***В.В. Ершов**, доцент кафедры БЖД УлГУ, к.в.н., доцент.*

Лекция 4.1.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРОИЗВОДСТВЕННОГО МЕНЕДЖМЕНТА И ЗАЩИТА ИНФОРМАЦИИ

Учебные вопросы:

1. ***ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРОИЗВОДСТВЕННОГО МЕНЕДЖМЕНТА***

2. ***ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ***

1. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРОИЗВОДСТВЕННОГО МЕНЕДЖМЕНТА

- К функциям организационного управления на предприятии относятся:
  - нормирование,
  - планирование,
  - учет,
  - отчетность,
  - регулирование (анализ и принятие решения),
  - контроль.

Функция нормирования

- **Функция нормирования носит название функции технической подготовки производства и, в свою очередь, подразделяется на конструкторскую и технологическую подготовку:**
  - Конструкторская подготовка производства представляет собой функцию управления, связанную с разработкой конструкций изделий. Данная функция реализуется отделом главного конструктора. Основная цель функции заключается в сокращении сроков подготовки к выпуску новой и модернизации освоенной продукции.
  - Технологическая подготовка производства является функцией управления по разработке технологического процесса изготовления изделия и реализуется в отделах главного технолога, главного механика и главного энергетика. Цель функции состоит в минимизации расходов материальных и временных ресурсов и обеспечении заданных свойств продуктов труда.

Функция планирования

- **Функция планирования включает технико-экономическое и оперативно-производственное планирование:**
  - Технико-экономическое планирование разрабатывает плановые технико-экономические показатели эффективной работы предприятия, цехов и участков. Функция технико-экономического планирования реализуется в ПЭО, ОТиЗ, в ФО, в ОМТС, маркетинга и рекламы, в структурных подразделениях. Цель функции заключается в снижении себестоимости продукции, повышении прибыли, увеличении выручки от реализации продукции за счет рационального использования ресурсов.
  - Оперативно-производственное планирование служит для непосредственного управления производством на уровне предприятия, цехов и участков и обеспечивает максимальную детализацию производственных заданий и технико-экономических показателей, доведение их до конкретного исполнителя, увязку заданий по всем подразделениям предприятия по номенклатуре, количеству и временным периодам. Функция выполняется в производственно-диспетчерском отделе предприятия, в подразделениях цехов и участков основного и вспомогательного производств. Цель функции заключается в обеспечении эффективного использования всех видов ресурсов.

Бухгалтерский учет и отчетность

- **Бухгалтерский учет и отчетность** - функция управления, объединяющая различные виды учета (первичного, аналитического и синтетического) в единое целое; осуществляется по основным участкам учета (учёта труда и заработной платы, основных средств, материальных ресурсов, готовой продукции, финансов, затрат на производство, сводного учета). В бухгалтерской отчетности (балансе) отражается деятельность предприятия по разделам актива (внеоборотные активы, оборотные активы) и пассива (капитал и резервы, долгосрочные пассивы, краткосрочные пассивы).
- В процессе реализации функции используются основные методы и приемы бухгалтерского учета (документирование, инвентаризация, системы аналитических и синтетических счетов и метод двойной записи). Функция выполняется в бухгалтерии и в учетных группах цехов. Цель функции состоит в определении фактического состояния управляемого объекта и его элементов в денежном выражении.

Статистический учет и отчетность

- **Статистический учет и отчетность** - функция, фиксирующая экономическое и финансовое состояние предприятия на основе использования специальных методов статистики. Функция реализуется в бухгалтерии, финансовом отделе, отделе организации труда и заработной платы.

Ее цель - подготовка и обработка информации для выявления тенденций возникновения экономических и финансовых событий, происходящих в процессе реализации производственной деятельности предприятия.

Оперативный учет и отчетность

- **Оперативный учет и отчетность** - разновидность учетной функции, связанной с наблюдением за ходом производственного процесса. Реализуется диспетчерской службой. Цель функции состоит в сборе необходимой информации для оперативного анализа и принятия решения по управлению ходом производственного процесса.
- **Функции принятия решения** (общего и оперативного) направлены на устранение причин возникновения отклонений. Функция реализуется менеджерами верхнего, среднего и нижнего уровней. Цель функции заключается в выработке управляющего воздействия для реализации производственного процесса.
- **Функция контроля** непосредственно связана с оценкой соответствия выполнения хозяйственных операций законодательству, правилам, стандартам, инструкциям, другим нормативно-правовым актам вышестоящих организаций и ответственных за деятельность предприятия должностных лиц.

