8 ТЕХНОЛОГИЧЕСКОЕ ПОСТРОЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

8.1. Общее содержание работ

Организационные системы - это сложные многоуровневые системы, состоящие из множества взаимодействующих элементов и подсистем. Характерной особенностью организационной системы, отличающей ее от систем другого типа, например от технических систем, является то, что каждый элемент организационной системы принимает решение по организации действий, т. е. является решающим элементом.

Линейная структура. Каждый исполнитель (И) Подчиняется только одному руководителю (Р) по всем вопросам своей деятельности. Основной недостаток линейных структур - сильная зависимость результатов работы всей ОС от качества решений первого руководителя.

Функциональная структура. Каждый исполнитель подчиняется нескольким функциональным руководителям (ФР) одновременно, причем каждому по строго определенным вопросам. При этой структуре руководящие указания более квалифицированны, но нарушается принцип единоначалия.

Линейно-штабная структура. В каждом звене управления создаются штабы (советы, отделы, лаборатории), в которых имеются специалисты по отдельным важным вопросам. Штабы (Ш) подготавливают квалифицированные решения, но утверждает и передает их на нижние уровни линейный руководитель.

Программно-целевая структура. Опираясь на осмысление закономерностей реальных процессов формирования ОС, а также с учетом традиционных этапов разработки больших систем, можно предложить следующие технологические этапы ОС для наиболее сложного вида проблем (непрограммируемых проблем).

Под проектированием КСЗИ будем понимать процесс разработки и внедрения проекта организационной и функциональной структуры системы защиты, использование возможностей существующих методов и средств защиты с целью обеспечения надежного функционирования объекта (предприятия) в современных условиях.

В зависимости от полноты перечня вопросов, подлежащих исследованию, проектные работы представляются в виде разработки комплексного или локального проекта.

- Комплексное - проектирование организации и технологии всего комплекса или большего числа мероприятий по ЗИ.
- **При локальном проектировании осуществляется проектирование отдельной подсистемы КСЗИ.**

8.2 Этапы разработки

Наилучшие результаты при создании систем любого уровня сложности достигаются, как правило, тогда, когда этот процесс четко разделяется на отдельные этапы, результаты которых фиксируются, обсуждаются и официально утверждаются.

Рекомендуется выделять следующие этапы:

На предпроектной стадии:

1) разработка технико-экономического обоснования;
2) разработка технического задания;

На стадии проектирования:

3) разработка технического проекта;
4) разработка рабочего проекта;

На стадии ввода в эксплуатацию:

5) ввод в действие отдельных элементов системы;
6) комплексная стыковка элементов системы;
7) опытная эксплуатация;
8) приемочные испытания и сдача в эксплуатацию.

Разработка технико-экономического обоснования. На этом этапе анализируется деятельность объекта, готовятся исходные данные для технико-экономического обоснования (ТЭО) и готовятся ТЭО. Главное на этом этапе – обоснование целесообразности и необходимости создания системы защиты, ориентировочный выбор защищаемых каналов, определение объемов и состава работ по созданию системы защиты, сметы и сроков их выполнения.

Разработка технического задания (ТЗ). Основная цель этапа - разработка и обоснование требований к структуре системы защиты и обеспечение совместимости и взаимодействия всех средств. Главное на этапе - сбор и подготовка исходных данных, определение состава системы, плана ее создания и оценка затрат. Разработка ТЗ начинается после утверждения ТЭО.

Разработка технического проекта (ТП). На этом этапе разрабатываются и обосновываются все проектные решения: разрабатывается и обосновывается выбранный вариант проекта; уточняются перечни технических средств, порядок и сроки их поставки. В ТП могут рассматриваться 2-3 варианта решения поставленной задачи по созданию системы защиты. Все варианты должны сопровождаться расчетом эффективности, на основе которого могут быть сделаны выводы о рациональном варианте.

При создании системы защиты небольшого или простого объекта этап технического проектирования может быть исключен.

Разработка рабочего проекта имеет своей целью детализировать проектные решения, принятые на предыдущем этапе. В частности:

- определяется и фиксируется регламент взаимодействия отдельных служб и составляющих системы обеспечения
- безопасности;
- составляются технологические и должностные инструкции персонала;
- разрабатывается рабочая документация.

Ввод в эксплуатацию. На этом этапе создается система защиты, состоящая из нескольких этапов (см. выше). На практике при создании систем защиты границы между этими этапами размыты. Состав выполняемых работ следующий:

- комплектация технического обеспечения системы;
- монтажные или строительно-монтажные работы и пусконаладочные работы;
- обучение персонала (предварительно должны быть укомплектованы все службы системы обеспечения безопасности с
- учетом требуемой квалификации);
- опытная эксплуатация компонентов и системы в целом;
- приемочные испытания и приемка системы в эксплуатацию.

