1 Выбрать компоненты, составляющие объект информатизации

Правильные ответы: биосоциальные системы, серверное помещение, компьютерные системы и помещения, в которых они расположены, периферийные устройства, machine learning, программное обеспечение рабочих станций

2 Выберите правильные утверждения

Правильные ответы: Наиболее подходящими технологиями для построения корпоративных ИС являются экстранет и интранет, Проблемы защиты информации обостряются, когда компании делают внутренние базы данных доступными для внешних пользователей, Через информационную систему должен проходить только авторизованный трафик, Веб-технологии при всех своих значительных преимуществах вносят и новые проблемы для корпоративных ИС

3 Основные особенности современного предприятия

Правильные ответы: Многоаспектность функционирования, Высокая техническая оснащенность, Возрастание степени безбумажных технологий обработки информации, Непосредственный и одновременный доступ к ресурсам ИС

4 Критерии эффективности КСЗИ характеризуют

Правильные ответы: Физический смысл, Количественную оценку

5 Выбрать процессы, связанные с разработкой и реализацией политики безопасности

Правильные ответы: Оценка соответствия эталону, Разработка документов, Статистика по событиям безопасности, Анализ рисков

6 Подсистема защиты информации от НСД включает подсистемы

Правильные ответы: Регистрации и учета, Обеспечения целостности

7 Подсистема обнаружения и предотвращения вторжений обеспечивает предотвращение на

Правильные ответы: Сетевом уровне, Системном уровне DDoS .

8 Выбрать состав научно-методологических основ КСЗИ

Правильные ответы: Положения теории систем, Законы кибернетики, Методы моделирования больших систем

9 КСЗИ основана на совместном применении следующих мер и средств защиты:

Правильные ответы: Мониторинг сетевой активности, Межсетевое экранирование, Централизованный аудит, Эшелонирование защиты

10 Отметьте управленческо-аналитические мероприятия в КСЗИ корпоративной ИС

Правильные ответы: Управление рисками, Управление политиками безопасности, Следование законодательным требованиям

11 Из конфиденциальной информации защите подлежит

Правильный ответ: вся конфиденциальная информация

12 Открытая информация должна защищаться от

Правильные ответы: Хищения, Разрушения, Нарушения целостности, Уничтожения

13 Выберите виды тайны, установленные правовыми документами Российской Федерации

Правильные ответы: тайна частной жизни, тайна переписки, военная тайна, банковская тайна, личная тайна, семейная тайна

14 Нарушителей классифицируют по

Правильные ответы: уровню знаний, уровню возможностей, времени действия

15 Информация в зависимости от категории доступа к ней подразделяется на:

Правильные ответы: ограниченного доступа, общедоступную

16 «Информация» это:

Правильный ответ: сведения (сообщения, данные) независимо от формы их представления

17 «Обладатель информации» это:

Правильный ответ: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

18 Субъектами доступа могут являться:

Правильные ответы: пользователи, процессы

19 Угроза безопасности информации это:

Правильный ответ: совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу

20 “Технический канал утечки информации” это

Правильный ответ: совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация

21 Техническими каналами утечки информации, приводящими к возникновению угроз безопасности информации являются:

Правильные ответы: утечки акустической (речевой) информации, утечки видовой информации, утечки информации по каналам побочных электромагнитных излучений

22 Несанкционированный доступ к информации может быть осуществлён путём:

Правильные ответы: Хищения носителей защищаемой информации, Подключения к техническим средствам и системам объекта информатизации

23 По признаку отношений к природе возникновения угрозы классифицируются, как:

Правильные ответы: Объективные, Субъективные

24 Уязвимость информационной системы это:

Правильный ответ: слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации

25 Источниками угроз НСД к информации являются:

Правильные ответы: аппаратные элементы компьютера , внутренние нарушители, внешние нарушители , аппаратные закладки

26 Реализация технического канала утечки информации может привести к нарушениям:

Правильный ответ: Конфиденциальности информации

27 Реализация НСД может привести к нарушениям:

Правильные ответы: Целостности информации, Доступности информации, Аутентичности информации, Конфиденциальности информации

28 Методами и способами защиты информации от НСД являются:

Правильные ответы: использование сертифицированных средств защиты информации, организация физической защиты помещений, учет и хранение съемных носителей информации

29 Внутренним нарушителем на предприятии может быть лицо из следующих категорий персонала

Правильные ответы: начальник отдела организации, сотрудник организации, администратор безопасности, охранник аутсорсинговой компании

30 Указать стадии творческого мышления, связанные с основными этапами информационной работы

Правильные ответы: накопление знаний и сведений, анализ материала, умозаключение и выводы

31 В модели отношений доступа и действий:

Правильные ответы: целью моделирования является выявление множества отношений доступа и действий, их допустимость и определенные возможности НСД к информации с помощью допустимых (разрешенных) преобразований первоначальных прав, предметом анализа являются отношения доступа между элементами системы и действий определенного элемента по отношению к другим элементам

32 Организационная модель КСЗИ показывает:

Правильные ответы: состав подразделений, подчиненность в управленческой иерархии, взаимосвязь подразделений

33 На этапе разработки технического проекта КСЗИ выполняются следующие действия

Правильный ответ: Разработка и обоснование всех проектных решений

34 Структурно-функциональная схема САПР защиты информации может быть представлена в виде основных модулей:

Правильные ответы: типовая сетевая модель процесса создания СЗИ, модули расчета параметров подсистем СЗИ, модуль выбора стандартных средств и типовых проектных решений

35 Модель, отображающая состав, содержание и взаимосвязи тех функций, осуществление которых достигается целью деятельности моделируемых систем – это

Правильный ответ: функциональная модель

36 В имитационной модели системы защиты:

Правильные ответы: делается оценка влияния разного рода параметров систем обработки информации и внешней среды на безопасность, изучается влияние на безопасность таких событий, которые нельзя наблюдать в реальных условиях

37 Методы удовлетворения потребностей в уважении

Правильные ответы: предлагать подчиненным более содержательную работу, продвигать подчиненных по карьерной лестнице

38 Критерием оптимизации плана системы защиты информации (СЗИ) может быть

Правильные ответы: минимизация затрат на реализацию СЗИ в АС при условии обеспечения заданных уровней защищенности информации от НСД со стороны всех вероятных стратегий нападения, минимизация затрат на реализацию СЗИ в АС при условии обеспечения приемлемых уровней защищенности информации от НСД со стороны всех вероятных стратегий нападения

39 Наиболее влиятельные характеристики на организацию КСЗИ

Правильные ответы: Характер деятельности, Экономическое состояние

40 Подсознательного неприятия или даже открытого противодействия политике безопасности можно избежать если

Правильные ответы: своевременно провести тщательное наблюдение, в ходе которого должен быть выявлен преобладающий тип корпоративной культуры каждого структурного подразделения,, определить неформальных лидеров, выявить наиболее авторитетные субкультуры, значительно влияющие на внутреннюю жизнедеятельность организации

41 Выделить виды адаптации работника на предприятии

Правильные ответы: К трудовой деятельности, Социально-психологическая, Социально-организационная

42 Причины нарушений безопасности сотрудниками предприятия, лежащие в кадровой сфере:

Правильные ответы: злой умысел, корыстный интерес, самоутверждение, текучесть кадров, отрицательное психическое воздействие

43 Профессиональный кодекс корпоративного поведения:

Правильный ответ: описывает профессиональные этические дилеммы, нормы и стандарты поведения

44 Организационная система (ОС) состоит из следующих элементов:

Правильные ответы: решающие, исполнительные, руководящие

45 Формирование позитивной корпоративной культуры с учетом специфики безопасности затрагивает изменение таких существенных представлений, как

Правильные ответы: внутренний психологический климат коллектива, устоявшиеся образцы поведения, совокупность формальных и неформальных требований к персоналу в виде норм

46 Выбрать типы организационной структуры (ОС)

Правильные ответы: Программно-целевая, Функциональная, Линейно-штабная

47 Указать недостатки аналитической модели

Правильные ответы: невозможность построения для всех случаев соответствующей расчетной модели, сложность учета влияния большого числа разнородных факторов, отсутствие представительной выборки необходимых статистических данных, нестационарный характер ряда показателей

48 В концептуальных моделях КСЗИ

Правильные ответы: анализируется совокупность возможных угроз для системы, каналов доступа к информации, уязвимых мест, определяется общая стратегия защиты , принимаются решения о составе и структуре системы защиты

49 Функциями для управления механизмом непосредственной защиты в функциональной модели являются

Правильные ответы: Оперативно-диспетчерское управление, Обеспечение повседневной деятельности

50 Указать типы моделей

Правильные ответы: цифровые, вербально-описательные, кибернетические, материальные

В информационной модели циркулирует несколько видов информации:
1) корреспонденция;
2) техническая документация;
3) периодика (журналы и проч.);
4) книги;
5) фактографическая быстроменяющаяся информация;
6) фактографическая медленноменяющаяся информация (исходная и регламентная);
7) фактографическая постоянная информация.
Информация циркулирует в информационной модели в несколько этапов:
l-й этап: генерирование информации;
2-й этап: ввод в систему обработки;
3-й этап: передача информации;
4-й этап: прием, хранение, накопление информации;
5-й этап: поиск информации;
б-й этап: функциональная переработка информации;
7-й этап: выдача информации для использования.

Организационная модель КСЗИ. Указанная модель **показывает состав, взаимосвязь и подчиненность в управленческой иерархии подразделений, входящих в состав КСЗИ**.

На построение данной модели влияет множество факторов различной природы: специфика задач, решаемых функциональными подразделениями, принципы и методы, выбранные в данной системе управления, технология реализации основных функций, кадровый состав сотрудников и др. По своим разновидностям все модели могут быть разделены на следующие группы:

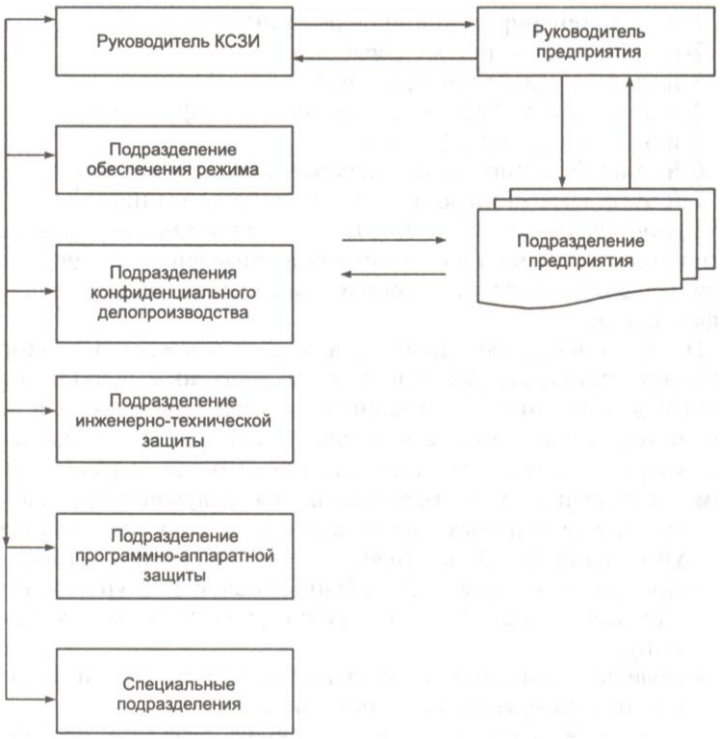

Рисунок 7.1 - Организационная модель КСЗИ

- модели, в которых организационная структура системы управления КСЗИ построена по линейному принципу;
- модели, в которых организационная структура системы управления КСЗИ построена по функциональному принципу;
- модели, в которых организационная структура построена по линейно-функциональному принципу;
- модели, в которых организационная структура построена по матричному типу.

Данная модель (**рисунок 71**) формируется с учетом структуры системы управления предприятия, где создается или функционирует КСЗИ, а также с учетом состава основных функций, осуществляемых в системе защиты.

Структурная модель. Она **отражает содержание таких компонентов КСЗИ, как кадровый, организационно-правовой и ресурсный.** При этом последний компонент представлен основными видами обеспечения: техническое, математическое, программное, информационное, лингвистическое. Организационно-правовой компонент представляет собой комплекс организационно-технических мероприятий и правовых актов, являющихся основой, регулирующей функционирование основных подсистем КСЗИ. Этот компонент играет связующую роль между кадровым и ресурсным. Таким образом, рассмотренные модели представляют архитектуру КСЗИ. Они отражают различные стороны проектируемого (анализируемого) объекта и сами образуют систему, как это показано в организационной модели.

8 ТЕХНОЛОГИЧЕСКОЕ ПОСТРОЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

8.1. Общее содержание работ

Система защиты информации характеризуется большим числом взаимодействующих между собой средств и многофункциональным характером решаемых с ее помощью задач. Чтобы такая сложная система эффективно функционировала, необходимо рассмотреть целый комплекс вопросов еще на стадии ее создания.

Для решения сложных проблем (экономических, социальных, политических, научных, технических), стоящих перед обществом, требуется организованная деятельность многих людей. Такая деятельность осуществляется в рамках искусственных (т. е. созданных человеком) формирований и называется организационной системой (ОС).

Решение сложных социально-экономических проблем требует скоординированных усилий многих людей и значительных затрат ресурсов. Кроме того, нужны знания (информация), без которых невозможно определить, какие средства и сколько их необходимо выделить для решения проблемы. При наличии необходимых знаний и средств (ресурсов) для решения проблем

разрабатывают комплекс мероприятий, реализация которых должна приводить к желаемому результату. В условиях ограниченности знаний и средств на решение проблемы ее разбивают на части (если это возможно) и решают по частям или поэтапно, постепенно приближаясь к цели. Для реализации намеченных мероприятий могут быть подготовлены специальное постановление, приказ, договор, либо разработана целевая комплексная программа. Если намеченный комплекс мероприятий невозможно реализовать с помощью указанных средств, для решения проблемы создается организационная система.