Функции технологического управления

- **Под функциями технологического управления** понимаются функции, выполняемые операторами и механизмами для обеспечения производственного процесса. В состав функций технологического управления входят функции:
  - календарного планирования, определяющего входные временные и технические параметры работы технологической линии;
  - учета ситуаций, анализа и принятия решения в реальном времени.

Технико-экономическое планирование

- **В технико-экономическом планировании решаются задачи:**
  - формирование оптимального производственного плана с точки зрения различных критериев оптимальности;
  - распределение годовой производственной программы на полугодие, квартал, два месяца, месяц;
  - расчет коэффициентов использования производственной мощности и загрузки оборудования по группам взаимозаменяемого оборудования на изделие-представитель;
  - определение дополнительной потребности в оборудовании.

Оперативное управление

- Подсистема оперативного управления основным производством реализует следующие функциональные задачи:
  - определение календарно-плановых нормативов;
  - формирование оптимальных производственных программ по предприятию, цеху, участку на декаду, смену, час;
  - расчет развернутого плана потребности в деталях, сборочных единицах на товарный выпуск;
  - оперативный учет состояния межцеховых и внутрицеховых заделов;
  - расчет плана сдачи и получения деталей, сборочных единиц в натуральном выражении;
  - расчет сменно-суточных заданий;
  - оперативный учет выполнения плана по номенклатуре и объему выпуска предприятием и цехом за час, смену, сутки, неделю, декаду;
  - оперативный учет простоев оборудования;
  - оперативный анализ отклонений от плана выпуска продукции;
  - оперативный анализ простоев оборудования по причинам и виновникам;
  - формирование планов-графиков запуска-выпуска изделий;
  - расчеты сменно-суточных заданий.

Подсистема управления материальными ресурсами

- **В подсистеме управления материальными ресурсами рассчитываются показатели:**
  - плановой и фактической величины поставки материалов на предприятие, фактических запасов материалов на складах, фактической занятости материалов в заделах в специфицированной и укрупненной номенклатуре;
  - осуществляется также сравнительный анализ с нормативными величинами запасов материальных ресурсов на складах и нормативными величинами заделов.

Подсистема управления сбытом

- **Подсистема управления сбытом** решает задачи формирования портфеля заказов, учета отгрузки и реализации продукции. Эти задачи непосредственно связаны с маркетингом, и от результатов анализа сбыта во многом зависит производственная деятельность предприятия. В качестве входной используется информация подсистемы технико-экономического управления, выходная информация используется в этой же подсистеме, а также подсистемах управления качеством и вспомогательным производством.

Подсистема управления вспомогательным производством

- **Подсистема управления вспомогательным производством** решает задачи:
  - определения плановой потребности в инструменте;
  - учета движения инструмента;
  - объема планово-предупредительных работ и фактического исполнения ремонта оборудования;
  - плановой и фактической величины грузооборота предметов и продуктов труда;
  - расчет потребности и учет всех видов энергии (электроэнергии, тепловой энергии и других видов энергии).

Задачи инженерного характера

- В подсистеме технологического управления решаются **задачи инженерного характера**:
  - расчет оптимального режима работы станков, инструмента и оптимального температурного режима;
  - определение вероятности отказа прибора, оборудования, инструмента, линии;
  - учет искажения информации датчиками;
  - обеспечение синхронизации протекания операций технологического процесса, складирования и транспортировки;
  - управление параметрами конкретного процесса;
  - оценка ситуаций и т.п.

2. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

- Под **безопасностью информационной системы** понимается *защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов*. Иначе говоря, это способность противодействовать различным возмущающим воздействиям на ИС.

Угроза безопасности информации

- Под **угрозой безопасности информации** понимаются *события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств*.

- **Активные угрозы** имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например:
  - вывод из строя компьютера или его операционной системы;
  - искажение сведений в БиД;
  - разрушение ПО компьютеров;
  - нарушение работы линий связи и т.д.