Практика показывает, что основной причиной плохих разработок является отсутствие единого руководства, единого координационного плана и неудовлетворительная организация контроля и управления ходом разработки со стороны заказчика.

8.3 Факторы, влияющие на выбор состава КСЗИ

На предпроектной стадии выполняется важнейшая работа - изучается объект защиты. Ошибки, допущенные в ходе этой работы, могут существенно снизить эффективность создаваемой системы защиты и, наоборот, тщательно проведенное обследование позволит сократить затраты на внедрение и эксплуатацию системы.

Изучение объекта защиты сводится к сбору и анализу следующей информации:

1) об организации процесса функционирования объекта. В состав этих данных входят сведения, характеризующие:

- график работы объекта и его отдельных подразделений;
- правила и процедуры доступа на объект, в отдельные помещения и к оборудованию персонала и посетителей (регулярный, случайный, ограниченный доступ);
- численность и состав сотрудников и посетителей объекта (постоянный штат; персонал, работающий по контракту; клиенты);
- процедуру доступа на территорию транспортных средств. Для получения этих данных можно применять следующие способы: анкетирование сотрудников; опрос сотрудников; личное наблюдение; изучение директивных и инструктивных документов. Следует иметь в виду, что ни один из этих способов не дает объективной информации; каждый имеет свои достоинства и недостатки. Поэтому их применяют вместе, в совокупности;

2) об организации транспортных и информационных потоков. В состав этих данных входят сведения, характеризующие:

- пути и организацию транспортировки и хранения материальных ценностей на территории объекта;
- уровни конфиденциальности информации, пути и способы ее обработки и транспортировки (документы, телефонная и радиосвязь и т. п.);

3) об условиях функционирования объекта. В состав этих данных входят сведения, характеризующие

- пространство, непосредственно прилегающее к территории объекта;
- ограждение периметра территории и проходы;
- инженерные коммуникации, подземные хранилища и сооружения на территории;
- размещение подразделений и сотрудников по отдельным помещениям (с поэтажными планами);
  - инженерные коммуникации в помещениях;
  - состояние подвальных и чердачных помещений;
  - размещение, конструкцию и состояние входов, дверей, окон;
  - существующую систему защиты;
  - экономические факторы и криминогенную обстановку на прилегающей территории.

На основе результатов анализа всех перечисленных сведений должны быть определены: назначение и основные функции системы защиты; основные виды возможных угроз и субъекты угроз; внешняя среда; условия функционирования системы защиты (наличие энергетических и других ресурсов, естественные преграды и т. п.).

Эти данные рекомендуется систематизировать в виде пояснительной записки, структурных схем и планов.

Целесообразно иметь следующие планы:

1) план территории объекта с указанием расположения всех зданий и других наземных сооружений; подземных сооружений; всех коммуникаций и мест их выхода за территорию объекта; всех ограждений, в том числе по периметру территории объекта, с обозначением их технического состояния на момент обследования; средств защиты (существующей системы, если она имеется);

2) поэтажные планы, где должно быть указано расположение всех помещений с обозначением дверных и оконных проемов, внутренних и наружных (пожарных) лестниц, толщины материала стен и существующих средств защиты; всех коммуникаций с обозначением коммуникационных шкафов и других мест санкционированного доступа к каналам связи и жизнеобеспечения;

3) планы помещений с указанием мест размещения оборудования и других технических средств (телефонов, персональных ЭВМ, принтеров и т.д.); расположения коммуникаций и мест размещения коммутационного оборудования (коробки, розетки и т.п.); функционального назначения и степени конфиденциальности получаемой и обрабатываемой

информации; особенностей технологического процесса (для производственных помещений), важных с точки зрения обеспечения безопасности.

На основе этих планов целесообразно подготовить структурные схемы:

- **ограждения каждого помещения**, указав на ней (схематично) все стены и другие инженерно-технические сооружения, окружающие помещение. Эта схема позволит оценить возможности эшелонирования защиты, выработать рекомендации по рубежам защиты, выбрать и определить зоны безопасности и оценить «прочность» рубежей;
- **документооборота** (для документов с ограниченным доступом), указав источник и приемники документа; его связи с другими документами; способ подготовки (ручной, машинный); способ транспортировки (с курьером, по телефону, по факсу, по компьютерной сети и т.п.); место хранения. Для описания документооборота используют специально разработанные формы.

