прогресс. К особенностям современных информационных технологий следует отнести массовость использования информационных систем.

С точки зрения обеспечения безопасности ИТ очень важно непосредственное воздействие на информацию на любом из уровней ее представления, которое возможно только средством ее обработки того же уровня.

Характерной особенностью современной информационной технологии является высокий уровень значимости ИС в их обеспечении. При этом специфика использования ИС заключена в трехуровневой схеме представления информационных техноло-



Рис.2. Концепция построения системы защиты

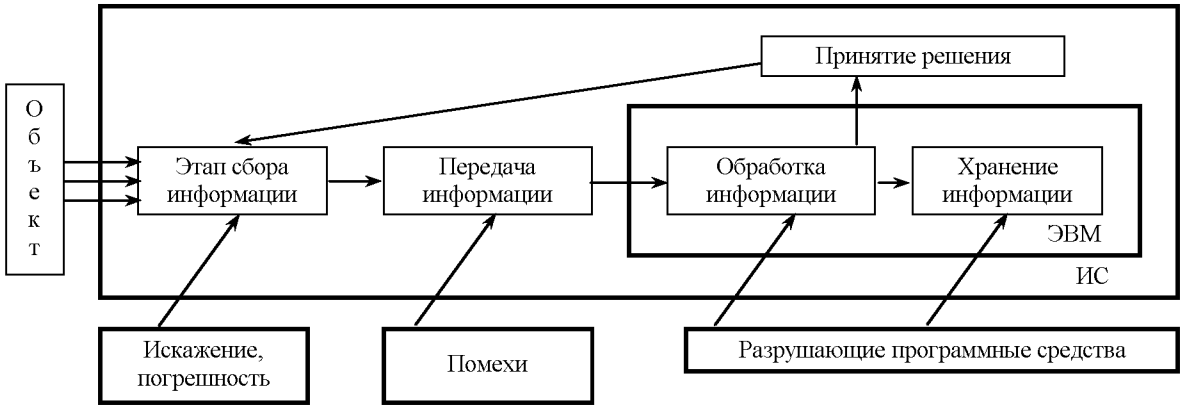


Рис.3. Трехуровневая схема представления ИТП с внешними разрушающими воздействиями

гических процессов, где каждый уровень характеризуется не только формой представления информации, но и соответствующими ей средствами обработки (рис.3).

Таким образом, создаваемая информационная система, претендующая на звание корпоративной, обязана иметь в своем составе инструментарий обеспечения информационной безопасности на всех уровнях представления информации. В случае модернизации уже существующей ИС специалисты, проводящие данную модернизацию с учетом специфики и особенностей технологических процессов, должны предусматривать возможность применения инструментария информационной безопасности.