Как правило, 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. Некоторые из них принимают решения по организации только своих собственных действий - это исполнительные элементы. Элементы, принимающие решения по организации не только своих собственных действий, но и действий некоторых других элементов, объединенных или не объединенных в коллективы или организации, - это руководящие элементы системы».

Основным элементом любой ОС являются люди, условно разбиваемые на организаторов и исполнителей. «Работа организаторов есть управление и контроль над исполнением; работа исполнителей - физическое воздействие на объекты труда». Множество исполнителей с их орудиями труда образует объект управления (ОУ), множество организаторов (управленцев) вместе с информацией, техникой, специалистами и обслуживающим персоналом - субъект управления (СУ).

Четкую границу между ОУ и СУ провести невозможно, поскольку исполнительская деятельность немыслима без управленческой, а последняя без исполнительской бессмысленна, однако для целей построения ОС такое разделение является полезным.

С понятием ОС тесно связано понятие «деятельность», так как основная задача ОС заключается в том, чтобы координировать и осуществлять деятельность людей, направленную на решение проблемы. В связи с этим деятельность можно определить как осознанное и направленное на решение проблемы поведение людей. Понятие «деятельность» будем относить не только к отдельному человеку или группе людей, но и к ОС в целом.

Каждая ОС выполняет множество видов деятельности (основной или обеспечивающей). Для того чтобы скоординировать различные виды деятельности с целью удовлетворения некоторой общественной потребности (проблемы), как правило, требуется установить информационные и деловые связи с ОС, осуществляющими эту деятельность. Образно говоря, координатора можно сравнить с дирижером оркестра. При этом оркестр может рассматриваться как ОС, дирижер - как СУ, а множество исполнителей - как ОУ.

Наряду с СУ и ОУ в ОС могут включаться обеспечивающие подсистемы, выполняющие вспомогательную деятельность: снабжение, ремонт, информационное обслуживание, энергообеспечение и др.

Каждая ОС построена по иерархическому принципу. Наибольшее распространение получили линейная, функциональная, линейно-штабная и программно-целевая (матричная) структуры.

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).

Этап 1. Постановка проблемы, которую требуется решить.

Этап 2. Исследование проблемы: сбор и анализ всех доступных объективных данных и знаний о проблеме и факторах, влияющих на ее решение, формирование банка проблемных знаний, построение и исследование модели проблемы (если проблема допускает модельное представление).

Этап 3. Определение границ (состава) проблемного объекта, т. е. всех потенциальных участников решения проблемы (организаций, коллективов и лиц, от деятельности которых зависит ее решение).

Этап 4. Обследование проблемного объекта. Проводится обследование ОС, входящих в состав проблемного объекта, и выбирается комплекс мер по решению проблемы. На этом этапе формируется план мероприятий (или целевая комплексная программа) по решению проблемы и решается вопрос о целесообразности создания ОС.

Этап 5. Выбор критерия эффективности ОС. На этом этапе начинается собственно разработка будущей ОС. Выбор критерия эффективности системы дает возможность в дальнейшем объективно оценивать альтернативные проекты ОС.

Этап 6. Выбор границ (состава) ОУ. Из всех потенциальных участников решения проблемы отбираются те, кто войдет в состав ОУ проектируемой ОС.

Этап 7. Обследование ОУ. Проводится углубленное обследование организаций, входящих в состав ОУ, с целью получения данных, необходимых для формирования альтернативных вариантов построения СУ и ОС в целом.

Этап 8. Разработка технического задания на создание ОС. Производится выбор наиболее эффективного варианта построения ОС и разработка технического задания.

Этап 9. Техническое и рабочее проектирование ОС.

Этап 10. Внедрение ОС.

Эти этапы не обязательно должны быть строго последовательными. На каждом из них допускается возврат к одному из предыдущих. В зависимости от особенностей проблемы и условий ее решения возможно объединение нескольких этапов в один или пропуск отдельных этапов. Например, если границы ОУ совпадут с границами проблемного объекта, то этап 7 может быть опушен. Этап 3 может быть объединен с этапом 4, этап 6 - с этапом 7 и т.д.

Предлагаемая технологическая схема имеет рекомендательный, а не обязательный характер и требует в каждом конкретном случае уточнения в зависимости от специфики решаемой проблемы.

Наряду с органами, осуществляющими управление по вертикали, создаются дополнительные органы, призванные обеспечивать управление по горизонтали.

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.

Поскольку форма производственных отношений всегда соответствует конкретной социально-экономической обстановке, процессы защиты должны рассматриваться с учетом этих условий.

Поскольку процессы защиты находятся во взаимосвязи и взаимодействии, при их исследовании обязателен комплексный подход, требующий исследования и учета внешних и внутренних отношений всей совокупности потенциальных угроз.

И наконец, системный подход - его задачей является оптимизация всей системы в совокупности, а не улучшение эффективности отдельных частей. Это объясняется тем, что, как показывает практика, улучшение одних параметров часто приводит к ухудшению других, поэтому необходимо стараться обеспечить баланс противоречивых требований и характеристик.

Для каждой системы должна быть сформулирована цель, к которой она стремится. Эта цель может быть описана как назначение системы, как ее функция. Чем точнее и конкретнее указано назначение или перечислены функции системы, тем быстрее и правильнее можно выбрать лучший вариант ее построения.

Так, например, цель, сформулированная в самом общем виде как обеспечение безопасности объекта, заставит рассматривать варианты создания глобальной системы защиты. Если уточнить ее, определив, например, как обеспечение безопасности информации, передаваемой по каналам связи внутри здания, то круг возможных технических решений существенно сузится.

Следует иметь в виду, что, как правило, глобальная цель достигается через достижение множества менее общих локальных целей (подцелей). Построение такого «дерева целей» значительно облегчает, ускоряет и удешевляет процесс создания системы.

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.

Перечень направлений комплексного проектирования определяется в зависимости от нужд конкретного предприятия и поставленных перед проектом задач и условий. Соответственно, при локальном проектировании круг задач сужается, и проект может быть ограничен разработками по одному из направлений. Но локальные проекты должны осуществляться как части комплексного проекта, последовательно реализуемые в ходе работы. Иначе внедрение проекта может привести к отрицательным результатам.

Можно выделить также индивидуальное и типовое проектирование. Индивидуальное представляет собой разработку проекта для какого-нибудь конкретного предприятия с учетом его специфических особенностей, условий и требований.

Типовые проекты преследуют цель унификации и стандартизации процессов защиты на различных предприятиях.

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.**

Поскольку системы обеспечения безопасности имеют определенную специфику по сравнению с другими системами, содержание некоторых этапов может отличаться от рекомендованного. Тем не менее, общая концепция сохраняется неизменной. Рассмотрим последовательность выполняемых работ.

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.**

Технико-экономическое обоснование должно согласовываться со всеми организациями и службами, ответственными за обеспечение безопасности, и утверждаться лицом, принимающим решения.

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.

В состав рабочей документации входят спецификация оборудования и материалов; схемы размещения технических средств системы защиты (охранно-пожарной сигнализации, охранного телевидения, охранного освещения и т. п.); схемы прокладки кабельной связи системы защиты; схемы прокладки электропитания системы защиты.

Каждая система защиты уникальна, поэтому документация, как правило, строго индивидуальна и зависит не только от типа и размера объекта защиты, но и от возможностей и опыта заказчика, который будет ее эксплуатировать.

Поскольку документация содержит конфиденциальные сведения, круг лиц, допущенных к ознакомлению и работе с ней, должен быть ограничен.

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.

Все эти работы начинаются только после утверждения всех документов и выделения финансовых средств. Разработчик системы защиты проводит техническое и коммерческое сравнение всех предложений от конкурирующих фирм-изготовителей защитного оборудования, после этого выбирает поставщика, заключает договор на поставку оборудования и оплачивает его.

При получении оборудования желательно сразу проводить его проверку на соответствие сопроводительным документам и техническим условиям, а также (если это возможно) проверку работоспособности в условиях эксплуатации.

Все работы по монтажу и отладке системы защиты должны выполнять специалисты. Силами заказчика можно выполнять только специфические и небольшие по трудозатратам работы, такие, как, например, установка скрытого теленаблюдения, перенос датчиков охранной сигнализации, ремонт системы радиосвязи и т. п. Желательно, чтобы в монтаже и настройке защитных систем участвовали те сотрудники службы охраны объекта, которые будут их эксплуатировать.

После окончания работ и испытаний необходимо уточнить все вопросы гарантийного и послегарантийного обслуживания системы защиты.

В разработке системы могут принимать участие несколько групп разработчиков, каждая из которых объединяет специалистов определенного профиля. Так, например, в разработке проектных решений в зависимости от стадии проектирования, особенностей объекта и видов защиты могут участвовать специалисты по охранно-пожарной сигнализации и охранному телевидению, системам связи и коммуникациям, общестроительным и монтажным работам и т. п. Поэтому важнейшая задача организации создания системы безопасности состоит в четком распределении функций и в согласовании выполняемых работ. **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

Идеология разрабатываемой системы, стратегические вопросы ее функционирования должны быть согласованы и утверждены высшим руководством заказчика.

Создание у заказчика группы, задачей которой является осуществление контакта с разработчиками, курирование разработки, утверждение и оперативная корректировка планов работы, выделяемых финансовых ресурсов, является крайне необходимым условием. Без создания такой группы, обладающей достаточным авторитетом и необходимыми полномочиями, разработка системы заранее обречена на неудачу. Но и при наличии такой группы результат будет неудовлетворительным, если ее руководитель не является квалифицированным и полномочным представителем заказчика.

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.

Каждое предприятие уникально. Поэтому и система защиты конкретного предприятия тоже уникальна. Тем не менее, можно' перечислить основные параметры предприятия и показать, каким образом они могут оказывать влияние на разрабатываемую комплексную систему защиты информации:

• **характер деятельности предприятия - на организационно-функциональную структуру КСЗИ, ее состав; состав и структуру кадров СЗИ, численность и квалификацию ее сотрудников; техническое обеспечение КСЗИ средствами защиты; 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.**

Организация КСЗИ на конкретном предприятии зависит от параметров рассмотренных характеристик данного предприятия. Эти характеристики определяют цели и задачи КСЗИ, объем ее материального обеспечения, состав и структуру КСЗИ, состав технических средств защиты, численность и квалификацию сотрудников СЗИ и т. д. Однако **степень воздействия различных характеристик предприятия на организацию КСЗИ различна**. Из числа **наиболее влиятельных** можно выделить следующие:

- **характер деятельности предприятия;**
- **состав защищаемой информации, ее объем, способы представления и отображения;**
- **численный состав и структуру кадров предприятия;**
- **техническую оснащенность предприятия;**
- **экономическое состояние предприятия;**
- **организационную структуру предприятия;**
- **нормативно-правовое обеспечение деятельности предприятия.**

В меньшей степени на организацию КСЗИ предприятия могут влиять:

- режим работы предприятия;
- технология производства и управления;
- тип и объем производства;
- местоположение и архитектурные особенности предприятия;
- форма собственности предприятия.

8.4 Модель системы автоматизированного проектирования защиты информации

Структурно-функциональная схема САПР защиты информации (**рисунок. 7.1**) может быть представлена в виде пяти основных модулей:

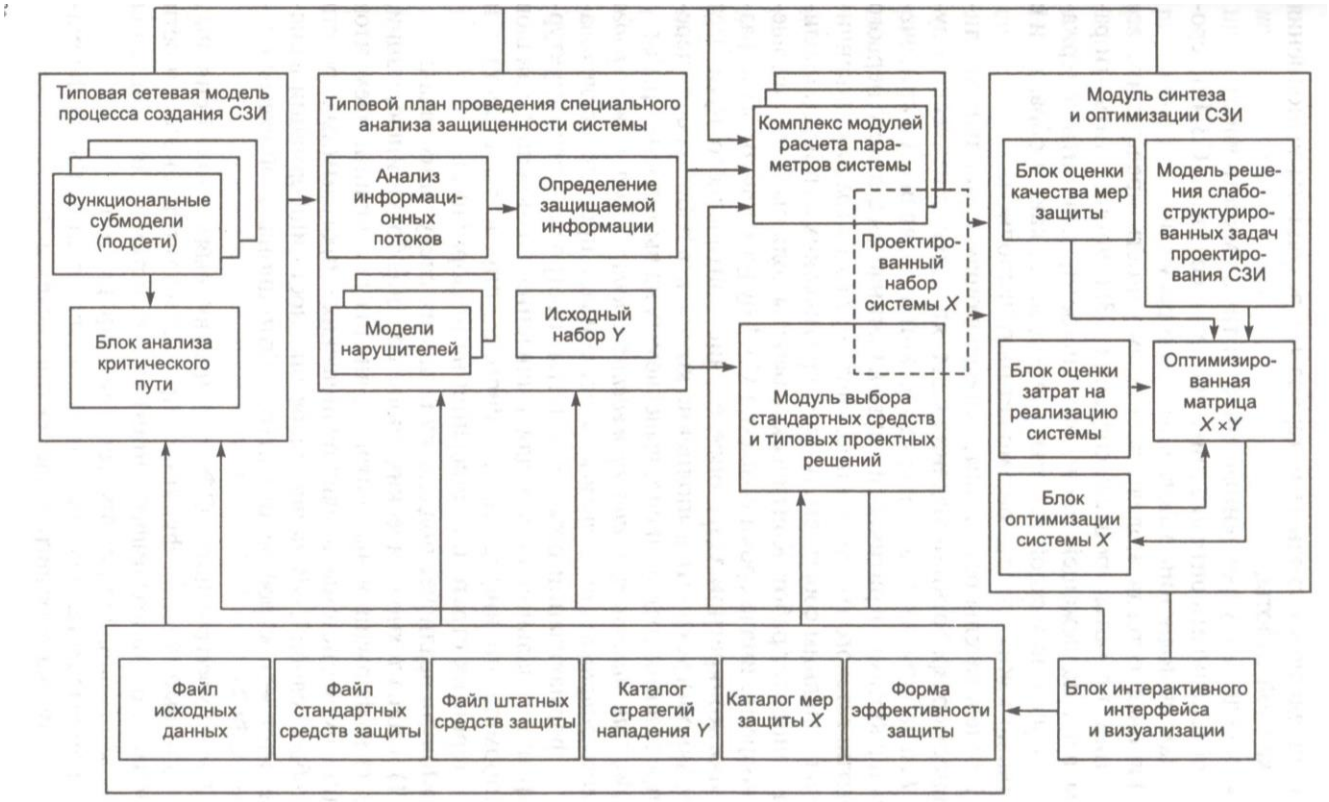

Рисунок 7.1 - Структурно-функциональная схема САПР защиты информации

- типовая сетевая модель процесса создания СЗИ;
- типовой план проведения специального инженерного анализа защищаемой системы;
- модули расчета параметров подсистем СЗИ;
- модуль синтеза и оптимизации СЗИ;
- модуль выбора стандартных средств и типовых проектных решений.

