Характеристика автоматизированной информационной системы управления компании

1.1. Сущность и понятие автоматизированной системы управления компании

Информация в настоящее время является наиболее важной из многих ресурсов, а информационные системы — это неотъемлемая часть практических во всех сферах деятельности компаний.

В современной мире и функционировании любой компании и организации, не вызывает сомнений потребность в автоматизированных системах, комплексах и устройствах для решения разнообразных задач, быстрого доступа к необходимой информации. Редко в современном обществе применяют традиционные информационные системы (ИС).

**Система** (греч., «целое, составленное из частей, соединение») –это множество элементов, связанных друг с другом определенными отношениями, и образующих определенную целостность, единство.

Так под системой понимают любой объект, который рассматривается как единое целое, для достижения поставленной задачи. Все систему могут различаться между собой как по составу, так и по главным целям.

Под автоматизацией представляется огромный комплекс действий и различных мероприятий, технического, организационного и экономического характера. Автоматизация помогает снизать степень участия, а в некоторых случая и полностью исключить участие человеческого фактора в организации производственного или технологического процесса.

Автоматизация предполагает использование технических средств и инновационных технологий для исполнения с помощью их многих организационных процессов. Также она служит фундаментом конкретных изменений во многих областях.

Перед автоматизацией стоит ряд основных задач, таких как:

- ускорение процессов обработки и сортирование информации;

- сокращение человеческого фактора при выполнении традиционных процессов и операций;

- нововведения или замена элементов в традиционных технологиях;

- повышение качества, доступности и оперативности обслуживания пользователей;

- облегчение в передаче широкого обмена информации;

- эффективность в использовании информационных ресурсах;

- расширенные возможности организации, эффективность использования ресурсов с помощью новых информационных технологий.

**Автоматизированная система** (согласно ГОСТу) – это система, состоящая из взаимосвязанной совокупности подразделений организации и комплекса средств автоматизации деятельности, реализующая автоматизированные функции по отдельным видам деятельности.

Изменилась коренным образом технология информационных процессов в управлении, благодаря опыту создания АИС управления компании и внедрения экономической работы методов оптимизации, формализации ситуаций производственно-хозяйственных процессов, оснащения государственных и коммерческих структур современными вычислительными средствами.

Далее рассмотрим следующие признаки автоматизированной информационной системы:

-АИС управления компании и технологическими процессами – это человеко-машинные системы, которые несут за собой задачу обеспечения управлением техническими устройства, какими-либо автоматическими линия, станка.

-АИС управления компании и организационно-техническими процессами представляют собой многоуровневые системы, сочетающие АИС управления технологическими процессами и АИС управления предприятиями.

- Для АИС организационного управления объектом служат производственного-хозяйственные, социально-экономические функциональные процессы, реализуемые на всех уровнях управления экономикой, в частности:

- банковские АИС;

- АИС фондового рынка;

- финансовые АИС;

- страховые АИС;

- налоговые АИС;

- АИС таможенной службы;

- статистические АИС;

-АИС промышленных предприятий и организаций (в современном мире актуальны бухгалтерские АИС) и др.

АИС научных исследований обеспечивают высокое качество и эффективность межотраслевых расчетов и научных опытов методической базой таких систем служат экономико-математические методы, технической базой – самая разнообразная вычислительная техника и технические средства для проведения экспериментальных работ моделирования.

В настоящее время широкое распространение получают обучающие АИС, в связи с тем, что всегда есть место подготовке специалистов в системе образования, при повышении квалификации, переквалификации работников разных отраслей деятельности.

При АИС организационного управления выделяют отраслевые, территориальные и межотраслевые АИС, которые в свою очередь являются системами организационного управления, но уже следующего – более высокого уровня иерархии

Задачей отраслевых АИС, является информационное обслуживание аппарата управления соответствующих ведомств. Отраслевые АИС функционируют в сферах промышленного и агропромышленного комплексов, а также в строительстве и на транспорте. Эти систем решают задачи информационного обслуживания аппарата управления соответствующих ведомств.