Основные параметры предприятия:

- **характер деятельности предприятия** - на организационно-функциональную структуру КСЗИ, ее состав; состав и структуру кадров СЗИ, численность и квалификацию ее сотрудников; техническое обеспечение КСЗИ средствами ащиты; количество и характер мер и мероприятий по ЗИ; цели и задачи КСЗИ;
- **состав защищаемой информации**, ее объем, способы представления и отображения, технологии обработки - на состав и структуру СЗИ; организационные мероприятия по ЗИ; состав технических средств защиты, их объем; состав нормативно-правового обеспечения КСЗИ; методы и способы ЗИ; объем материальных затрат на ЗИ;
- **численный состав и структура кадров предприятия** - на численный состав сотрудников СЗИ; организационную структуру СЗИ; объем затрат на ЗИ; техническую оснащенность КПП; объем организационных мероприятий по ЗИ;
- **организационная структура предприятия** - на организационную структуру КСЗИ; количество и состав сотрудников СЗИ;
- **техническая оснащенность предприятия** - на объем и состав технических средств ЗИ; количество и квалификацию технического персонала СЗИ; методы и способы ЗИ; размер материальных затрат на ЗИ;
- **нормативно-правовое обеспечение деятельности предприятия** - на формирование нормативно-правовой базы КСЗИ; регулирует деятельность СЗИ; влияет на создание дополнительных нормативно-методических и организационно-правовых документов СЗИ;
- **экономическое состояние предприятия** (кредиты, инвестиции, ресурсы, возможности) определяет: объем материальных затрат на ЗИ; количество и состав сотрудников и квалифицированных специалистов СЗИ; уровень технической оснащенности СЗИ средствами защиты; методы и способы ЗИ;
- **режим работы предприятия** - на режим функциональности КСЗИ, всех ее составляющих; состав технических средств ЗИ; объем затрат на ЗИ; численность персонала СЗИ;
- **местоположение и архитектурные особенности предприятия** - на состав и структуру СЗИ; состав технических средств ЗИ; объем материальных затрат на ЗИ; численный состав и квалификацию сотрудников СЗИ;
- **тип производства** - на организационно-функциональную структуру СЗИ;
- **объем производства** - на размеры материальных затрат на ЗИ; объем технических средств защиты; численность сотрудников СЗИ;
- **форма собственности** - на объем затрат на ЗИ (например, на некоторых государственных предприятиях затраты на защиту информации (СЗИ) могут превышать стоимость самой информации); методы и способы ЗИ.

Возможны следующие методы оценки параметров qij:

- расчетные;
- на основе статистических данных;
- метод экспертных оценок.

Все затраты на реализацию системы защиты информации по своей структуре состоят из суммы капитальных вложений и текущих расходов.

В качестве информационной базы структурно-функциональной схемы защиты информации используется проблемно-ориентированный банк данных, в который входят:

- файл исходных данных;
- файл стандартных средств защиты;
- файл штатных средств защиты;
- каталог стратегий нападения у;
- каталог мер защиты Х;
- нормы эффективности защиты.

Каталог потенциальных стратегий нападения, направленных на несанкционированные действия, является результатом специального инженерного анализа.

Каталог мер защиты - перечень мер, обеспечивающих защиту от стратегий нападения.

Каталог норм эффективности защиты. Нормой эффективности защиты информации в АСОД от утечки информации при воздействии конкретной стратегии нападения называется допустимая вероятность Р несанкционированного доступа к информации при реализации данной стратегии нападения в условиях противодействия со стороны защиты. Однако для целого

ряда прикладных задач по защите информации нормы отсутствуют. В таких случаях в качестве ориентиров используются требования заказчика, согласованные с разработчиком системы.

9 КАДРОВОЕ ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

9.1 Подбор персонала

около 70 % всех нарушений, связанных с безопасностью информации, совершаются именно сотрудниками предприятия.

Можно выделить пять причин этого факта:

1) при нарушениях, вызванных **безответственностью**, сотрудник целенаправленно или случайно производит какие-либо действия по компрометации информации, связанные со злым умыслом;

2) бывает, что сотрудник предприятия ради самоутверждения (для себя или коллег) затевает своего рода игру «пользователь против системы». И хотя намерения могут быть безвредными, будет нарушена сама практика безопасности. Такой вид нарушений называется **зондированием системы**;

3) нарушение может быть вызвано и **корыстным интересом**. В этом случае сотрудник будет пытаться целенаправленно **преодолеть систему защиты** для доступа к хранимой, перерабатываемой и обрабатываемой на предприятии информации;

4) за рубежом известна практика **переманивания специалистов**, так как это позволяет ослабить конкурента и дополнительно получить информацию о предприятии.