Кроме этого, модель включает в себя проблемно-ориентированный банк данных и блок интерфейса и визуализации.

Модуль типовой сетевой модели процесса создания СЗИ. В качестве метода планирования комплекса работ по созданию системы защиты целесообразно принять метод сетевого планирования, так как создание СЗИ определяется большим числом и различным содержанием работ, требующих взаимной увязки по срокам исполнения; необходимая цель создания СЗИ достигается коллективом специалистов; необходимо обеспечивать заданные сроки создания СЗИ и т. д.

Типовая сетевая модель позволяет разработчику:

- формулировать общую программу работ и их последовательность;
- определять содержание работ по созданию СЗИ;
- определять исполнителей работ;
- определять исходные материалы, необходимые для выполнения каждой работы;
- определять выходные материалы и результаты выполнения каждой работы;
- определять усредненные сроки и трудоемкость работ;
- обеспечивать оптимизацию процесса создания СЗИ по срокам выполнения работ, затратам и ресурсам.

Типовая сетевая модель дает возможность представить все операции и работы процесса создания СЗИ, упорядочить эти работы в их надлежащей последовательности, выяснить содержание и значение каждой работы и определить, каким образом и с помощью каких средств она может быть выполнена.

Последовательность работ, определяющая наибольшую длительность разработки и создания СЗИ, является критическим путем *L,* а работы, входящие в критический путь, являются критическими работами. Критический путь *L* начинается с самого первого события сетевого графика и проходит через весь график, заканчиваясь последним событием. Анализ критических путей устанавливает приоритет работ. Критические работы должны быть завершены вовремя, иначе сроки создания СЗИ будут сорваны. При разработке конкретной СЗИ определение критического пути дает возможность ускорить выполнение комплекса работ за счет перераспределения средств и сил, выделяемых на выполнение работ.

Модуль типового плана проведения специального инженерного анализа защищаемой системы. Обеспечивает процесс исследования и формализации объекта защиты, построения его структурно-функциональной схемы для выявления возможных каналов компрометации информации в системе, определение состава и характеристик стратегий нападения на информацию.

Модуль реализует поддержку решения следующих задач:

1) анализ технологических процессов обработки информации, анализ информационных потоков, анализ дислокации элементов защищаемой системы, анализ технических и программных средств и особых условий, влияющих на безопасность информации в системе; итог - построение структурно-функциональной схемы системы (СФС);

2) деструктуризация СФС с целью выявления основных (в плане выполнения функций управления и в плане общности решений по защите информации) узлов системы для выявления возможных каналов компрометации информации;

3) определение состава системы нападения на информацию *Y,* оценка параметров элементов системы *Y.*

Модуль выбора стандартных средств и типовых проектных решений. Модуль базируется на информации банка данных и ограничений проектировщика и заказчика системы.

Блок модели нарушителей содержит в себе описания категорий людей, которые могут предпринять попытку несанкционированного доступа к информации случайно или преднамеренно. Это могут быть: операторы, инженерно-технический персонал, пользователи, разработчики, обслуживающий персонал и т. д. Нарушитель может быть осведомлен о структуре защищаемой системы, характере информации, технического и программного обеспечения, наличии средств защиты, их устройстве и технических характеристиках. Неизвестными можно считать лишь те параметры и элементы средств защиты, которые подлежат периодической смене (ключи, пароли и т. п.).

Блок «Исходный набор *Y*» предназначен для определения потенциальных стратегий нападения, которые выявляются посредством неформально-логического анализа выявленных в деструктурированных узлах системы возможных каналов компрометации информации и вероятных нарушений безопасности с использованием каталога основных потенциальных стратегий нападения на информацию.

Результатом работы данного модуля САПР является сформированный рабочий набор стратегий нападения *Y* в виде табличного файла (**таблица 8.1**).

Таблица 8.1 - Характеристики стратегии нападения

N п/п	Обозначение стратегии *Y*	Содержание и краткая характеристика стратегий нападения	Информативность стратегии J_j;. байт/сутки	Категория лиц - потенциальных нарушителей	Вероятность применения

Модуль комплекса моделей расчета параметров подсистем СЗИ. Он включает в себя программно-математические средства проектирования системы криптозащиты, технических средств, системы разграничения доступа, системы постобработки регистрационной информации и т. д. В процессе функционирования САПР комплекс моделей должен пополняться и совершенствоваться.

Модуль синтеза и оптимизации СЗИ. Модуль осуществляет разработку мер защиты. Этот этап следует непосредственно после проведения инженерного анализа СЗИ и определения состава и основных характеристик системы нападения на информацию. В результате выполнения этапа определяется оптимальный состав СЗИ и основные требования к качеству мер защиты информации, а также производится оценка затрат, требующихся для реализации СЗИ.

Синтез и оптимизация СЗИ выполняется в следующей последовательности:

- для каждой стратегии нападения на информацию, выявленной в результате анализа защищаемой системы, из каталога основных мер защиты выбираются такие меры, с помощью которых обеспечивается противодействие каждой вошедшей в набор *Y* стратегии нападения, т. е. такие меры защиты, для которых в матрице качества элементы q_{ij} для данной стратегии нападения отличны от нуля. При этом качество каждой *j*-й меры защиты по отношению к *i*-й стратегии нападения определяется величиной q_{ij} - вероятностью блокировки *i*- й стратегии нападения с помощью *j*- й меры защиты информации;
- для каждой выбранной меры защиты в соответствии с методикой оценки качества мер защиты от конкретных стратегий нападения производится уточнение величин q_{ij};
- в соответствии с методикой оптимизации плана СЗИ составляется и решается система уравнений задачи оптимизации. В дальнейшем при разработке конкретных мер защиты, вошедших в оптимальный план СЗИ, необходимо обеспечить выполнение требований к качеству мер защиты информации;
- определяются оценочные затраты, необходимые для реализации СЗИ, равные сумме затрат на реализацию мер защиты, вошедших в оптимальный план СЗИ.

Блок оценки качества мер защиты содержит методики оценки качества мер защиты. **Возможны следующие методы оценки параметров q_{ij}:**

- **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.

Капитальные вложения представляют затраты на разработку мер защиты СЗИ в целом, разработку и отладку аппаратуры, предназначенной для защиты информации, на конструктивную доработку комплекса технических средств в целях обеспечения их специальных свойств, создание экранирующих сооружений, создание системы заземления, на приобретение аппаратуры, монтаж и отладку охранной и противопожарной сигнализации.

Текущие расходы представляют затраты на заработную плату персонала, обслуживающего СЗИ, накладные расходы, затраты на энергоснабжение и т. д.

Критерием оптимизации плана СЗИ может быть минимизация затрат на реализацию СЗИ в АСОД при условии обеспечения заданных уровней защищенности информации от несанкционированных действий со стороны всех вероятных стратегий нападения, т. е.

$$C = \sum_j C_j = \sum_j \sum_i d_{ij} C_i \to \min$$

$$\log P = U \le U_0 = \log P_0$$

где C_i - затраты на реализацию *i*- й стратегии;

$$d_{ij} = \left\{ \begin{array}{l} 1, \text{ если } i\text{-я мера защиты входит в } j\text{-й набор мер;} \\ 0, \text{ если } i\text{-я мера защиты не входит в } j\text{-й набор мер.} \end{array} \right\}$$

U = **log** P - уровень защищенности информации в АСОД;

$$P = \prod_{k=1}^{S} \prod_{i-1}^{m_k} \left(1 - q_i \prod_{i=1}^{n_k} ij \right)$$

где q_j - вероятность применения стратегии;
S - число возможных подсистем стратегий нападения;
m_k - число возможных стратегий нападения в составе *k-ŭ* подсистемы нападения;
n_k - число мер защиты, направленных на противодействие *k-ŭ* подсистеме стратегий нападения.
В качестве системы защиты принимается такой набор мер защиты R_i, для которого C_i = **min** $\{C_j\}$.
Визуализация оптимизированной матрицы может быть представлена в виде **таблицы 8.2**.

Таблица *8.2* - Характеристики мер защиты информации

Y	Мера защиты информации		Значение $1 - q_{ij}$	Ошибки затрат, тыс. руб.	Проектное время реализации
	Обозначение *X*	Содержание мер защиты			

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 *X;*
- 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 *P* 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

Большинство систем не может функционировать без участия человека, что является верным и для комплексных систем ЗИ. Группа обеспечения таких систем, с одной стороны, - ее необходимый элемент, с другой - он же может быть причиной и движущей силой нарушения и преступления. Сотрудник предприятия является определяющей фигурой в обеспечении сохранности сведений. Он может выступать в качестве создателя интеллектуальной собственности предприятия (совершенствуя технологию, создавая какие-либо товары и др.). При этом значительная часть ценнейшей для предприятия информации не отражается в технической документации, а остается в голове. И в дальнейшем, накопив опыт, многие из них потенциально готовы в будущем реализовать свои идеи на практике. Кроме того, если сотрудник привлекается к закрытым работам, руководитель предприятия вынужден предоставить ему наиболее ценную информацию, полученную другим работником.

Проведя анализ статистических данных по отечественным и зарубежным источникам, можно сделать вывод, что **около 70 %** (а по некоторым источникам эта цифра еще выше) **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. Таким образом, не обеспечив закрепление лиц, осведомленных в секретах талантливых специалистов, невозможно в полной мере сохранить секреты предприятия. Вопросам предупреждения текучести кадров в зарубежных фирмах уделяют большое внимание. Представители японской администрации рассматривают компанию как совокупность различных ресурсов. При этом люди стоят на первом месте, так как именно они воплощают технологию и в них в первую очередь заключается конкурентоспособная сила фирмы. То есть **текучесть кадров** - четвертая причина;

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. Выполняя требования режима секретности, сотрудник вынужден действовать в рамках ограничения своей свободы, что может привести его к стрессам, психологическим срывам, и как результат нарушения безопасности информации.

Понимая ведущую роль кадров в сохранении секретов, руководителям предприятия важно помнить, какие личные качества человека не способствуют сохранению доверенной ему тайны. То есть причины нарушения безопасности информации связаны с психологическими особенностями человека, его личными качествами, следовательно, и **способы предотвращения перечисленных нарушений вытекают из анализа побудительных мотивов - тщательного подбора персонала, подготовки персонала, поддержания здорового рабочего климата, мотивации и стимулирования деятельности сотрудников**.

В любой профессиональной деятельности есть стабильные составляющие и переменные, связанные с конкретными условиями, в которых эта деятельность осуществляется. При подборе кадров важно принимать во внимание обе составляющие, т. е. дается описание психологических характеристик, соблюдение которых необходимо для выполнения определенных профессиональных обязанностей. В **психограмму включаются требования**, предъявляемые профессиональной деятельности, **к психологическим процессам** (памяти, воображению, восприятию), **психическим состояниям** (усталости, апатии, стрессу), **вниманию**, как состоянию сознания, э**моциональным** (сдержанность, индифферентность) и **волевым** (настойчивость, импульсивность) **характеристикам**. Некоторые из этих психологических требований являются основными, главными, без них вообще невозможна качественная деятельность.

Психологическое несоответствие требованиям профессии особенно сильно проявляется в сложных ситуациях, когда требуется мобилизация всех личностных ресурсов для решения сложных задач. Поэтому это особенно важно в рамках комплексной системы защиты информации.

Но описание психологических требований недостаточно, чтобы, ориентируясь только на них, подбирать человека для работы. **При подборе кадров необходимо ориентироваться не только на отдельные характеристики психики, а на черты личности, как ее системные свойства**. Выделим наиболее результативные **методы изучения личности**:

- изучение жизненного пути личности;
- изучение мнения коллектива, в котором работает личность;
- изучение ближайшего окружения личности;
- создание ситуации, наиболее подходящей для проявления профессионально важных качеств и свойств;
- изучение высказывания личности о собственной роли в делах коллектива.

К **качествам, соответствующим работе** в таких условиях, относятся: честность, добросовестность, принципиальность (строгое следование основным правилам), исполнительность, пунктуальность, дисциплинированность, эмоциональная устойчивость (самообладание), стремление к успеху и порядку в работе, самоконтроль в поступках и действиях, правильная самооценка собственных способностей и возможностей, осторожность, умение хранить секреты, тренированное внимание и неплохая память.

Качества, не способствующие сохранению доверенной тайны: эмоциональное расстройство, неуравновешенность поведения, разочарование в себе, отчужденность от коллег по работе, недовольство своим служебным положением, ущемленное самолюбие, эгоистичные интересы, нечестность, употребление наркотиков и алкоголя, постепенно разрушающих личность.