Территориальные АИС предназначены для управления административно-территориальными районами. То есть деятельность система предназначена для качественного обслуживания аппарата управления соответствующих ведомств.

Межотраслевые АИС являются специализированными системами функциональных органов управления национальной экономикой (банковских, финансовых, снабженческих, статистических и др). Межотраслевые АИС имеют мощные вычислительные комплексы, многоуровневые АИС обеспечивают максимально точную разработку экономических и хозяйственных прогнозов, государственного бюджета, осуществляют контроль результатов и регулирование деятельности всех звеньев хозяйства, а также контроль наличия и распределения ресурсов.

В настоящее время развитие информатизация прогрессирует в различных областях, такая деятельность как экономическая и управленческая требуют единых подходов для решения организационных, технических и различных технологических проблем. Основными факторами, определяющими результаты создания и функционирования АИС и процессов информатизации, являются:

-активная роль человека – профессионала в системе автоматизации принятия управленческих решений, обработки информации;

- интерпретация информационной деятельности как одного из видов бизнеса;

-наличие научно обоснованной программно-технической, технологической платформы, реализуемой на конкретном экономическом объекте;

-создание и внедрение научных и прикладных разработок в области информатизации в соответствии с требованием пользователей;

-формирование условий организационно-функционального взаимодействия и его математическое, модельное, системное и программное обеспечение;

-постановка и решение конкретно поставленных задач в области управления, с учетом заданных критериев эффективности.

Определяя АИС как организованную для достижения общей цели совокупность специалистов, средств вычислительной и другой техники, математических методов и моделей, интеллектуальных продуктов и их описаний, а также способов и порядка взаимодействия указанных компонентов, следует подчеркнуть, что главным звеном и управляющим субъектом в перечисленном комплексе элементов был и остается до сих пор человек, специалист.

Существуют следующие виды информационных технологий:

-информационная технология обработки данных;

-информационная технология управления;

-автоматизация офиса;

-информационная технология поддержки принятия решений;

-информационная технология экспертных систем.

Информационная технология обработки данных необходима для решения структурированных задач, у которых имеется входная информация данных, алгоритмы и стандарты для обработки и сортировки информации. Данная технология применяется на уровне операционной деятельности персонала невысокой квалификации, для автоматизации каждодневных рутинных операций управленческого труда. Из этого можно заметить, что внедрение информационных технологий и систем на этом уровне существенно повышают производительность труда организации.

Целью информационной технологии управления является удовлетворение информацион­ных потребностей всех без исключения сотрудников фирмы, имеющих дело с принятием решений. Она может быть полезна на любом уровне управления.

Эта технология ориентирована на работу в среде информационной системы управления и используется при худшей структурированности решаемых задач, если их сравнивать с задачами, решаемыми с помощью информационной технологии обработки данных.

Под автоматизацией офиса нужно понимать комплексную автоматизацию работы всех офисных подразделений:

 -кадровой службы;
 -канцелярии;

-бухгалтерии;

-секториата;

-планово-экономического отдела и другое.

Целью автоматизации офисной деятельности является повышение эффективности управления предприятием и обеспечение согласованности и бесперебойной работы всех служб. Автоматизация офиса гарантирует комфортные условия работы для всех сотрудников, полностью ликвидирует или минимизирует ручное выполнение рутинных операций, практически исключает случайные ошибки исполнителей, оптимизирует все имеющиеся бизнес-процессы.

Главной особенностью информационной технологии поддержки принятия решений является качественно новый метод организации взаимодействия человека и компьютера. Выработка решения, что является основной целью этой технологии, происходит в результате итерационного процесса (рисунок ), в котором участвуют:

- система поддержки принятия решений в роли вычислительного звена и объекта управления;

- человек как управляющее звено, задающее входные данные и оценивающее полученный результат вычислений на компьютере.



Рис. 1.1. – Схема уровня информационной потребности

Окончание итерационного процесса происходит по воле человека. В этом случае можно говорить о способности информационной системы совместно с пользователем созда­вать новую информацию для принятия решений.