5) специалист, работающий с конфиденциальной информацией, испытывает **отрицательное психическое воздействие**, обусловленное спецификой этой деятельности. Поскольку сохранение чего-либо в тайне противоречит потребности человека в общении путем обмена информацией, сотрудник постоянно боится возможной угрозы утраты документов, содержащих секреты.

Способы предотвращения перечисленных нарушений вытекают из анализа побудительных мотивов - тщательного подбора персонала, подготовки персонала, поддержания здорового рабочего климата, мотивации и стимулирования деятельности сотрудников.

9.3 Мотивация

Мотивация - это процесс побуждения себя и других к деятельности для достижения личных целей или целей организации.

Мотивация, определяющая отношение к деятельности, - это личное побуждение к деятельности, т. е. побуждение, основанное на потребностях личности, ее ценностных ориентациях, интересах. Среди мотивов в первую очередь следует выделить интерес к деятельности, чувство долга, стремление к профессиональному росту. Мотивация на основе интереса связана с удовлетворением стремления к знанию и развитию. Причем существует два аспекта этой мотивации - интерес к деятельности и интерес к самому к себе как субъекту, овладевшему этой деятельностью.

Мотивация на основе чувства долга связана с потребностью соответствовать требованиям организации, ее нуждам. Особое значение составляют мотивы, основывающиеся на принципе взаимной ответственности и требовательности, характерные для коллективных отношений.

9.4 Разработка кодекса корпоративного поведения

Кодекс корпоративного поведения может выполнять три основные функции:

1) репутационную;

2) управленческую;

3) развития корпоративной культуры.

Репутационная функция кодекса заключается в формировании доверия к организации со стороны референтных внешних групп (государства, заказчиков, клиентов, конкурентов и т. д.). Наличие у компании кодекса корпоративного поведения становится общемировым деловым стандартом.

Управленческая функция кодекса состоит в регламентации поведения в сложных этических ситуациях. Повышение эффективности деятельности сотрудников осуществляется путем:

- регламентации приоритетов во взаимодействии со значимыми внешними группами;
- определения порядка принятия решений в сложных этических ситуациях;
- указания на неприемлемые формы поведения.

кодексы содержат две части:

- идеологическую (миссия, цели, ценности);
- нормативную (стандарты рабочего поведения).

декларативный вариант - это только идеологическая часть кодекса без регламентации поведения сотрудников. декларативный вариант кодекса решает в первую очередь задачи развития корпоративной культуры.

Общий план разработки:

1-й этап. Проектирование

2-й этап. Обсуждение.

3-й этап. Интеграция.

10. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

10.1 Значение нормативно-методического обеспечения

Нормативно-методическое обеспечение КСЗИ представляет собой комплекс положений законодательных актов, нормативов, методик, правил, регламентирующих создание и функционирование КСЗИ, взаимодействие подразделений и лиц, входящих в структуру системы, а также статус органов, обеспечивающих функционирование КСЗИ.

Нормативные документы, определяющие порядок защиты, должны удовлетворять следующим требованиям: соответствовать структуре, целям и задачам предприятия; описывать общую программу обеспечения безопасности, перечислять возможные угрозы информации и каналы ее утечки, определять ответственных за внедрение и эксплуатацию всех средств защиты; определять права и обязанности пользователей,

Прежде чем приступить к разработке документов, определяющих порядок ЗИ:

- нужно провести оценку угроз
- определить информационные ресурсы
- подумать, что необходимо для обеспечения их безопасности

10.2 Состав нормативно-методического обеспечения

Состав нормативно-методического обеспечения может быть определен следующим образом:

- законодательная база,
- руководящие методические документы
- информационно-справочная база.

К первому компоненту относятся: законы, указы Президента, постановления Правительства, кодексы, ГОСТы.

Во второй компонент могут входить документы министерств и ведомств (ФСТЭК, ФСБ), документы, разработанные на предприятиях по вопросам защиты информации.

Нормативно-методическая документация должна содержать следующие вопросы защиты информации:

- какие информационные ресурсы защищаются;
- какие программы можно использовать на служебных компьютерах;
- что происходит при обнаружении нелегальных программ или данных;
- дисциплинарные взыскания и общие указания о проведении служебных расследований;
- на кого распространяются правила;
- кто разрабатывает общие указания;
- точное описание полномочий и привилегий должностных лиц; кто может предоставлять полномочия и привилегии;
- порядок предоставления и лишения привилегий в области безопасности; полнота и порядок отчетности о нарушениях
- безопасности и преступной деятельности; особые обязанности руководства и служащих по обеспечению безопасности;
- объяснение важности правил (пользователи, осознающие необходимость соблюдения правил, точнее их выполняют),
- дата ввода в действие и даты пересмотра; кто и каким образом ввел в действие эти правила.