9.2 Подготовка персонала для работы в новых условиях

С целью максимальной эффективности использования вновь принятого на работу человека необходимо, принимая на работу нового сотрудника, не ограничиваться ознакомлением его с техникой безопасности, режимами работы, с рабочим местом, навыками владения средствами и предметами труда. В качестве примера влияния адаптационного периода рассмотрим результаты исследования феномена «летунов», т. е. людей, часто меняющих профессию или место работы, которые показывают, что в начале их трудового пути, как правило, был неудачный опыт адаптации к предприятию и коллективу. В результате, столкнувшись с первыми трудностями на работе, с первыми сложностями, с конфликтами, такой человек в силу особенностей психики уходит от этих трудностей путем увольнения с работы по собственному желанию.

Причина этих явлений - условия, не способствующие адаптации вновь принятого работника. Такими неблагоприятными условиями могут быть условия обыденные, удобные, даже рациональные с точки зрения работников, хорошо приспособившихся к окружающей их производственной среде. Поэтому трудности новичков не замечаются.

Условно сложная адаптация может быть разделена на виды: профессиональная, социально-организационная, социально-психологическая.

Профессиональная адаптация - это адаптация к самой трудовой деятельности со всеми обеспечивающими ее предметными и временными составляющими. Она характерна при обстоятельствах, возникающих при первом знакомстве человека с условиями его новой работы. Эта адаптация неизбежна при всех изменениях, происходящих на предприятии или на рабочем месте.

Социально-организационная адаптация включает в себя знакомство с работой органов управления и обеспечения работы предприятия (отдел кадров, администрация и т. д.), со сферой жизни коллектива, связанной с бытом и отдыхом.

Социально-психологическая адаптация связана с вхождением нового работника в первичный коллектив.

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. Продуктивность мотивации, основанной на интересе к деятельности, связана с содержательностью, т. е. той стороной деятельности, которая вызывает наибольший интерес.

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. Мотивация на основе стремления к профессиональному росту может проявляться, когда человек уже достаточно прочно чувствует себя как субъект деятельности. Тогда обостряется желание быстрее достичь некоторых стандартов деятельности или превзойти их.

Напрашивается способ мотивации, связанный со стимулированием, или другими словами, мотивация через потребности. Поскольку характер каждого человека - это соединение самых разнообразных черт, то, следовательно, существует огромное число человеческих потребностей, которые, по мнению каждого человека, приводят к удовлетворению его потребностей. Например, потребность в утверждении собственного «я» одного человека можно удовлетворить, признав его лучшим работником отдела, а удовлетворить аналогичную потребность кого-то другого означает признать лучшим фасоном его одежду, объявив всем, что он одевается лучше других в группе.

По теории Маслоу, все потребности человека можно расположить в виде строго иерархической структуры. Верхний уровень образует вторичные потребности. К ним относятся потребности в самовыражении, уважении и социальные. А первичные

потребности - безопасности, защищенности и физиологические потребности - образуют нижние уровни. Этим он хотел сказать, что потребности нижних уровней требуют удовлетворения и влияют на поведение человека прежде, чем на мотивации начнут сказываться потребности более высоких уровней. В каждый конкретный момент времени человек будет стремиться к той потребности, которая для него является наиболее важной или сильной. **Прежде чем потребность следующего уровня станет решающим фактором в поведении человека, должна быть удовлетворена потребность более низкого уровня**. Для того чтобы следующий, более высокий уровень потребностей начал влиять на поведение человека, не обязательно удовлетворять полностью потребности более низкого уровня, т. е., хотя в данный момент одна из потребностей может преобладать, деятельность человека стимулируется не только ею. И хотя для большинства людей их основные потребности располагались приблизительно в том же порядке, как мы рассмотрели, однако бывают исключения.

Методы удовлетворения потребностей высших уровней следующие.

I. **Социальные потребности**:

1) давайте сотрудникам такую работу, которая позволяет им общаться;

2)создавайте на рабочих местах дух единой компании;

3)проводите с подчиненными периодические совещания;

4)не старайтесь разрушить возникшие неформальные группы;

5) создавайте условия для социальной активности членов организации вне ее рамок.

II. **Потребность в уважении**:

1) предлагайте подчиненным более содержательную работу;

2) обеспечьте им положительную обратную связь с достигнутым результатом;

3) высоко оценивайте и поощряйте достигнутые подчиненными результаты;

4) привлекайте подчиненных к формулированию целей и выработке решений;

5) делегируйте подчиненным дополнительные права и обязанности;

6) продвигайте подчиненных по карьерной лестнице;

7) обеспечьте обучение и переподготовку, которая повышает уровень компетентности.

III. **Потребности в самовыражении**:

1) обеспечивайте подчиненных возможностью для обучения и развития, которые позволили бы полностью использовать их потенциал;

2) давайте подчиненным сложную и важную работу, требующую их полной отдачи;

3) поощряйте и развивайте у подчиненных творческие способности.

Большое значение для мотивации имеет климат в коллективе. И если все-таки дело дошло до увольнения, очень важно, чтобы работник ушел, не затаив зла. Возможно, необходимо поговорить с ним, выяснить причины ухода и в том случае, если уход связан с конфликтом, чувством неудовлетворенности и т. д., потребовать еще раз разобраться в ситуации и тем самым, возможно, поправить положение.

9.4 Разработка кодекса корпоративного поведения

Большинство компаний для создания и поддержания организационной культуры используют правила внутреннего трудового распорядка. Стоит заметить, что они не отвечают современным требованиям и к тому же не являются мотивационным инструментом. По соотношению доступности и результативности формирования и поддержания позитивной организационной культуры внедрение кодекса корпоративного поведения является наиболее эффективным. В таком кодексе должны быть максимально четко обозначены приоритетные цели и задачи организации, ее миссия, а также расставлены акценты во внутренних и внешних отношениях с сотрудниками, клиентами, руководством. Это элемент традиционной корпоративной культуры, улучшающий и укрепляющий психологическую атмосферу коллектива.

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**.

Корпоративная этика, кроме того, является составной частью организационной культуры и кодекс корпоративного поведения - значимый фактор ее развития. Кодекс призван выявлять приоритетные для организации ценности и доводить их до каждого сотрудника, как новичка, так и опытного профессионала. В идеале персонал будет ориентироваться на единые цели и тем самым повышать корпоративную идентичность, приверженность общему делу.

Содержание кодекса компании определяется, прежде всего, ее особенностями, структурой, задачами развития, установками ее руководителей.

Как правило, кодексы содержат две части:

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

При этом идеологическая часть может не включаться в содержание кодекса.

В профессионально однородных организациях (банки, исследовательские центры, консультационные компании) часто используются кодексы, описывающие в первую очередь узкоспециальные дилеммы. Эти кодексы являются производными от кодексов профессиональных сообществ. Соответственно, содержание таких кодексов в первую очередь регламентирует поведение сотрудников в сложных профессиональных этических ситуациях. В банковской деятельности, например, это доступ к конфиденциальной информации о клиенте и сведениям об устойчивости банка. Кодекс описывает правила обращения с такой информацией, запрещает использовать сведения в целях личного обогащения.

В первую очередь здесь решаются управленческие задачи. Дополнение такого кодекса главами о миссии и ценностях компании способствует развитию корпоративной культуры. При этом кодекс может иметь значительный объем и сложное специфическое содержание и адресоваться всем сотрудникам компании.

В больших неоднородных корпорациях сочетание всех трех функций становится сложным. С одной стороны, существует ряд политик и ситуаций, традиционно закрепляемых этическими кодексами в международной практике. Это политики по отношению к клиентам, поставщикам, подрядчикам - описание ситуаций, связанных с возможными злоупотреблениями; например взятки, подкуп, хищения, обман, дискриминация. Исходя из управленческой функции, кодекс описывает стандарты образцового поведения в таких ситуациях. Такой кодекс имеет значительный объем и достаточно сложное содержание. Адресация его всем группам сотрудников в условиях значительной разницы в образовательном уровне и социальном статусе сотрудников затруднена. В то же время развитие корпоративной культуры компании требует единого кодекса для всех сотрудников - он должен задавать единое понимание миссии и ценностей компании для каждого сотрудника.

По сути, **декларативный вариант - это только идеологическая часть кодекса без регламентации поведения сотрудников**. При этом в конкретных ситуациях сотрудники сами должны ориентироваться, как им себя вести, исходя из базовых этических норм, обозначенных в кодексе. Однако в ряде случаев сотрудникам трудно оценить этическую правомерность конкретного поступка, исходя из общих принципов.

Таким образом, **декларативный вариант кодекса решает в первую очередь задачи развития корпоративной культуры**. При этом для предоставления кодекса международному сообществу и решения конкретных управленческих задач необходима разработка дополнительных документов.

В развернутых вариантах кодекса с подробной регламентацией этики поведения сотрудников фиксируются конкретные поступки персонала в отдельных областях, где риск нарушений наиболее высок или возникают сложные этические ситуации. Эти регламенты описываются в виде политик в отношении заказчиков, государства, клиентов, политической деятельности, конфликта интересов, безопасности труда.

При этом большой объем и сложность содержания таких кодексов определяют их выборочную адресацию. В большинстве компаний такие кодексы разрабатываются для высшего и среднего менеджмента и не являются всеобщим документом, объединяющим всех сотрудников.

Итак, каждая компания определяет собственные задачи, для решения которых она намерена использовать такой инструмент, как кодекс корпоративного поведения (**таблица 9.1**). Но создание кодекса, естественно, не ограничивается только написанием текста документа. Существует специфика исполнения подобных документов: заставить исполнять этический кодекс нельзя. Поэтому для того чтобы он действительно работал, еще на этапе его создания необходимо предусмотреть процедуры, включающие в процесс разработки документа по возможности всех сотрудников компании. Только при условии принятия каждым сотрудником кодекса корпоративного поведения он будет реально исполняться.

Таблица 9.1 - Адресация кодекса корпоративного поведения

Показатель	Кодекс		
	профессиональный	декларативный	развернутый
Характеристики организации	Профессионально однородные организации.	Крупные, профессионально неоднородные организации.	
Содержание	Описывает профессиональные этические дилеммы, нормы и стандарты поведения. Может содержать идеологическую часть.	Описывает идеологию и общие правила поведения.	Описывает политику в отношении ключевых групп. Регламентирует поведение сотрудников. Может содержать идеологическую часть.
Основные функции	Может реализовывать все три функции: репутационную, управленческую и функцию развития корпоративной Культуры.	Реализует в основном функцию развития корпоративной культуры, частично – управленческую.	Реализует репутационную и управленческую функции.
Кому адресовано	Всем сотрудникам.	Всем сотрудникам.	Преимущественно менеджменту.
Формат	Профессиональный язык, большой объем.	Понятный текст, небольшой объем.	Специальная терминология, большой объем.

Основным решением проекта стала идея «улицы с двусторонним движением»:

•«сверху вниз» - определение базовых ценностей и целей высших руководителей, разработка на их основе проекта;

«снизу вверх» - каждому сотруднику предоставлялась возможность стать соавтором кодекса через его обсуждение и внесение собственных предложений

Общий план разработки:

1-й этап. Проектирование. Разработка проекта кодекса с основным акцентом на цели и ценности, среди которых важное место отведено контролю безопасности и сохранности конфиденциальной информации. Здесь же указано отношение первых лиц и высшего руководства к существующей в организации проблематике этического характера.

Для этого проводится анализ существующих кодексов других компаний в контексте их применения. Определялись базовые ценности и цели данной организации, а также наиболее актуальные сферы применения кодекса.

В итоге должна быть сформирована концепция кодекса, в том числе его идеология, формат, сферы применения, и создан предварительный проект текста.

2-й этап. Обсуждение. Обсуждение проекта кодекса в трудовых коллективах, во всех подразделениях организации и сбор предложений по доработке текста кодекса и системы его исполнения.

На этом этапе важно провести работу по следующим позициям:

- разъяснение сотрудникам смысла, значения и сфер применения кодекса;
- привлечение рядовых сотрудников к процессу создания кодекса;
- создание позитивного общественного мнения в отношении кодекса среди персонала, а также подготовка менеджмента и квалифицированных сотрудников как ресурса по внедрению кодекса в практику ежедневной деятельности.

Процесс обсуждения включает в себя такие элементы, как:

- очную и заочную формы обсуждения проекта кодекса, которые позволяют сотрудникам стать соавторами кодекса;
- оригинальную методику групповой работы по обсуждению проекта кодекса, как с руководителями, так и с неформальными лидерами общественного мнения, которые бы инициировали дальнейшее обсуждение документа в трудовых коллективах;
- оперативную обработку и передачу данных очного обсуждения для незамедлительного использования в параллельно идущем заочном обсуждении в корпоративных средствах массовой информации;
- интерактивную модульную схему информационной кампании, позволяющую вести в диалоговом режиме разъяснение ключевых смыслов кодекса и отвечать на самые актуальные вопросы.

Очное обсуждение ориентировано на включение в диалог работников, заинтересованных в будущем своей организации, у которых есть что высказать и предложить ради повышения общего морального климата.

Заочное обсуждение (информационная кампания в корпоративных и федеральных СМИ, а также в корпоративных виртуальных сетях) теоретически может охватить более высокий процент сотрудников, чем физически осуществимо при очном учете масштабов корпорации. В период обсуждения кодекса должны быть задействованы все доступные средства, печатные издания, освещение темы на корпоративном сайте организации, в стенгазетах.

Обратная связь. Само обсуждение кодекса уже является началом его внедрения. Процесс обсуждения служит основой для поиска общих интересов сотрудников и руководства, построения единой ценностно-целевой картины и развития диалога между сотрудниками и руководством.

3-й этап. Интеграция. Этот этап включает анализ всех поступивших предложений, внесение изменений в содержание проекта, выработку механизмов исполнения и внедрения документа.