Дополнительно к этой особенности информационной технологии поддержки принятия решений можно указать еще ряд ее отличительных характеристик:

- ориентация на решение плохо структурированных задач;

- сочетание традиционных методов доступа и обработки компьютерных данных с возможностями математических моделей и методами решения задач на их основе;

- направленность на непрофессионального пользователя компьютера;

- высокая адаптивность, обеспечивающая возможность приспосабливаться к особенностям имеющегося технического и программного обеспечения, а также требованиям пользователя.

Информационная технология экспертных систем, основана на использовании искусственного ин­теллекта. Экспертные системы дают возможность менеджеру или специалисту получать консультации экспертов по любым проблемам, о которых этими системами накоплены знания.

Назначение экспертных систем заключается в решении достаточно трудных для экспертов задач на основе накапливаемой базы знаний, отражающей опыт работы экспертов в рассматриваемой проблемной области.

Под искусственным интеллектомпонимают способности ком­пьютерных систем к таким действиям, которые назывались бы интеллектуальными, если бы исходили от человека. Обычно имеются в виду способности, связанные с челове­ческим мышлением. Работы в области искусственного интеллекта включают в себя создание роботов, систем, моделирующих нервную систему человека, его слух, зрение, обоняние, способность к обу­чению.

Такое положение стало возможным благодаря стремительному распространению персональных ЭВМ (ПЭВМ) и других компактных и относительно дешевых средств вычислительной техники (СВТ). Кроме компьютеров к техническим средствам АИС относят средства связи (телекоммуникации) и оргтехнику (телефон, факс и т.п.).

Появилась возможность объединять персональные ЭВМ в сети, что создает пользователю качественно новые условия для проведения оперативного анализа производственных, экономических и финансовых ситуаций, а в сочетании с ЭВМ эти возможности практически не ограничены.

Несмотря на всю важность технических решений, ценность и уникальность АИС составляют интеллектуальные продукты, разрабатываемые участниками проектирования и последующих доработок. При этом очень важное, а иногда решающее значение для долговечности и устойчивого функционирования систем имеет наличие хорошо написанных для пользователей системы подробных инструкций по эксплуатации, совокупность которых образует документацию АИС.

 1.2 Анализ информационных ресурсов и информационных потоков автоматизированной системы управления компании

1.3 Основные аспекты информационной безопасности автоматизированной информационной системы управления компании

Характерной особенностью информации является возможность посторонних лиц быстро исказить, копировать или уничтожить ее. Эти и другие угрозы вызывают необходимость организации безопасного функционирования данных в любых информационных системах. Такие мероприятия называют защитой информации или информационной безопасностью.

Проблемы информационной безопасности имеют не только местные и государственные, но и геополитические аспекты. Это – комплексная проблема, поэтому ее решение рассматривается на разных уровнях: законодательном, административном, процедурном и программно-техническом.

Безопасность информации (англ. «information security») или информационная безопасность - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам и пользователям информации, и поддерживающей ее структуре.

Под угрозой безопасности информации понимают действие или событие, способное привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

Несанкционированное и санкционированное использование характеризуется такими понятия как несанкционированный и санкционированный доступы.

 Несанкционированный доступ – бесправное вторжение к информационным ресурсам и системам для их использования (прочтения, копирования, модификации, и другого), а также искажения или уничтожения.

Санкционированный доступ – это доступ к информации, программам и данным пользователей, имеющих право выполнять определенные действия, а также полномочия и права пользователей на использование ресурсов и услуг, определенных администратором системы.

Все угрозы можно разделить на непреднамеренные и умышленные.

Источником случайных угроз могут быть как природные явления и техногенные катаклизмы, так и ошибки в программном обеспечении, выход из строя аппаратных средств, неправильного действия пользователей или администрации.

Умышленные угрозы преследуют цель нанести ущерб информации и пользователям АИС и самой АИС. Они подразделяются на активные и пассивные.