План защиты информации может содержать следующие сведения:

- назначение ИС

- перечень решаемых ИС задач
- конфигурация
- характеристики и размещение технических средств и программного обеспечения;
- перечень категорий
- информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в ИС;
- требования по обеспечению доступности, конфиденциальности, целостности различных категорий информации;
- список пользователей и их полномочий по доступу к ресурсам системы;
- цель защиты системы и пути обеспечения безопасности ИС и циркулирующей в ней информации;
- перечень угроз безопасности ИС, от которых требуется защита, и наиболее вероятных путей нанесения ущерба;
- основные требования к организации процесса функционирования ИС и мерам обеспечения безопасности обрабатываемой информации;
- требования к условиям применения и определение зон ответственности установленных в системе технических средств защиты от НСД;
- основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности ИС (особые обязанности должностных лиц ИС);
- цель обеспечения непрерывности процесса функционирования ИС, своевременность восстановления ее работоспособности и чем она достигается;
- перечень и классификация возможных кризисных ситуаций;
- требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов и т. п.);
- обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования системы;
- разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;
- определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;
- определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т. п.);
- определение порядка разрешения споров в случае возникновения конфликтов.

Полномочиями по отнесению сведений к государственной тайне обладают следующие органы государственной власти и должностные лица:

1. Палата Федерального собрания.
2. Президент Российской Федерации.
3. Правительство РФ.
4. Органы государственной власти РФ, органы государственной власти субъектов РФ и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий.
5. Органы судебной власти.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет.

Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.

Коммерческой тайной предприятия может быть все, что не запрещено законом или иными правовыми актами, охраняется предприятием и имеет ценность для предпринимательской деятельности, давая преимущество перед конкурентами, не владеющими ею.

Документы предприятия, регулирующие отношения с государством и с коллективом сотрудников на правовой основе:

- устав предприятия
- трудовые договоры
- правила внутреннего трудового распорядка
- должностные обязанности

Для предприятия необходимо:

Внести в устав следующие дополнения

Разработать «Перечень сведений, составляющих коммерческую тайну».

Начало работы по защите коммерческой тайны связано с разработкой перечня сведений, составляющих коммерческую тайну.

На первом этапе работы комиссия на основе анализа всех направлений деятельности предприятия должна установить весь состав циркулирующей на предприятии информации

На втором этапе определяется, какая из установленной информации должна быть конфиденциальной и отнесена к коммерческой тайне.

Также следует заметить, что нецелесообразно относить информацию к коммерческой тайне, если затраты на ее защиту превысят количественные и качественные показатели преимуществ, получаемых при ее защите.

Политика по сохранению коммерческой тайны реализуется путем максимального ограничения круга лиц, физической сохранности документов, содержащих такие сведения, внесения требований по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами и других мер по решению руководства.

Защита и обработка конфиденциальных документов предусматривает:

• порядок определения информации, содержащей коммерческую тайну, и сроков ее действия;

• систему допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну;

• обеспечение сохранности документов на различных носителях с грифом конфиденциальности;

• обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну;

• принципы организации и проведения контроля за обеспечением режима при работе со сведениями, составляющими коммерческую тайну;

• ответственность за разглашение сведений, утрату документов, содержащих коммерческую тайну.

11 УПРАВЛЕНИЕ КОМПЛЕКСНОЙ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

информации об этом объекте может быть получено от различных групп людей:

имеющих опыт управления предприятием и представляющих его цели и задачи, но не знающих досконально особенностей функционирования объекта информатизации;

б) знающих особенности функционирования объекта информатизации, но не имеющих полного представления о его целях;

в) знающих теорию и практику организации защиты, но не имеющих четких представлений о целях, задачах и особенностях функционирования объекта информатизации как системы в целом и т. П

Если же такого аналога найти не удается, на помощь приходят здравый смысл и интуиция, частично дополняемые известными методами проектирования организационных структур управления, среди которых наибольшее распространение получили

- системный подход,
- нормативный метод,
- метод параметрического моделирования,
- метод функционального моделирования
- программно-целевой метод

сложной системы разбивается на два этапа:

- внешнее (или макро-) Этап внешнего проектирования складывается из подэтапов анализа и синтеза. На первом подэтапе формулируется цель разрабатываемой системы, проводится изучение существующей системы, составляется генеральная схема будущей системы. На втором этапе последовательно выполняется эскизное, техническое и рабочее проектирование системы.
- внутреннее (или микро-) проектирование

То есть в КСЗИ должно быть предусмотрено два вида функций:

• основной целью которых является создание механизмов защиты;

• осуществляемые с целью непрерывного и оптимального управления механизмами защиты.