После обсуждения документа проводится анализ предложений, полученных от сотрудников, и на его основе корректируется содержание кодекса. Кроме того, на этом этапе применяется схема построения механизмов внедрения и исполнения кодекса, основанная на изучении опыта других компаний, а также на предложениях сотрудников. Итогом третьего этапа проекта становится создание окончательного варианта текста кодекса, его полиграфическое исполнение и распространение среди персонала.

Спустя некоторое время возможна ситуация, когда однажды принятый кодекс корпоративного поведения потеряет актуальность, морально устареет. В этом случае высшему руководству требуется созвать комиссию по его пересмотру, и в случае решения о неизбежности внесения изменений разработать новый проект кодекса, с обязательным учетом прошлого опыта.

Формирование позитивной корпоративной культуры с учетом специфики безопасности затрагивает изменение таких существенных представлений, как внутренний психологический климат коллектива, фундаментальные ценности, устоявшиеся паттерны поведения, совокупность формальных и неформальных требований к персоналу в виде норм, и наконец, общие представления представителей коллектива об окружающей среде, организации и индивидуальности каждого из сотрудников.

Все эти понятия являются составляющими организационной культуры и обусловливают деятельность, осуществляемую сознательно или неподконтрольно отдельными нормами субкультур организации, которые должны быть скорректированы таким образом, чтобы не противостоять первичным ценностям безопасности, установленным основной доминирующей культурой, не находиться в оппозиции к ним.

Чтобы действия, преследующие цели укрепления механизмов безопасности, были адекватно восприняты и приняты коллективом, они должны быть не только разумны, но и соответствовать базовым представлениям сотрудников о правильности, чему способствует изучение и понимание корпоративной культуры. Подсознательного неприятия или даже открытого противодействия политике безопасности можно избежать, если своевременно провести тщательное наблюдение, в ходе которого должен быть выявлен преобладающий тип корпоративной культуры каждого структурного подразделения, который может варьироваться в зависимости от функциональных, возрастных, профессиональных, географических или иных особенностей. Также крайне важно определить неформальных лидеров и выявить наиболее авторитетные субкультуры, значительно влияющие на внутреннюю жизнедеятельность организации. Важно выбрать наиболее эффективно работающую субкультуру и использовать ее в качестве исходной позиции для введения инноваций.

10. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

10.1 Значение нормативно-методического обеспечения

В целях обеспечения комплексного подхода к формированию законодательства по проблемам защиты информации и информатизации в России в апреле 1992 г. была утверждена «Программа подготовки законодательного и нормативного обеспечения работ в области информатизации и защиты информацию». В соответствии с этой Программой была намечена разработка базового Закона РФ в области информатизации «Об информации, информатизации и ЗИ» (кстати, который сегодня уже не актуален), а также еще ряда специальных законов.

Реализация Программы должна была позволить создать правовые основы процесса информатизации в России, нормативно закрепить права граждан, организаций и государства на информацию и системы автоматизации с учетом правил охраны государственной и коммерческих тайн, порядка правовой, организационной и технической защиты информации и информационного ресурса в целом, основ защиты и правовых гарантий прав потребителя информации, защитить права собственника и автора и решить многие другие проблемы.

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.

К содержанию нормативно-методических документов по ЗИ предъявляются требования. ИС должна быть защищена путем внедрения продуманных правил безопасности. СЗИ должна использовать набор правил для того, чтобы определить, может ли данный субъект получить доступ к данному объекту. Для предприятия целесообразно внедрение правил обеспечения безопасности и получение полномочий, с помощью которых можно было бы эффективно реализовать доступ к конфиденциальной информации. Пользователи, не обладающие соответствующими полномочиями, не должны получать доступ к конфиденциальной информации. Кроме того, необходимо применение дискриминационных методов управления, обеспечивающих доступ к данным только для некоторых пользователей или пользовательских групп, например, исходя из служебных обязанностей. Информационная система должна быть защищена с помощью правил безопасности, которые ограничивают доступ к объектам (файлы, приложения) со стороны субъектов (пользователи). Нормативные документы, определяющие порядок защиты, должны удовлетворять следующим требованиям: соответствовать структуре, целям и задачам предприятия; описывать общую программу обеспечения безопасности, включая вопросы эксплуатации и усовершенствования; перечислять возможные угрозы информации и каналы ее утечки, результаты оценки опасностей и рекомендуемые защитные меры; определять ответственных за внедрение и эксплуатацию всех средств защиты; определять права и обязанности пользователей, причем таким способом, чтобы этот документ можно было использовать в суде при нарушении правил безопасности.

Прежде чем приступить к разработке документов, определяющих порядок ЗИ, нужно провести оценку угроз, определить информационные ресурсы, которые целесообразно защищать в первую очередь, и подумать, что необходимо для обеспечения их безопасности. Правила должны основываться на здравом смысле. Целесообразно обратить внимание на следующие вопросы: принадлежность информации; об информации обязан заботиться тот, кому она принадлежит, - определение важности информации; пока не определена значимость информации, не следует ожидать проявлений должного отношения к ней, - значение секретности; как пользователи хотели бы защищать секретность информации? Нужна ли она им вообще?

Если право на сохранение тайны будет признано в вашей организации, то может ли она выработать такие правила, которые обеспечивали бы права пользователей на защиту информации?

10.2 Состав нормативно-методического обеспечения

Состав нормативно-методического обеспечения может быть определен следующим образом: законодательная база, руководящие методические документы и информационно-справочная база. К первому компоненту относятся: **законы, указы Президента, постановления Правительства, кодексы** (гражданский, уголовный, административный), **ГОСТы**. Во второй компонент могут входить **документы министерств и ведомств** (ФСТЭК, ФСБ), а также **документы, разработанные на предприятиях по вопросам защиты информации**. В состав информационно-справочной базы входят словари, каталоги, специализированные журналы, справочники, электронные базы данных.

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**.

10.3 Порядок разработки и внедрения документов

В ст. 7 Закона РФ «О государственной тайне» заранее установлен состав сведений, которые не могут быть засекречены, т. е. отнесены к государственной тайне:

«Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствия, а также о стихийных бедствиях и их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах РФ;
- о состоянии здоровья высших должностных лиц РФ;
- о фактах нарушения законности органами государственной власти и их должностными лицами».

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную и дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениями ст. 5 и ст. 7 закона о государственной тайне.

Обоснованность отнесения сведений к государственной тайне и их засекречивание заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий засекречивания, исходя из баланса жизненно важных интересов государства, общества и граждан. Своевременность отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

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.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с Законом о государственной тайне.

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной власти, наделяемой полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается президентом РФ, подлежит открытому опубликованию и пересматривается по мере необходимости.

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии в Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которых наделены указанные органы, и устанавливается степень их секретности. В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

Основаниями для рассекречивания сведений являются:

- взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в

РФ государственную тайну;

• изменение объективных обстоятельств, вследствие которых дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих в органах государственной власти, на предприятиях, учреждениях и организациях перечней сведений и их соответствия установленной ранее степени секретности.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите государственной тайны.

Правом изменения действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, наделяются утвердившие их руководители органов государственной власти, которые несут персональную ответственность принятых ими решений по рассекречиванию сведений. Решения указанных руководителей, связанные с изменением перечня сведений, отнесенных к государственной тайне, подлежат согласованию с межведомственной комиссией по защите государственной тайны, которые вправе приостанавливать и опротестовывать эти решения.

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

К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Руководители органов государственной власти, наделенные полномочиями по отнесению сведений к государственной тайне, организуют разработку перечня и несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Для разработки перечня создается экспертная комиссия, в состав которой включаются компетентные специалисты, работающие со сведениями, составляющими государственную тайну.

В ходе подготовки проекта перечня экспертные комиссии в соответствии с принципами засекречивания сведений, установленными Законом Российской Федерации «О государственной тайне», проводят анализ всех видов деятельности соответствующих органов государственной власти, предприятий учреждений и организаций с целью определения сведений, распространение которых может нанести ущерб безопасности Российской Федерации. Обоснование необходимости отнесения сведений к государственной тайне с указанием соответствующей степени секретности осуществляется собственниками этих сведений и оформляется в виде предложений для включения в проект соответствующего перечня.

Степень секретности сведений, находящихся в распоряжении нескольких органов государственной власти, устанавливается по взаимному согласованию между ними.

В перечень могут быть включены сведения, которые получены (разработаны) другими органами государственной власти, органами местного самоуправления, предприятиями, организациями или гражданами, не состоящими в отношении подчиненности к руководителю органа государственной власти, утверждающему перечень. Степень секретности таких сведений устанавливается по согласованию между органами государственной власти, разрабатывающими перечень, и собственником сведений.

Проект перечня, разработанный экспертной комиссией, представляется на утверждение руководителю органа государственной власти, наделенному полномочиями по отнесению сведений к государственной тайне, который также решает вопрос о целесообразности засекречивания самого перечня.

Утвержденные перечни в целях координации работ по защите государственной тайны направляются в Межведомственную комиссию.

После утверждения перечни доводятся до:

• заинтересованных органов государственной власти в полном объеме либо в части, их касающейся;

• предприятий, учреждений и организаций, действующих в сфере ведения органов государственной власти, в части, их касающейся, по решению должностного лица, утвердившего перечень;

• предприятий, учреждений и организаций, участвующих в проведении совместных работ, в объеме, определенном заказчиком этих работ.

Еще Закон РСФСР «О предприятиях и предпринимательской деятельности» юридически закреплял понятие «коммерческая тайна». Так, в п. 2 ст. 28 Закона говорилось, что «предприятие имеет право не предоставлять информацию, содержащую коммерческую тайну». Перечень сведений, которые не могут составлять коммерческую тайну, определяется постановлением Правительства Российской Федерации N 35 от 05.12.91 г.

В главе 6 Гражданского кодекса РФ (ст. 128, 138) среди объектов гражданских прав предусмотрена интеллектуальная

собственность, в том числе исключительные права на нее, а также защита информации, составляющей служебную или коммерческую тайну (ст. 139).

Согласно ст. 139 действующего ГК РФ, информация составляет служебную или коммерческую тайну в том случае, если она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам; к ней нет свободного доступа на законном основании; обладатель информации принимает меры к охране ее конфиденциальности. Эта статья ГК, в отличие от упомянутой выше ст. 28 Закона РСФСР «О предприятии и предпринимательской деятельности», усиливает возможность запрета отнесения к коммерческой тайне тех или иных сведений, поскольку в ней содержится норма, согласно которой «сведения не могут составлять служебную или коммерческую тайну, определяются законом или иными правовыми актами».

Согласно этой же статье ГК РФ, лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая обязанность возлагается на работников, разгласивших коммерческую тайну, вопреки трудовому договору и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Из упомянутых правовых норм следует, что **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**.

Таким образом, фиксируется право собственника охранять свои интересы во взаимоотношениях со всеми субъектами рынка, включая государство.

Реализация этого права осуществляется в соответствии с Законом о КТ РФ путем создания и поддержания на договорной основе с другими физическими и юридическими лицами защиты коммерческой информации, включающей в себя комплекс правовых, организационных, инженерно-технических, социально-психологических и других мер, основывающихся на административно-правовых нормах РФ и организационно-распорядительных документах руководства предприятия. Введение их в действие на предприятии приказом руководства является необходимым условием функционирования систем защиты конфиденциальной информации, поскольку эти документы представляют собой основной пакет нормативных документов, регулирующих правовые отношения в процессе обеспечения безопасности.

Однако не стоит забывать, что любой закон будет действовать только при наличии механизма его реализации в виде организационных структур, обеспечивающих выполнение положений этого закона на всех уровнях управления.

Серьезное значение для обеспечения безопасности информационных ресурсов приобретают документы предприятия, регулирующие отношения с государством и с коллективом сотрудников на правовой основе.

К таким **основополагающим документам** можно отнести:

- **устав предприятия**, закрепляющий условия обеспечения безопасности деятельности и защиты информации;
- **трудовые договоры** с сотрудниками предприятия, содержащие требования по обеспечению защиты сведений, составляющих коммерческую тайну и др.;
- **правила внутреннего трудового распорядка** рабочих и служащих;
- **должностные обязанности** руководителей, специалистов и обслуживающего персонала.

Эти документы играют важную роль в обеспечении безопасности предприятия.

Для предприятия необходимо:

1. Внести в устав следующие дополнения:

- предприятие имеет право: определять состав, объем и порядок защиты сведений, составляющих коммерческую тайну; требовать от своих сотрудников обеспечения ее сохранности;
- обязано обеспечить сохранность коммерческой тайны;
- состав и объем информации, являющейся конфиденциальной и составляющей коммерческую тайну, а также порядок защиты определяются руководителем предприятия;
- имеет право не предоставлять информацию, содержащую коммерческую тайну;
- руководителю предоставляется право возлагать обязанности, связанные с защитой информации, на сотрудников.

Внесение этих дополнений дает право администрации:

- создавать организационные структуры по защите коммерческой тайны;
- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих коммерческую тайну, и механизмы их защиты;
- включать требования по защите коммерческой тайны в договоры по всем видам деятельности;
- требовать защиты интересов фирмы перед государственными и судебными органами;
- распоряжаться информацией, являющейся собственностью, в целях извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств производства .

2. Разработать «Перечень сведений, составляющих коммерческую тайну».

Начало работы по защите коммерческой тайны связано с разработкой перечня сведений, составляющих коммерческую тайну. Перечень должен разрабатываться специальной комиссией, в которую включаются квалифицированные специалисты по всем направлениям деятельности предприятия. В состав комиссии должны входить руководители службы защиты информации (службы безопасности) и лицо, ответственное за конфиденциальное делопроизводство. Комиссия назначается приказом руководителя предприятия. В этом же приказе устанавливаются общий механизм и сроки разработки перечня. Разработка перечня может быть возложена и на экспертную комиссию предприятия, осуществляющую экспертизу ценности документов, если ее состав отвечает требованиям, предъявляемым к комиссии по составлению перечня.