Пассивные угрозы – направлены на несанкционированное использование информационных ресурсов и систем, не оказывающее влияния на их функционирование. Пассивной угрозой является, например, попытка получения циркулирующей в каналах информации, посредством ее прослушивания или копирования.

Активные угрозы - нацелены на нарушение нормального процесса функционирования и используют целенаправленное воздействие на аппаратные, программные и информационные ресурсы. К активным угрозам относят, например, разрушение или радиоэлектронное подавление линий связи вывод из строя компьютера или операционных систем, искажение сведений в базах данных или в системной информации в компьютерных технологиях. Источниками активных угроз могут быть непосредственные действия злоумышленников, программных вирусов и другое.

К основным угрозам безопасности информации и работоспособности АИС управления компании относят:

- несанкционированное использование информационных ресурсов и АИС;

- ошибочные действия пользователей, приводящие к частичной или полной потере информации и работоспособности АИС;

- сбои программных и технических средств, приводящие к частичной или полной потере информации и работоспособности АИС;

- иные виды воздействий, приводящие к частичной, полной потере или замене информации, к замене АИС или её компонентов, изменению технологии её работы;

- различные виды воздействий, приводящие к потере работоспособности АИС или её уничтожению.

Несанкционированные воздействия на АИС управления компании (а также информацию, здания, помещения и людей) могут быть вызваны различными причинами и угрозами. Они осуществляются с помощью различных методов. Например, несанкционированные воздействия на АИС управления компании могут быть обусловлены стихийными бедствиями (ураганы, ливни, молнии, наводнения, пожары, взрывы и др.), техногенными катастрофами, террористическими актами и т.п. Борьба с такими воздействиями обычно весьма затруднена из-за значительной степени их непредсказуемости. В частности, достаточно трудно предвидеть не только время, но и возможные воздействия подобных факторов на конкретные АИС.

Наибольший ущерб информации и АИС управления компании наносят неправомерные действия сотрудников и компьютерные вирусы. Американские специалисты утверждают, что до 85% случаев промышленного шпионажа ведётся силами сотрудников компании, в которой это происходит. При этом не менее трети финансовых потерь и потерь данных в организациях происходит по вине их собственных сотрудников. Вирусы представляют широко распространённое явление, отражающееся на большинстве пользователей компьютеров, особенно работающих в сетях и с нелицензионным программным обеспечением.

Данные факторы можно предвидеть и принять соответствующие меры. К ним относят, например, использование специальных программно-технических средств защиты, надлежащую организационную и техническую их поддержку, точность выполнения предусмотренных в документации процедур и др. Решение этих проблем обычно входит в компетенции администрации и службы безопасности организации.

Защита от вредоносных воздействий на информацию и программное обеспечение осуществляется путём использования соответствующих средств и методов защиты. Средства и методы защиты информации и АИС управления компании можно разделить на две большие группы: организационные и технические.

Под организационными подразумеваются законодательные, административные и физические, а под техническими – аппаратные, программные и криптографические мероприятия, направленные на обеспечение защиты объектов, систем, людей и информации.

Организационные мероприятия и процедуры, используемые для решения проблем безопасности, решаются на всех этапах проектирования и в процессе эксплуатации АИС управления компании.

Существенное значение при проектировании придается предпроектному обследованию объекта. На этой стадии:

- устанавливается наличие секретной (конфиденциальной) информации в разрабатываемой АИС, оценивается уровень конфиденциальности и объемы;

- определяются режимы обработки информации (диалоговый, телеобработки и режим реального времени), состав комплекса технических средств, общесистемные программные средства и т.д.;

- анализируется возможность использования имеющихся на рынке сертифицированных средств защиты информации;

- определяется степень участия персонала, функциональных служб, специалистов и вспомогательных работников объекта автоматизации в обработке информации, характер взаимодействия между собой и со службой безопасности;

- определяются мероприятия по обеспечению режима секретности на стадии разработки.