Общая цель управления - обеспечение максимально возможной эффективности использования ресурсов.

Задачи управления:

1. Обеспечение заданного уровня достижения цели при минимальном уровне затрат.
2. Обеспечение максимального уровня достижения цели при заданном уровне затрат.

Технология управления должна быть разработана так, чтобы обеспечить:

• комплексную автоматизацию;

• единство органов, средств и методов управления;

• максимальную автоматизацию

В соответствии с этим сформулируем требования к технологии управления:

1. Обеспечение разделения труда
2. Максимальная формализация всех трудовых процессов
3. Регламентация взаимодействия работников органов управления между собой и средствами автоматизации
4. Обеспечение психологических совместимостей
5. Повышение исполнительной дисциплины

Первым шагом построения технологии управления, удовлетворяющей современным требованиям, является структуризация основных процессов управления, т. е. схематизация объектов, процессов или явлений до степени однозначного определения каждого элемента.

Элемент процесса или явления считается структурированным, если он удовлетворяет следующим условиям:

- однозначности
- четкости
- простоте внутренней организации объекта
- простоте изучения
- модульности
- гибкости
- доступности

Поэтому под структурированной технологией управления будем понимать управляемую совокупность приемов, правил и методов осуществления всех процессов управления.

Основные критерии построения и рационализации технологии управления:

- выполнение всех процедур управления в полном объеме
- максимально эффективное информационное обеспечение
- максимальная автоматизация

Требования, предъявляемые к системам управления, по которым можно судить о степени организованности систем:

• детерминированность элементов;

• динамичность системы;

• наличие в системе управляющего параметра; Управляющим параметром в системе управления следует понимать такой ее параметр (элемент), посредством которого можно управлять деятельностью всей системы и ее отдельными элементами. Таким параметром (элементом) в социально управляемой системе является руководитель подразделения данного уровня.

Внешнюю информацию воспринимает руководитель организации, который организует работы по выполнению поручения, распределяет задания в соответствии с должностными инструкциями при наличии условий, необходимых для выполнения поручений.

• наличие в системе контролирующего параметра; контролировал бы состояние субъекта управления, не оказывая при этом на него (или на любой элемент системы) управляющего воздействия. Любые управленческие решения в системе управления должны проходить только через элемент, выполняющий функции контролирующего параметра

• наличие в системе каналов (по крайней мере, одного) обратной связи.

В структуре управления предприятием должен быть отдел совершенствования структуры управления.

11.2 Планирование деятельности

Вся сложная совокупность управленческих действий может быть сведена к перечню функций, составляющих замкнутый цикл управления:

• принятие управленческого решения;

• реализация решения;

• контроль

- Планирование является первым шагом в цикле управления. Планирование как функция управления имеет сложную структуру и реализуется через свои подфункции: прогнозирование, Прогнозирование должно обеспечить решение следующих задач:
  - •научное предвидение будущего на основе выявления тенденций и закономерностей развития;

• определение динамики экономических явлений;

• определение в перспективе конечного состояния системы ее переходных состояний, а также ее поведения в различных ситуациях на пути к заданному оптимальному режиму функционирования.

- Моделирование, Важное условие прогнозирования - моделирование различных ситуаций и состояний СЗИ в течение планируемого периода.
- программирование. Задача программирования - исходя из реальных условий функционирования системы, запрограммировать ее переход в новое заданное состояние.

Назначение планирования как функции управления состоит в стремлении заблаговременно учесть по возможности все внутренние и внешние факторы, обеспечивающие благоприятные условия для нормального функционирования и развития предприятия.

Обобщенные цели планирования регламентируют общий целевой подход в процессе разработки плана, а именно выделяются две постановки целей:

• задан результат, который должен быть достигнут при минимальном расходе ресурсов;
• заданы ресурсы и при заданных ресурсах необходимо достичь максимального результата.

Формы планирования в зависимости от длительности планового периода:

а) перспективное планирование (на 5 лет и более). При данном виде планирования нет ограничений по ресурсам; Особенностями перспективного планирования являются:

• совершенствование концепции управления ЗИ
• изменение структурного построения СЗИ, режимов их функционирования и технологических схем;
• обосновываться требования к совершенствованию концепции построения и использования системы защиты
• учитывают возможные условия изменения внешней среды.