На первом этапе работы комиссия на основе анализа всех направлений деятельности предприятия должна установить весь состав циркулирующей на предприятии информации, отображенной на любом носителе, любым способом и в любом виде, а также с учетом перспектив развития предприятия и его взаимоотношений с партнерами определить характер

дополнительной информации, которая может возникнуть в результате деятельности предприятия. Эта информация классифицируется по тематическому признаку.

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

В соответствии со СТ. 139 ГК РФ и другими нормами федеральных законов информация может составлять коммерческую тайну, если она отвечает следующим требованиям (критерии правовой охраны):

- имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам;
- не подпадает под перечень сведений, доступ к которым не может быть ограничен, и перечень сведений, отнесенных к государственной тайне;
- к ней нет свободного доступа на законном основании;
- обладатель информации принимает меры к охране ее конфиденциальности.

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**.

В то же время, наряду с общим перечнем сведений, доступ к которым по закону не может быть ограничен, в действующем законодательстве установлен специальный перечень в отношении сведений, которые не могут составлять коммерческую тайну (ст. 5 закона о КТ).

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

Результаты работы оформляются перечнем сведений, составляющих коммерческую тайну (таблица 10.1).

Таблица 10.1 - Структура перечня сведений

№ п/п	Название сведений	Сроки конфиденциальности

При значительном объеме конфиденциальных сведений они классифицируются в перечнях по разделам, составляющим сферы деятельности предприятия.

Перечни подписываются всеми членами комиссии, утверждаются и вводятся в действие приказами руководителя предприятия. В приказах должны быть определены мероприятия по обеспечению функционирования перечней и контролю их выполнения. С приказами и перечнями необходимо ознакомить под расписку всех сотрудников предприятия, работающих с соответствующей конфиденциальной информацией.

Дополнения и изменения состава включенных в перечни сведений могут вноситься с разрешения руководителя предприятия за подписями руководителя подразделения по принадлежности сведений и руководителя службы защиты информации (службы безопасности). При существенном изменении состава сведений перечни должны составляться заново.

Информацию, подлежащую защите, можно отнести к трем областям: выработка решений, имеющих стратегическое значение, и осуществление соответствующих планов; сведения о технологии сбора и обработки конфиденциальной информации; переговоры о заключении сделок.

3. Внести в трудовой договор:

3.1. В обязанности работника отдельным пунктом «Работник обязан соблюдать конфиденциальность сведений, которые ему стали известны в процессе работы. В случае нарушения конфиденциальности работник несет материальную и административную ответственность в соответствии с действующим законодательством РФ и правилами внутреннего распорядка Работодателя. Обязательства по соблюдению конфиденциальности остаются в силе и после прекращения срока действия настоящего Договора в течение одного года»;

3.2. Отдельную статью, связанную с конфиденциальностью, в которой бы содержалось следующее:

3.2.1. Под «коммерческой тайной» понимаются носящие конфиденциальный характер сведения и их носители, полученные в рамках настоящего Договора и отвечающие следующим условиям:

- сведения и их носители, указанные в «Перечне сведений, составляющих коммерческую тайну»;
- сведения и их носители не являются общеизвестными или общедоступными из других источников;
- сведения и их носители не передавались Работодателем в распоряжение других лиц без обязательства, касающегося их конфиденциальности.

3.2.2. Под «разглашением коммерческой тайны» понимаются умышленные или неосторожные действия Работника, приведшие к преждевременному, не вызванному служебной необходимостью, открытому опубликованию сведений, составляющих коммерческую тайну, либо к утрате документов с такими сведениями или бесконтрольному использованию и распространению этих сведений.

4. Разработать должностные инструкции сотрудников. Необходимым организационно-правовым документом с точки зрения защиты информации для фирмы является Должностная инструкция сотрудника. Такой документ должен содержать следующие разделы: 1. Общие положения; 2. Должностные обязанности; 3. Права.

Утверждается должностная инструкция руководителем или иным должностным лицом, уполномоченным утверждать должностные инструкции.

5. Разработать «Обязательство о неразглашении коммерческой тайны».

Следующим важным шагом с правовой точки зрения является разработка «Обязательства о неразглашении коммерческой тайны».

Разглашение информации, составляющей коммерческую тайну - это «действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору».

В обязательство должен быть включен пункт, который не позволял бы использовать любую информацию, полученную сотрудником в ходе выполнения им служебных обязанностей для осуществления любой деятельности, не связанной с этим предприятием.

6. Разработать «Подписку при увольнении с работы». Очевидно, что некоторые сотрудники в силу обстоятельств могут покинуть фирму, соответственно необходимо учесть этот момент при правовом регулировании отношений с сотрудниками. В Обязательстве на этот счет сказано, что сотрудник обязуется в течение определенного времени после увольнения не разглашать сведения, ставшие известными ему по работе.

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

11.1 Понятие и цели управления

Социотехнические системы, представляя собой единение человека и техники, всегда характеризуются определенными целями, которые ставят перед собой люди, достигая их с помощью технических средств, с которыми общаются через интеллектуального посредника. Цели и допустимые стратегии социотехнической системы в реальных ситуациях принятия решений по их защите зачастую субъективны и не могут быть точно определены. Это происходит преимущественно по той причине, что, помимо объективных законов, в их функционировании существенную роль играют субъективные представления, суждения, поступки и даже эмоции людей. Действительно, при исследовании безопасности объекта информатизации, предприятия значительное количество информации об этом объекте может быть получено от различных групп людей:

а) 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.

Поэтому получаемая от них информация, как правило, носит субъективный характер, а ее представление на естественном языке, не имея аналогов в языке традиционной математики, содержит большое число неопределенностей типа «много», «мало», если речь идет о вложениях денежных средств в совершенствование системы защиты объекта или об изменении количества персонала, работающего в подразделениях его защиты: «не выполнены частично», «выполнены частично», «почти выполнены», если речь идет о выполнении требований руководящих документов по защите информации и т. д. Поэтому математическое

описание подобной информации обедняет математическую модель исследуемой реальной системы и делает ее слишком грубой.

В связи с развитием системного анализа как основного инструментария о решении сложных проблем стали использовать понятие «проблема», или «задача» («проблема» - от греч. «задача»). Проблемы могут быть простыми и сложными. Можно различать также объектные, процессные и научно-исследовательские проблемы.

Для создания сложной системы, имеющей аналоги в прошлом, разработчик подыскивает подходящий аналогичный проект и принимает его за основу будущей системы. 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 и программно-целевой метод.**

Разработка сложной системы разбивается на два этапа: внешнее (или макро-) и внутреннее (или микро-) проектирование. Внешнее проектирование отвечает на вопрос: с какой целью создается система? Внутреннее проектирование - на вопрос: какими средствами реализуется система? При внешнем проектировании формируется цель и критерий эффективности будущей системы, создается и экспериментально проверяется, а затем корректируется ее модель. Локализуется сама система, определяются ее границы, фиксируются факторы внешней среды, влияющие на систему или находящиеся под ее влиянием; определяются входы, на которые система должна реагировать, и виды реакций, критерии эффективности ее функционирования. Внутреннее проектирование определяет содержание самой системы.

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**.

КСЗИ создается с целью обеспечения надежной защиты информации на соответствующем объекте, поэтому функциями, подлежащими осуществлению в данной системе, будут функции защиты, т. е. совокупность мероприятий, регулярно осуществляемых на предприятии с целью создания и поддержания условий, необходимых для надежной ЗИ.

Максимально эффективной защита информации будет лишь в том случае, если созданы надежные механизмы защиты, а в процессе функционирования системы осуществляется непрерывное управление этими механизмами.

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.**

Технологию организационного управления можно определить как регламентированную совокупность методов и средств управления коллективами людей в процессе достижения целей их деятельности.

Организационное управление может рассматриваться в двух основных аспектах:

- организация содержания деятельности, т. е. что делается (каковы функции и цели системы управления);
- организация самого процесса, т. е. как делается (какими методами достигается поставленная цель и осуществляется сам процесс управления).

Управление определяется как элемент, функция организованных систем различной природы, обеспечивающая сохранность их определенной структуры, поддержание режимов деятельности, реализацию их программ и целей.

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** всех процессов обработки данных и управления;
- **единство** органов, средств и методов управления;
- **максимальную автоматизацию** при решении всех задач, объективно возникающих в процессе функционирования органов управления, в том числе задач персонального информационного обеспечения, задач выработки управленческих решений и задач информационного сопряжения взаимодействующих систем.

Одним из активных звеньев технологии управления является человек, причем человек рассматривается как субъект управления и как объект управления.

В соответствии с этим сформулируем **требования к технологии управления**:

1. Обеспечение **разделения труда**, выражающееся в конкретизации функциональных обязанностей руководителей и специалистов органов управления.

2. **Максимальная формализация всех трудовых процессов**, осуществляемых в органах управления, заключается во введении количественных оценок в управленческие процессы, в использовании математических методов в управлении, а также в применении к управленческим системам таких понятий, как устойчивость, надежность и эффективность.

3. **Регламентация взаимодействия работников органов управления между собой и средствами автоматизации**, которая заключается в создании комплекса правил, предписаний, указаний и ограничений, закрепленных в соответствующих нормативно-методических документах и носящих обязательный характер.

4. **Обеспечение психологических совместимостей** руководителей и специалистов органов управления со средствами автоматизации.

5. **Повышение исполнительной дисциплины** работников органов управления.

Главным направлением построения технологии организационного управления, удовлетворяющим перечисленным выше требованиям, является разработка технологий на индустриальной основе с широким применением вычислительной техники и автоматизации технологических процессов управления.

Чтобы разработать эффективную технологию управления, необходимо решить следующие проблемы.

1. Разработать, утвердить и внедрить стандартные элементы технологии управления.

2. Разработать и внедрить стандартные методы решения задач всех классов.

3. Максимально формализовать решения всех задач, объективно возникающих в процессе функционирования системы управления.

4. Разработать эффективные средства, методы и способы обеспечения безопасности информации, хранимой и обрабатываемой с использованием ВТ.

5. Разработать нормативно-методические документы, регламентирующие взаимодействие работников органов управления между собой и со средствами автоматизации.

6. Разработать и внедрить типовую методологию построения и проектирования технологии организационного управления и стандартных элементов.

Таким образом, **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:

1**) однозначности** определения функционального назначения объекта, процесса или явления;

2) **четкости** и однозначности общей архитектуры объекта процесса или явления;

3) **простоте внутренней организации** объекта, процесса или явления в целом, его составных частей и взаимосвязи между ними;

4) **стандартности и унифицированности** внутренней структуры элементов их составляющих частей и взаимосвязей между ними;

5) **простоте изучения** структур и содержания элементов любой их совокупности и взаимосвязей между элементами;

6) **модульности**, т. е. автономной организации элементов, позволяющей стандартными способами объединять элементы в сложные структуры, а также заменять любые элементы или совокупность этих элементов;

7) **гибкости**, т. е. возможности расширения и реорганизации элементов и их частей без изменения или несущественными изменениями других элементов;

8) **доступности** для изучения элементов и их частей специалистами (инперсонификация).

Структуризация основных процессов технологии управления является не только этапом разработки технологии управления, но и сама по себе позволяет в значительной степени повысить эффективность управления за счет рационализации и единой организации управления труда независимо от степени использования в управлении средств автоматизации.

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**, своевременно и в строгом соответствии с обоснованными решениями;
- **максимально эффективное информационное обеспечение** всего процесса управления;
- **максимальная автоматизация** рутинных процедур технологии управления и информационного обеспечения.

Рационализацию технологии управления в общем виде можно представить последовательностью следующих действий:

1. Определение совокупности процедур управления, подлежащих осуществлению в соответствующем интервале времени.

2. Определение перечня и содержания информации, необходимой для осуществления процедур управления в данном интервале времени.

3. Организация подготовки необходимой информации.

4. Организация и обеспечение осуществления процедур управления.

Структуризация процессов позволяет сама по себе независимо от использования средств автоматизации значительно повысить эффективность управления за счет лучшей ее организации. Поэтому функционирование системы управления в самом общем виде можно представить как разработку планов функционирования управляемых объектов и их реализацию.

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

- **детерминированность элементов**;
- **динамичность системы**;
- **наличие** в системе **управляющего параметра**;
- **наличие** в системе **контролирующего параметра**;
- **наличие** в системе **каналов** (по крайней мере, одного) **обратной связи**.

Соблюдение этих требований должно обеспечивать условия эффективного уровня функционирования органов управления.

В системах управления детерминированность проявляется в организации взаимодействия подразделений органов управления, при которой деятельность одного элемента (управления, отдела) сказывается на других элементах системы. Если в организационной структуре управления, например, есть отдел, действия которого не влияют на другие подразделения, то такой отдел не реализует ни одну из целей функционирования организации и является лишним в системе управления.

Вторым требованием является динамичность, т. е. способность под воздействием внешних и внутренних возмущений оставаться некоторое время в определенном неизменном качественном состоянии.

Любые воздействия среды оказывают возмущающее действие на систему, стремясь нарушить ее. В самой системе также могут появиться возмущения, которые стремятся разрушить ее «изнутри». Например, в организации нет достаточного количества квалифицированных кадров, отсутствует по каким-то причинам ряд ответственных работников, плохие условия работы и т. д. К внешним возмущениям следует отнести указы вышестоящих организаций, изменения ситуаций на рынке, экономические и политические факторы. Под воздействием таких внешних и внутренних возмущений орган управления любого

уровня вынужден перестраиваться, приспосабливаться к изменившимся условиям.

С целью обеспечения быстрого перестроения системы в условиях изменения среды в системе управления должен быть элемент, фиксирующий факт появления возмущения; система должна обладать минимально допустимой инерционностью, чтобы своевременно принимать управленческие решения, в системе управления должен быть элемент, фиксирующий факт упорядочения состояния системы в соответствии с изменившимися условиями. В соответствии с этими требованиями **в структуре управления предприятием должен быть отдел совершенствования структуры управления**.