Среди организационных и технических мероприятий по обеспечению безопасности важное место занимает охрана объекта, на котором расположена защищаемая АИС (территория здания, помещения, хранилища информационных носителей). При этом устанавливаются соответствующие посты охраны, технические средства, предотвращающие или существенно затрудняющие хищение средств вычислительной техники, информационных носителей, а также исключающие несанкционированный доступ к АИС и телекоммуникациям.

Функционирование системы защиты информации от несанкционированного доступа, как комплекса программно-технических средств и организационных (процедурных) решений, предусматривает:

- учёт, хранение и выдачу пользователям информационных носителей, паролей, ключей;

- ведение служебной информации (генерация паролей, ключей, сопровождение правил разграничения доступа);

- оперативный контроль за функционированием систем защиты секретной информации;

- контроль соответствия общесистемной программной среды эталону;

- приемку включаемых в АИС новых программных средств;

- контроль за ходом технологических процессов в АИС путём регистрации и анализа действий пользователей;

- сигнализацию опасных событий и т.д.

Организационные средства защиты – это организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций и программных продуктов для обеспечения их безопасности.

Технические средства безопасности реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические. Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу.

Физические средства защиты реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решётки на окнах, электронно-механическое оборудование охранной сигнализации (турникеты, металлодетекторы и др.).

Программные средства представляют собой специальное (специализированное) программное обеспечение, предназначенное для выполнения функций защиты информации АИС управления компании.

Морально-этические средства защиты подразумевают применение норм, традиционно сложившихся или складывающихся по мере распространения в обществе технических средств, телекоммуникаций и АИС. Они обычно не обязательны как законодательные меры, но несоблюдение их может привести к потере авторитета и престижа человека или организации.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Все рассмотренные средства защиты разделены на формальные и неформальные. Формальные средства защиты выполняют защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека. Неформальные средства защиты определяются целенаправленной деятельностью человека или регламентируют её.

Эффективность защиты информации и АИС управления компании в значительной степени зависит от своевременности обнаружения и исключения воздействий на них, восстановления программ, информации, работоспособности систем и компьютерных устройств. Важной составляющей выполнения подобных действий являются программные и технические средства защиты.

В современных информационных технологиях для эффективного использования методов защиты широко применяются программно-технические средства, основанные на использовании биометрических систем и др.

Программные средства защиты представляют комплекс алгоритмов и программ специального назначения и общего обеспечения работы компьютеров, информационных сетей и программ (в том числе АИС). Они нацелены на: контроль и разграничение доступа к информации, исключение несанкционированных действий с ней, управление охранными устройствами и т.п. Проверка подлинности пользователя обычно осуществляется операционной системой. Пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

Работа любого субъекта (пользователя или процесса) в АИС управления компании должна быть идентифицирована системой.

Идентификация – это метод сравнения предметов, систем или лиц по их характеристикам, с целью их опознания и определения полномочий, связанных с доступом к ним («это тот, кем назвался и имеет право выполнять данную деятельность?»).

Аутентификация – метод независимого от источника установления подлинности информации, АИС и др. на основе проверки подлинности их внутренней структуры («это тот, кем назвался?»).

Основным средством аутентификации пользователей в АИС обычно является использование схемы «имя пользователя/пароль». При этом система должна допускать возможность расширения процедур аутентификации на основе использования смарт-карты, touch memory, дискеты, флеш-памяти и др. Также должна присутствовать возможность дифференцированного считывания информации с токена (пароля или ПИН-кода) при аутентификации, ключа при шифровании или электронно-цифровой подписи.

Авторизация в информационных технологиях – это предоставление определённых полномочий лицу или группе лиц на выполнение некоторых действий в системе обработки данных («имеет ли некто право выполнять данную деятельность?»).

Посредством авторизации устанавливаются и реализуются права доступа к ресурсам и АИС.

Для определения единообразного уровня доступа субъектов к информационным объектам (к АИС) существуют возможности распределения доступа к:

- группе или нескольким группам объектов;

- объекту;

- набору частей объекта.