б) **среднесрочное планирование** (от 1 до 5 лет). При таком планировании есть резерв ресурсов;

• Особенностями среднесрочного планирования являются:
• основные цели - рациональное использование в планируемый период имеющихся средств и методов ЗИ, а также обоснование предложений по развитию этих средств и методов;
• структура СЗИ, как правило, изменению не подлежит
• при необходимости могут и должны разрабатываться предложения по совершенствованию СЗИ

в) **текущее (рабочее)** планирование (от 1 мес. до 1 года). Используются только имеющиеся ресурсы. При текущем планировании:

• основной целью является рациональное использование имеющихся средств обеспечения защиты
• структура и режимы функционирования системы защиты изменению не подлежат. Могут производиться лишь незначительные изменения технологии управления СЗИ;
• предложения по включению в состав системы управления защитой новых средств

Поскольку оценка перспектив неопределенна, перспективное планирование не может быть ориентировано на достижение количественных показателей

Среднесрочные планы содержат количественные показатели

Основными звеньями текущего плана являются календарные планы (месячные, квартальные, полугодовые)

общими принципами управления, которые и должны быть положены в основу планирования:

1) директивность
2) преемственность
3) конкретность
4) гибкость
5) проблемность

6) комплексность
7) экономичность

Планирование может быть организовано разными способами.

1. Анализ.
2. Синтез.
3. Итерация

На определение сроков осуществления намеченных мероприятий влияют прошлый опыт их реализации, трудоемкость, условия, в которых они будут выполняться, подготовленность исполнителей. Содержание мероприятия должно включать: желаемый результат, краткую программу действий, планируемые к использованию силы и средства, срок исполнения.

Мероприятия в плане следует систематизировать по следующим четырем разделам: 1) организационно-методическая работа; 2) контрольно-проверочная работа; 3) профилактическая работа; 4) работа с кадрами.

В процессе планирования должны быть выделены следующие стадии.

1. Обоснование целей и критериев:
   • формулирование целей,
   • выбор критериев
2. Анализ условий
3. Формирование задач
4. Анализ ресурсов
5. Согласование целей, задач, условий, ресурсов
6. Определение последовательности выполнения задач
7. Определение методов контроля выполнения планов
8. Определение порядка корректировки планов.

Таким образом, можно сделать следующие основные выводы:

• планирование является неотъемлемой частью деятельности КСЗИ, как и деятельности любых других систем;

• от рационального планирования зависит эффективность деятельности КСЗИ, а также принятие решений в экстремальных ситуациях.

11.3 Контроль деятельности

Цель контроля - выявить слабые места системы, допущенные ошибки, своевременно исправить их и не допустить повторения.

Процесс контроля включает три стадии:

1. Установление фактического состояния СЗИ.
2. Анализ сравнения фактического положения с заданным
3. Разработка мероприятий по улучшению и корректировке

Основными задачами контроля являются:

1. Определение обоснованности и практической целесообразности проводимых мероприятий по ЗИ.
2. Выявление фактического состояния СЗИ в данный период времени
3. Установление причин и обстоятельств отклонений показателей качества, характеризующих СЗИ, от заданных.
4. Изучение деловых качеств и уровня профессиональной подготовки лиц, осуществляющих ЗИ.

Меры контроля:

- Организационных. Организационные меры контроля включают:

1) проверку выполнения сотрудниками требований по обеспечению сохранности КТ
2) проверку выполнения пропускного режима

3) проверку выполнения сотрудниками правил работы с конфиденциальными документами
4) проверку наличия защищаемых носителей конфиденциальной информации

- технических мероприятий

Могут применяться следующие виды контроля:

• предварительный; Предварительный контроль обычно реализуется в форме определенной политики, процедур и правил. Прежде всего, он применяется по отношению к трудовым, материальным и финансовым ресурсам.

• текущий; Текущий контроль осуществляется, когда работа уже идет и обычно производится в виде контроля работы, подчиненного его непосредственным начальником.

• заключительный. Заключительный контроль осуществляется после того, как работа закончена или истекло отведенное для нее время.

Периодический контроль (ежедневный) проводится сотрудниками предприятия в части проверки наличия носителей информации, с которыми они работают.

Негласный контроль осуществляется с целью объективной оценки уровня ЗИ и, прежде всего, выявления слабых мест в СЗИ, психологическое воздействие на сотрудников

12 УПРАВЛЕНИЕ КСЗИ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

12.1 Понятие и виды чрезвычайных ситуаций

Все ситуации, возникающие в процессе функционирования, можно условно разделить на две группы:

- Нормальные
- ненормальные.
  - Аварийные
  - потенциально аварийные
  - нештатные

Любая из этих ситуаций требует принятия ответных мер, направленных:
• на сокращение комплекса факторов, влияющих на возникновение чрезвычайной ситуации;
• защиту людских, информационных, материальных и других ресурсов от негативного воздействия, нанесения ущерба и уничтожения;
• обеспечение работы объекта во время нештатной ситуации и после нее.