Под **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**. Он отвечает за деятельность подчиненного ему подразделения, воспринимает управляющие сигналы руководства организации, организует их выполнение, несет ответственность за выполнение всех управленческих решений.

При этом руководитель должен обладать необходимой компетенцией, а условия работы - позволять выполнить данное поручение. Условие наличия управляющего параметра можно считать выполненным, если **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.

Несоблюдение данного требования, т. е. наличия управляющего параметра, приводит к принятию субъективных управленческих решений и так называемому волевому стилю руководства. Это требует четкой организационной структуры и распределения обязанностей между руководителями подразделений, наличия должностных инструкций и прочих документов, регламентирующих их деятельность.

Следующим, четвертым требованием, предъявленным к системам управления, следует назвать наличие в ней контролирующего параметра, т. е. такого элемента, который постоянно **контролировал бы состояние субъекта управления, не оказывая при этом на него** (или на любой элемент системы) **управляющего воздействия**.

Контроль субъекта управления предполагает курирование обработки любого управляющего сигнала, поданного на вход данной системы. Функцию контролирующего параметра в системе управления, как правило, реализует один из сотрудников аппарата управления. Например, подготовку плана важнейших работ курирует главный специалист по экономике. На уровне министерства такие функции осуществляют кураторы по определенным проблемам в управлениях. **Любые управленческие решения в системе управления должны проходить только через элемент, выполняющий функции контролирующего параметра.**

Рисунок 11.1 – Структура процесса управления

Наличие прямых и обратных связей (пятое требование) в системе обеспечивается четкой регламентацией деятельности аппарата управления по приему и передаче информации при подготовке управленческих решений.

В целом структура процесса управления представлена на рисунке 11.1.

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, моделирование и программирование**.

Первую ступень планирования составляет прогнозирование. Прогнозы носят вероятностный характер, но, если прогнозирование выполняется качественно, его можно использовать как основу для планирования.

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.

Важное условие прогнозирования - **моделирование** различных ситуаций и состояний СЗИ в течение планируемого периода.

Задача программирования - исходя из реальных условий функционирования системы, запрограммировать ее переход в новое заданное состояние. Сюда входит разработка алгоритма функционирования системы, определение требующихся ресурсов, выбор средств и методов управления.

Таким образом, **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**. Оно предусматривает разработку комплекса мероприятий, определяющих последовательность достижения конкретных целей с учетом возможностей наиболее эффективного использования ресурсов каждым подразделением. Поэтому планирование также должно обеспечить взаимоувязку между отдельными структурными подразделениями предприятия, включающими всю технологическую цепочку.

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

а) если достижение некоторого результата является обязательным условием планируемой деятельности, то план должен разрабатываться таким образом, чтобы этот результат достигался при минимальных затратах ресурсов, т. е. **задан результат, который должен быть достигнут при минимальном расходе ресурсов**;

б) если для планируемых действий выделяются ограниченные ресурсы, то план должен быть разработан таким образом, чтобы при расходовании выделенных ресурсов достигался наибольший конечный результат, т. е. заданы ресурсы и **при заданных ресурсах необходимо достичь максимального результата**.

Планирование охватывает как текущий, так и перспективный периоды.

Если перспективное планирование должно определять общие стратегические цели и направления развития предприятия, необходимые для этого ресурсы и этапы решения поставленных задач, то разрабатываемые на его основе текущие планы ориентированы на фактическое достижение намеченных целей, исходя из конкретных условий. Поэтому текущие планы дополняют, развивают и корректируют перспективы направления развития с учетом конкретной обстановки.

Формы планирования в зависимости от длительности планового периода:

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

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

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

Особенностями **перспективного** планирования являются:

- основными целями планирования является **совершенствование концепции управления ЗИ**, формирование планов развития средств обеспечения защиты, разработка программ оптимальных систем управления защиты проектируемых систем;
- при необходимости может предусматриваться **изменение структурного построения СЗИ**, **режимов** их функционирования и **технологических схем**;
- при необходимости могут и должны обосновываться требования к совершенствованию концепции построения и использования системы защиты в соответствии с требованиями управления этими системами;
- при разработке планов **учитывают возможные условия изменения внешней среды**.

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**, но могут быть изменены режимы функционирования и технология управления защиты информации;
- при необходимости могут и должны разрабатываться **предложения по совершенствованию СЗИ**, исходя из требования повышения эффективности защиты и управления системы защиты информации.

При **текущем** планировании:

- основной целью является **рациональное использование имеющихся средств обеспечения защиты** в соответствии с планами управления комплексной системы защиты информации;
- **структура и режимы функционирования системы защиты изменению не подлежат**. Могут производиться лишь **незначительные изменения технологии управления СЗИ**;
- при необходимости могут и должны разрабатываться **предложения по включению** в состав системы управления защитой **новых средств** и по совершенствованию структуры этой системы.

Таким образом, перспективное планирование предусматривает разработку общих принципов ориентации системы защиты информации на перспективу; определяет стратегическое направление и программы развития, содержание и последовательность осуществления важнейших мероприятий, обеспечивающих достижение поставленных целей.

Поскольку оценка перспектив неопределенна, **перспективное планирование не может быть ориентировано на достижение количественных показателей** и поэтому обычно ограничивается разработкой лишь важнейших качественных характеристик, конкретизируемых в программах или прогнозах.

На основе программы разрабатываются **среднесрочные планы**, которые уже **содержат** не только качественные характеристики, но и **количественные показатели**, детализированные и конкретизированные с точки зрения выбора средств для реализации целей, намеченных в рамках перспективного планирования.

Основными звеньями текущего плана являются календарные планы (месячные, квартальные, полугодовые), которые представляют собой детальную конкретизацию целей и задач, поставленных перспективными и среднесрочными планами.

Планирование, как функция управления системой сохранения секретов реализуется через систему принципов, связанных с **общими принципами управления**, которые и должны быть положены в основу планирования:

1) **директивность**, т. е. обязательный характер планов;

2) **преемственность** - сочетание и взаимосвязь перспективного и текущего планирования: использование положительного опыта работы; учет допущенных недостатков и просчетов;

3) **конкретность** - постановка четких целей и задач, определение наиболее рациональных путей, методов и способов их достижения, установление ответственности конкретных лиц за организацию и выполнение плановых мероприятий, определение

оптимальных и реальных сроков их реализации;

4) **гибкость** - наличие возможностей маневра имеющимися силами и средствами в ходе выполнения плана, а также корректировка плана в случае изменения обстановки;

5) **проблемность** - нацеленность мероприятий на решение значимых вопросов, сосредоточение усилий работников на основных направлениях их деятельности, недопущение распыленности в использовании сил и средств;

6) **комплексность** - обеспечение использования всей системы мер по защите тайны на различных направлениях, в подразделениях, учет интересов всех, кто ведет работу на смежных участках, согласование и увязка на различных уровнях всех задач и способов их достижения;

7) **экономичность** - максимальные результаты должны достигаться при наименьших затратах сил и средств.

Качественное планирование позволяет организовать работу по решению первостепенных, наиболее важных вопросов в конкретный период времени, добиться наилучших результатов в работе при затрате наименьших сил и средств, повысить ответственность исполнителей за порученный участок работы, улучшить контроль за выполнением мероприятий в установленные сроки. В процессе составления плана руководитель готовит организационную основу для объединения усилии работников в единую систему в интересах достижения поставленной цели.

Планирование может быть организовано разными способами.

1. **Анализ**. При таком способе планирования на самом высшем уровне разрабатываются основные компоненты плана: цели, задачи возможные условия, выделенные ресурсы и др. Определяются основные задачи подразделений. Также на уровне подразделений анализируют цели, задачи, ресурсы, сроки. Аналогично происходит на низшем уровне.

2. **Синтез**. В этом случае сначала составляют планы на низшем уровне, которые затем, последовательно обобщенные, синтезируют в соответствии с иерархической структурой.

3. **Итерация**. На основе отправных установок вырабатывается первое приближение плана. На основе наилучшего варианта уточняются и корректируются исходные установки, и разрабатывается следующее приближение плана и так до тех пор, пока не будет получен приемлемый вариант плана, который должен удовлетворять требованиям, как отдельных структур, так и всей системы в целом. Чем выше влияние неопределенности на характер планируемой деятельности, тем более целесообразен итерационный способ планирования. **Данный способ планирования наиболее приемлем для КСЗИ**.

При определении тех или иных мероприятий плана необходимо получить ответы на следующие вопросы:

1. Способствует ли данное мероприятие достижению поставленных задач, замыслу?
2. Является ли оно правомерным, не противоречит ли законам, нормативным актам?
3. Будет ли оно оптимальным, не дублирует ли другие мероприятия?

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.

Основные положения вновь разработанного плана базируются на результатах проделанной работы по выполнению планов за предыдущий период и согласовываются с планами на смежных направлениях деятельности.

В начальной стадии планирования руководитель всесторонне изучает обстановку по защите информации на предприятии, ту совокупность условий, событий, обстоятельств проведения закрытых работ, которые оказывают существенное влияние на надежность и эффективность защиты. Моделируются вероятные тенденции ее изменения, появление принципиально новых факторов (условий, событий).

Мероприятия в плане следует систематизировать по следующим четырем разделам:

1) организационно-методическая работа;
2) контрольно-проверочная работа;
3) профилактическая работа;
4) работа с кадрами.

Во вводной части делается анализ и оценка обстановки на предприятии с точки зрения решения вопросов по защите сведений, акцентируется внимание на ее главных особенностях. Оценка и прогноз развития обстановки служат исходной базой для определения содержания основных разделов плана.

Организационно-методическая деятельность может включать в себя:

- разработку инструкций, методик по различным направлениям режима охраны информации;
- внесение изменений и дополнений в действующие инструкции, методики с учетом изменившихся условий;
- разработку и внедрение новых организационных методов защиты информации;
- обеспечение мероприятий в связи с приемом делегаций, командированных, участием в работе конференций и т. д.;
- подготовку и проведение крупных совещаний, заседаний, экспертных комиссий, выставок и т. П.;
- совершенствование системы делопроизводства, технологии обработки документов;
- сокращение закрытой переписки;
- разработку и внедрение информационно-поисковых систем для классифицированных документов;
- заслушивание руководителей различных уровней о ходе выполнения утвержденных директором мероприятий;
- обоснование и внедрение новых технических средств охраны;
- совершенствование структуры подразделения экономической безопасности, создание и оборудование новых рабочих мест;
- меры по координации и взаимодействию различных подразделений предприятия и т. п.

Контрольно-проверочная работа может рассматриваться и как проверка исполнения, и как изучение состояния дел, что приближает ее к аналитической работе. Она включает в себя:

- контроль за выполнением работниками предприятия требований соответствующих приказов, инструкций;

- проверку выполнения мероприятий, разработанных по результатам предыдущих анализов, проверок;
- контроль за порядком хранения и обращения с носителями тайны на рабочих местах;
- проверку подразделений предприятия;
- проверку режима при приеме командированных лиц, делегаций, проведении совещаний;
- проверку охраны, пропускного режима и т. п.

В разделе **профилактических мероприятий** планируются действия, направленные на формирование у исполнителей мотивов поведения, побуждающих к неукоснительному соблюдению в полном объеме требований режима, правил проведения закрытых работ и т. п.

В разделе **работы с кадрами** целесообразно включение мероприятий по обучению исполнителей и работников новым приемам, методам защиты тайны и т. п. Одним из направлений обучения и практической работы должен быть курс социально-психологических проблем взаимоотношений в коллективах лиц, допущенных к классифицированной информации.

Разработка плана не возможна без анализа предыдущей деятельности. Оцениваются имевшиеся случаи нарушения режима, причины и условия, им сопутствующие. С учетом возможностей определяется надежность принимаемых мер по защите сведений. Рассматривается целесообразность привлечения необходимых средств и сил.

В процессе планирования должны быть выделены следующие стадии.

1. **Обоснование целей и критериев**:

- **формулирование целей**, которые представляют собой совокупность желаемых результатов и имеют иерархическую структуру. Плановые цели должны обеспечивать основу для единообразного планирования на всех уровнях управления, предпосылки для последующего более детального планирования, основу для руководства выполнения планов, для мотивации поведения людей, т. е. понимания ими значения выполняемых работ; основу для четкого распределения ответственности и децентрализации планирования на всех уровнях управления, для координации различной деятельности функциональных подразделений аппарата управления КСЗИ;
- **выбор критериев**, определяющемся целями планируемой деятельности.

2. **Анализ условий**. Анализируются условия, в которых будет осуществляться планируемая деятельность. Анализу подлежат как внешние условия, так и внутренние (организационная структура, характеристики персонала, имеющиеся технологические схемы и т. д.). Кроме того, в ходе функционирования КСЗИ могут возникнуть различные непредвиденные ситуации, а также система будет испытывать на себе воздействие дестабилизирующих факторов. Все эти условия должны быть проанализированы.

3. **Формирование задач**. Осуществляется постановка задачи и формируется комплекс задач, решение которых приведет к достижению конкретных плановых целей, а также определяются методы и разрабатываются процедуры решения каждой задачи.

4. **Анализ ресурсов**, которые могут быть использованы для решения задач. Анализируются материальные (информационные, технические, программные, математические, лингвистические) и людские ресурсы. Разрабатываются прогнозы изменения этих ресурсов в процессе реализации планов. Определение факторов, влияющих на удовлетворение потребностей в ресурсах, зависит от вида планирования, т. е. от длительности планируемого периода.

5. **Согласование целей, задач, условий, ресурсов**. На этой стадии происходит выделение комплексов задач в соответствии с целями и условиями распределения ресурсов по задачам и закрепление за каждой задачей конкретных исполнителей.

6. **Определение последовательности выполнения задач**. Данная стадия выполняется путем установления взаимосвязи результатов решений задач. Определяется время, необходимое для выполнения каждой задачи, сроки выполнения, ответственные за выполнение задач.