При организации доступа к АИС используются следующие виды ограничений:

- нет доступа;

- доступ только на чтение;

- доступ на изменение и (или) добавление (отдельно с чтением и без чтения);

- доступа на удаление и др.

Схема определения доступа должна предусматривать возможность группового или ролевого доступа, то есть создание абстрактного профиля прав пользователя. При включении нового пользователя в конкретную группу он автоматически наследует все права, присущие пользователям этой группы. Информация об атрибутах профиля пользователя (пароли, ключи) должна сохраняться в виде, исключающем возможность прямого доступа к ним пользователей. Это означает, что указанные данные при постоянном хранении должны быть защищены средствами криптографии с предоставлением доступа только самому пользователю, процессам подсистемы безопасности, или администратору, уполномоченному подсистемой безопасности.

Для каждого информационного объекта (АИС или её подсистем) должен существовать владелец с полными правами доступа. При этом система контролирует обязательное наличие хотя бы одного пользователя (владельца или администратора) для каждого информационного объекта.

В большинстве случаев для защиты информации и АИС управления компании, ограничения несанкционированного доступа к ним и др. приходится одновременно использовать программные и технические средства, системы и устройства. Так, с целью защиты сетей и контроля доступа в них используют:

- фильтры пакетов, запрещающие установление соединений, пересекающих границы защищаемой сети;

- фильтрующие маршрутизаторы, реализующие алгоритмы анализа адресов отправления и назначения пакетов в сети;

- шлюзы прикладных программ, проверяющие права доступа к ним.

Для обеспечения безопасности АИС применяют различные средства и механизмы. Механизмы безопасности должны использоваться в форме широко известных в мире, опробованных и одобренных стандартов и протоколов. При этом должно обеспечиваться сохранение данных, связанных с АИС (собственно модулей системы, системных и прикладных данных).

В АИС должна иметься собственная встроенная или внешняя подсистема проверки целостности файлов, модулей и системных данных самой АИС на предмет их несанкционированной модификации. При этом должна присутствовать настройка на запрет удаления отдельных категорий данных. Система также должна предусматривать возможность восстановления удалённых данных в течение определенного промежутка времени.

Процессы, требующие от АИС монопольного использования ресурсов и препятствующие интерактивной работе пользователей, должны переноситься на время наименьшей активности (ночь) и занимать в сумме не более 10–15% суточного рабочего времени системы.

АИС должна иметь возможность резервного копирования и восстановления средствами самой системы. Резервное копирование должно осуществляться на различные носители, при этом общий объём резервной копии может быть распределён между двумя или более носителями. Резервное копирование должно предусматривать как сохранение прикладных, так и системных данных, и осуществляться в режиме с криптографической защитой по заранее установленному графику от одного до нескольких раз в день или вручную по команде оператора. При этом процедура не должна забирать ресурсы системы в монопольное использование.

Системы настройки аутентификационных механизмов, авторизации, прав доступа и прочих элементов схемы безопасности должны четко различать варианты локальной и удаленной работы и, соответственно, иметь возможность применения различных правил в зависимости от режима доступа.

Создание базовой системы защиты информации в АИС управления компании основывается на следующих принципах:

Комплексный подход к построению системы зашиты при ведущей роли организационных мероприятий, означающий оптимальное сочетание программных аппаратных средств и организационных мер защиты и подтвержденный практикой создания отечественных и зарубежных систем защиты.

Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки, т. е. предоставление пользователям минимума строго определённых полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автоматизированной обработки доступной им конфиденциальной информации.

Полнота контроля и регистрации попыток несанкционированного доступа, т. е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в АИС без её предварительной регистрации.

Обеспечение надёжности системы защиты – это невозможность снижения уровня надёжности при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала.

Обеспечение контроля за функционированием системы защиты – создание средств и методов контроля работоспособности механизмов защиты.

«Прозрачность» системы защиты информации для общего, прикладного программного обеспечения и пользователей АИС управления компании.

Экономическая целесообразность использования системы защиты, выражающаяся в том, что стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации АИС управления компании без системы защиты информации.