Чрезвычайную ситуацию (ЧС) можно определить, как комплекс событий, проявление и протекание которых могут привести к нарушению нормального функционирования КСЗИ либо создать условия для проявления различных форм уязвимости защищаемой информации.

Чрезвычайные ситуации можно классифицировать личным признакам.

1. По масштабам сферы действия:
   • межгосударственные;
   • общегосударственные;
   • местные;
   • объектовые
2. По виду наносимого ущерба:
   • с прямым ущербом;
   • с косвенным ущербом;
   • представляющие угрозу жизни людей;
   • приводящие к нарушению экологического равновесия, уничтожению материальных ресурсов и т. д
3. . По времени и динамике развития:
   • стратегические, приводящие к катастрофическим последствиям;
   • медленнотекущие;

• оперативного плана, с выраженной динамикой развития.

4. По вероятности возникновения:
   • прогнозируемые;
   • трудно прогнозируемые;
   • непрогнозируемые.
5. По степени сложности при ликвидации последствий:
   • легкоустранимые;
   • требующие определенных временных и ресурсных затрат для их ликвидации;
   • трудно устранимые;
   • требующие особых средств и мероприятий для ликвидации их последствий.

12.2 Технология принятия решения в условиях чрезвычайной ситуации

Контрмеры должны быть приняты срочно, однако обычный
порядок не позволяет это сделать по ряду причин:

• существующие планы работы не соответствуют новой ситуации;
• возникают новые задачи;
• информация, которую следует изучить и проанализировать, поступает мощным потоком.

Инициатива снизу, часто повышающая в обычных условиях эффективность принимаемых решений, в условиях ЧС теряет свою действенность и может оказаться небезопасной.

Таким образом, система управления ЧС должна функционировать в следующих четырех режимах:

• повседневной деятельности; Режим характеризуется отсутствием информации о явных признаках угрозы возникновения ЧС. Задача системы управления ЧС в стационарных условиях (повседневных) состоит в противоаварийном упреждающем планировании, основными целями которого являются сбор информации для прогнозирования возможного развития ЧС и контроля ее последствий, ресурсов, необходимых для их ликвидации, разработка специальных прогнозов

• повышенной готовности (активная подготовка и осуществление превентивных мероприятий); Второй режим повышенной готовности характеризуется наличием информации о признаках потенциальной угрозы возникновения ЧС. Задачами системы управления ЧС в этом режиме являются разработка и осуществление детальных планов мероприятий по предупреждению либо смягчению последствий ЧС на основе заранее подготовленных сценариев

• чрезвычайный (действия в чрезвычайных ситуациях); Чрезвычайный режим характеризуется обстоятельствами, совокупность которых определяется как чрезвычайная ситуация. Задачей системы управления ЧС в этом режиме является осуществление оперативных действий по защите объектов различного типа.

• постчрезвычайный режим (ликвидация долговременных последствий ЧС). Режим ликвидации последствий ЧС характеризуется отсутствием активных поражающих фактов ЧС и необходимостью про ведения мероприятий по восстановлению нормативного функционирования объекта. Задачей системы управления ЧС в этом режиме является оперативное и долгосрочное планирование действий по смягчению или полной ликвидации последствий ЧС.

12.3 Факторы, влияющие на принятие решения

Основными причинами запаздывания ответных действий являются:

1. Инерционность информационной системы
2. Необходимость проверки и подтверждения достоверности информации о возникновении ЧС
3. Психологические особенности человека

Решения в условиях ЧС принимаются в различной оперативной обстановке, включая кризисную, и в крайне ограниченное время. Однако оно должно:

- быть принято своевременно,
- быть максимально обоснованным
- обеспечивать наиболее полное и эффективное использование имеющихся возможностей.

На ранних стадиях потенциальной опасности ЧС ответные меры, очевидно, должны быть общего характера, направленные на увеличение стратегической гибкости организации.

12.4 Подготовка мероприятий на случай возникновения чрезвычайной ситуации

Для решения задач предупреждения, нейтрализации (локализации) и ликвидации последствий ЧС на предприятии создаются специальные структуры. Среди них выделяют

- кризисные группы,
- штабы,
- службы обеспечения защиты в условиях ЧС,
- оперативные бригады

Обязанности рассматриваемой структуры (штаб, кризисная группа):

• выявление тенденций развития ЧС;
• оценка масштабов ее негативного воздействия и последствий;
• расчет времени и ресурсов, необходимых для локализации и ликвидации
• сбор, обработка и предоставление необходимой информации для руководителей

Необходимо проводить различные тренинги, комплексы учебных занятий, которые позволили бы подготовить персонал