7. **Определение методов контроля выполнения планов**. Эта стадия:

- зависит от целей планирования, выбранных критериев, а также подхода и методов планирования;
- включает в себя определение параметров плана и разработку соответствующих процедур контроля.

Методы контроля будут эффективны только тогда, когда они выявляют характер и причины отклонения от плана.

8. **Определение порядка корректировки планов**.

Порядок должен быть регламентирован. Корректировка должна проводиться в той мере, в какой это необходимо для достижения поставленных целей. На этой стадии определяются параметры планов, подлежащих корректировке, условия корректировки планов, способы корректировки, а также разрабатываются процедуры 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

Контроль является одним из важнейших и необходимых направлений работ по ЗИ. **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** режимом, обстановкой и оценка характера допущенных отклонений и недоработок.

3. **Разработка мероприятий по улучшению и корректировке** процесса управления и принятие мер по их реализации.

При принятии управленческого решения контроль выступает как источник информации, использование которого позволяет судить о содержании управленческой работы, ее качестве, результативности. Отказаться от контроля нельзя, так как это будет означать утрату информации и, следовательно, потерю управления. Контроль не является самоцелью и нужен для того, чтобы

качественно обеспечить выполнение принятых решений.

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 представляют собой совокупность организационных и технических мероприятий, проводимых с целью проверки выполнения установленных требований и норм по ЗИ.

Организационные меры контроля включают:

1) проверку **выполнения сотрудниками требований по обеспечению сохранности КТ**. Такая проверка может проводиться в течение рабочего дня руководителем предприятия, его заместителем, исполнительными директорами, начальниками объектов;

2) проверку выполнения **пропускного режима**, т. е. проверку наличия постоянных пропусков у сотрудников предприятия, проверку работы охранника (на месте или нет, проверяет пропуска или нет). Может проводиться ежедневно начальником охраны объекта;

3) проверку **выполнения** сотрудниками **правил работы с конфиденциальными документами** (правила хранения, размножения и копирования). Может проводиться заместителем руководителя в любое время;

4) проверку **наличия защищаемых носителей конфиденциальной информации**. Может проводиться сотрудниками предприятия в конце рабочего дня.

Могут применяться следующие **виды контроля**:

- **предварительный;**
- **текущий;**
- **заключительный**.

Предварительный контроль обычно реализуется в форме определенной политики, процедур и правил. Прежде всего, он **применяется по отношению к трудовым, материальным и финансовым ресурсам**. Предварительный контроль осуществляется при любых изменениях состава, структуры и алгоритма функционирования СЗИ, т. е. при установке нового технического устройства, при приеме нового сотрудника, при проведении ремонтных работ.

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

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

Также с целью обеспечения систематического наблюдения за уровнем защиты может осуществляться периодический контроль. **Периодический контроль** (ежедневный) проводится сотрудниками предприятия в части **проверки наличия носителей информации**, с которыми они работают. Периодический контроль может быть гласным и негласным.

Гласный периодический контроль эффективности ЗИ проводится выборочно (применительно к отдельным структурным подразделениям или отдельным работам) или на всем предприятии по планам, утвержденным руководством.

Негласный контроль осуществляется с целью объективной оценки уровня ЗИ и, прежде всего, **выявления слабых мест в СЗИ**. Кроме того, такой контроль оказывает психологическое воздействие на сотрудников, вынуждая их более тщательно выполнять требования по обеспечению ЗИ. Добросовестное и постоянное выполнение сотрудниками требований по ЗИ основывается на рациональном сочетании способов побуждения и принуждения. Принуждение - способ, при котором сотрудники вынуждены соблюдать правила обращения с носителями конфиденциальной информации под угрозой материальной, административной или уголовной ответственности. Побуждение предусматривает использование моральных, этических, психологических и других нравственных мотивов для создания у сотрудников установки на осознанное выполнение требований по ЗИ. Поэтому на эффективность защиты влияет климат на предприятии, который формируется его руководством.

12 УПРАВЛЕНИЕ КСЗИ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

12.1 Понятие и виды чрезвычайных ситуаций

Обеспечение продолжительного нормального функционирования в любой системе требует пристального внимания по отношению к потенциальным нештатным ситуациям. Подготовка к работе в условиях таких ситуаций призвана свести к минимуму потери из-за нарушения функционирования, обеспечить согласованность и эффективность действий персонала и локализовать негативные воздействия.

Все ситуации, возникающие в процессе функционирования,

можно условно разделить на две группы: нормальные и ненормальные. Ненормальные ситуации в свою очередь делятся на аварийные, потенциально аварийные и 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

Основные особенности функционирования систем управления в условиях ЧС состоят в том, что проблема (чрезвычайная ситуация) возникает неожиданно, внезапно; возникая, она ставит перед системой управления задачи, не соответствующие стационарному режиму работы организации и ее прошлому опыту. 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.

В этих условиях может возникнуть опасность всеобщей паники. Руководители нижнего уровня, оказавшись в неожиданной ситуации, не имея указаний сверху и общей картины ситуации, могут поддаться этой панике и непродуманными решениями способствовать неразберихе. К тому же следует отметить, что многие руководители не могут изменить стиль своего мышления и деятельности в условиях скачкообразных, неожиданных изменений ситуации. Поэтому **инициатива снизу**, часто повышающая в обычных условиях эффективность принимаемых решений, **в условиях ЧС теряет свою действенность и может оказаться небезопасной**.

Функциональная структура системы управления по предупреждению ЧС и действиям в ЧС должна охватывать весь круг проблем, касающихся ЧС, включая этапы их прогнозирования, предупреждения и подготовки к функционированию в условиях ЧС, а также ликвидации ее последствий.

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

- **повседневной деятельности**;
- **повышенной готовности** (активная подготовка и осуществление превентивных мероприятий);
- **чрезвычайный** (действия в чрезвычайных ситуациях);
- **постчрезвычайный режим** (ликвидация долговременных последствий ЧС).

Первый 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, которые позволяют эффективно реагировать на ожидаемые проблемы, паспортизация и категоризация организаций, цехов, технологий и т. д. В данном режиме определяются и создаются нормативные, законодательные и экономические механизмы, направленные на минимизацию риска и ущерба от ЧС.

Эффективные подсистемы противоаварийного упреждающего планирования должны не только прогнозировать возникновение ЧС, но и предусматривать соответствующие меры, причем упор должен делаться на устранение исходных причин, а не возникающих последствий.

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 ее развития и ответных действий.

Прогнозирование возможностей возникновения ЧС и процедуры планирования базируются на регулярной оценке тенденций развития текущей ситуации, а также ресурсов, необходимых для ее улучшения, стабилизации и снижения тяжести последствий развития ЧС.

Отсутствие необходимой информации часто становится основным препятствием для организации системы раннего

предупреждения. Часто это обусловлено недостаточно активным использованием данных. Когда некоторые неожиданные факторы лишь начинают влиять на организацию (структуру), их воздействие обычно остается скрытым в рамках обычных, нормальных колебаний.

Момент времени, когда накопившиеся данные с высокой степенью вероятности свидетельствуют о том, что ухудшение ситуации становится необратимым и необходимо принятие контрмер, назовем моментом начала развития ЧС. Этот момент является самым опасным и критическим для лиц, которые первыми должны среагировать на возникновение ЧС.

12.3 Факторы, влияющие на принятие решения

Основными причинами запаздывания ответных действий являются:

1. **Инерционность информационной системы**, объясняемая необходимостью затрат времени на наблюдение, обработку и интерпретацию результатов наблюдения, передачу полученной информации соответствующим руководителям. Инерционность является также следствием затрат времени со стороны руководства на обмен информацией друг с другом и выработку общей позиции.

2. **Необходимость проверки и подтверждения достоверности информации о возникновении ЧС**.

Безусловно, это необходимо, но даже при абсолютно достоверной информации некоторые руководители будут утверждать, что нет абсолютной уверенности в реальности возникновения ЧС, устойчивом и угрожающем характере ее развития. Они будут выступать за то, чтобы еще немного подождать и посмотреть, не отпадет ли угроза сама собой (Чернобыль).

3. **Психологические особенности человека**.

Некоторые руководители считают, что признание существования ЧС отразится на их репутации либо приведет к потере занимаемого положения. Другие руководители, даже если убеждены в реальности ЧС, будут тянуть время, чтобы выработать тактику для реабилитации своего положения.

Эти причины вызывают значительное запаздывание адекватной реакции руководства на появление ЧС и могут привести к резкому увеличению общего ущерба, а в ряде случаев способны свести на нет все потенциальные возможности противоаварийных действий.

Таким образом, чтобы не потерять и полностью использовать имеющиеся возможности и преимущества, необходимо не только совершенствовать работу подсистемы противоаварийного упреждающего планирования, но и повышать готовность руководителей к работе в условиях высокой степени неопределенности.

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.

В отличие от обычных систем планирования и управления, в том числе систем стратегического планирования, которые призваны рассматривать стратегические задачи в течение достаточно долгого периода, системы управления в условиях ЧС должны действовать в реальном масштабе времени. Стратегические задачи должны решаться в системе управления ЧС на ограниченном интервале времени оперативно и непрерывно.

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.

Принятие и реализация решения - сложные процессы управленческой деятельности, в которых, как в никаких других, от руководства органов управления требуется компетентность, высокая оперативная подготовка, знания и навыки использования техники, умение ставить цели и достигать их, брать ответственность на себя. 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 и обеспечивать наиболее полное и эффективное использование имеющихся возможностей.

Для этого требуется четкое уяснение руководством целей и задач операции, всесторонняя и объективная оценка обстановки, компетентность. Говоря о принятии решений, следует иметь в виду следующие основные составляющие этого сложного процесса: сбор и подготовку исходящих данных, построение модели ЧС, формулировку (принятие) решения руководителем, конкретизацию и детализацию решения в плане операции, доведение данного решения до исполнителей, а также организацию, оперативное управление и контроль за его реализацией.

Информационная поддержка принятых решений. При управлении в условиях ЧС не существует затрат, не связанных с использованием информации. Информация, информационный фонд в условиях ЧС становятся основным ресурсом эффективного принятия решений, направленных на ликвидацию ЧС.

Как правило, в условиях ЧС основной проблемой в принятии и реализации эффективных управленческих решений является недостаток не ресурсов и капитала, а информации, необходимой для использования этих ресурсов и капитала с наибольшим успехом.

Информация о возможности возникновения ЧС и тенденциях ее развития поступает в систему управления в ходе изучения обстановки.

Степень предсказуемости ЧС очень невелика: к моменту получения информации, достаточной для выработки эффективных ответных мер, образуется дефицит времени для их реализации. Это приводит к очевидному парадоксу в условиях ЧС: ожидая получения достоверной и достаточной для принятия решений информации, руководитель не может предпринять продуманные меры в целях разрешения возникающих проблем.

Поэтому **на ранних стадиях потенциальной опасности ЧС ответные меры**, очевидно, **должны быть общего характера, направленные на увеличение стратегической гибкости организации**. По мере поступления конкретной, детализированной информации должны быть конкретизированы и ответные меры, конечной целью которых является либо устранение угрозы

возникновения ЧС, либо использование создавшихся возможностей для ликвидации ЧС и ее последствий.

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** и т. п. Круг лиц, входящих в состав данных групп, определяется с учетом направленности деятельности предприятия, наличия или отсутствия филиалов, географией размещения служебных, производственных, складских, транспортных помещений и других факторов. В числе постоянных представителей подобных структур выступают руководители предприятия и службы безопасности, руководители функциональных подразделений, юрист, специалист финансового отдела, специально выделенные сотрудники функциональных подразделений.

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**, определение приоритетов при разработке и осуществлении основных мероприятий;
- **сбор, обработка и предоставление необходимой информации для руководителей**, принимающих решения в условиях протекания ЧС, предупреждение о внезапных изменениях в зонах действия ЧС.

При разработке мероприятий по подготовке к действиям в условиях ЧС необходимо учитывать, что в период протекания подобных ситуаций психологические нагрузки возрастают, поведенческие и эмоциональные реакции человека меняются, может нарушаться координация движений, понижается внимание и восприятие окружающей действительности. Поэтому **необходимо проводить различные тренинги, комплексы учебных занятий, которые позволили бы подготовить персонал** и повысить эффективность его работы, выражающуюся в принятии четких адекватных мер в сложившейся ситуации.

ЗАКЛЮЧЕНИЕ

Рассмотрены вопросы организации КСЗИ на предприятии. Затронуты наиболее важные аспекты научно-методологических основ, рассмотрены основные виды угроз и каналы утечки информации, технология организации СЗИ.

Главная цель курса - показать, что построение именно комплексной системы может сделать работу по организации защиты информации наиболее эффективной.

При этом надо понимать, что именно комплексность решений подразумевает взвешенный дифференцированный подход к этой проблеме. При создании КСЗИ обязательно надо учитывать особенности предприятия, ценность информации и т. д.

Начинать работу по организации КСЗИ необходимо с выявления информационных ресурсов предприятия, подлежащих защите. Далее следует провести оценку возможного ущерба от утечки данных, подлежащих защите, и классифицировать информацию по степеням важности. Затем определить все виды носителей информации, требующих защиты, и возможные угрозы. Учитывая именно эти (и еще ряд других) факторы, необходимо определить состав разрабатываемой системы.

КСЗИ представляет собой действующие в единой совокупности законодательные, организационные, технические и другие меры, обеспечивающие защиту информации. Связующим звеном в этой системе является управляющий орган (например, отдел по ЗИ), который может быть представлен, как подразделением, осуществляющим руководство, так и одним сотрудником, отвечающим за эту деятельность.

И наконец, никакую систему защиты нельзя считать абсолютно надежной, поэтому необходимо осуществлять постоянный мониторинг и развитие функционирующей на предприятии системы защиты информации.