Источники активных угроз

- **Несанкционированный доступ** - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.
- **Логические бомбы**, как вытекает из названия, используются для искажения или уничтожения информации, реже с их помощью совершаются кража или мошенничество. Манипуляциями с логическими бомбами обычно занимаются чем-то недовольные служащие, собирающиеся покинуть данную организацию, но это могут быть и консультанты, служащие с определенными политическими убеждениями и т.п.

Программные вирусы

- **Троянский конь** - программа, выполняющая в дополнение к основным, т.е. запроектированным и документированным деист действиям, дополнительные, не описанные в документации.
- **Вирус** - программа, которая может заражать другие программы путем включения в них модифицированной копии, обладающей способностью к дальнейшему размножению.
- **Червь** - программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. Червь использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.
- **Захватчик паролей** - это программы, специально предназначенные для воровства паролей. При попытке обращения пользователя к терминалу системы на экран выводится информация, необходимая для окончания сеанса работы.

Политика безопасности

- **Политика безопасности** - представляет собой набор законов, правил и практического опыта, на основе которых строятся управление, защита и распределение конфиденциальной информации.

Методы и средства построения систем информационной безопасности

- **Создание систем информационной безопасности (СИБ) в ИС и ИТ основывается на следующих принципах:**

1. Системный подход к построению системы зашиты, означающий оптимальное сочетание взаимосвязанных организационных, программных, аппаратных, физических и других свойств, подтвержденных практикой создания отечественных и зарубежных систем защиты и применяемых на всех этапах технологического цикла обработки информации.
2. Принцип непрерывного развития системы. Этот принцип, являющийся одним из основополагающих для компьютерных информационных систем, еще более актуален для СИБ.
3. Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки, т.е. предоставление как пользователям, так и самим работникам ИС минимума строго определенных полномочий, достаточных для выполнения ими своих служебных обязанностей.

Принципы создание систем информационной безопасности

4. Полнота контроля и регистрации попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ИТ без ее предварительной регистрации.
5. Обеспечение надежности системы защиты, т. е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий взломщика или непреднамеренных ошибок пользователей и обслуживающего персонала.
6. Обеспечение контроля за функционированием системы защити, т.е. создание средств и методов контроля работоспособности механизмов защиты.
7. Обеспечение всевозможных средств борьбы с вредоносными программами.
8. Обеспечение экономической целесообразности использования системы защиты, что выражается в превышении возможного ущерба ИС и ИТ от реализации угроз над стоимостью разработки и эксплуатации СИБ.

Обеспечение защиты информации

- **Правовое обеспечение** - совокупность законодательных актов нормативно-правовых документов, положений, инструкций, руководств, требования которых являются обязательными в рамках сферы их деятельности в системе защиты информации.
- **Организационное обеспечение** - имеется в виду, что реализация информационной безопасности осуществляется определенными структурными единицами, такими, например, как служба безопасное фирмы и ее составные структуры: режим, охрана и др.
- **Информационное обеспечение** - включающее в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование СИБ.
- **Техническое (аппаратное) обеспечение** - предполагается широкое использование технических средств как для защиты информации, так и для обеспечения деятельности СИБ.

Обеспечение защиты информации

- **Программное обеспечение** - имеются в виду различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и способов несанкционированного доступа к информации.
- **Математическое обеспечение** - это - математические методы, используемые для различных расчетов, связанных с оценкой опасности технических средств, которыми располагают злоумышленники, зон и норм необходимой защиты.
- **Лингвистическое обеспечение** - совокупность специальных языковых средств общения специалистов и пользователей в сфере обеспечения информационной безопасности.
- **Нормативно-методическое обеспечение** - сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации; различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований соблюдения конфиденциальности.

Этапы внедрения систем защиты информации

- **Первый этап (анализ объекта защиты)**

  Состоит в определении того, что нужно защищать:

  - определяется информация, которая нуждается в защите;
  - выделяются наиболее важные элементы (критические) защищаемой информации;
  - определяется срок жизни критической информации (время, необходимое конкуренту для реализации добытой информации);
  - определяются ключевые элементы информации (индикаторы) отражающие характер охраняемых сведений;
  - классифицируются индикаторы по функциональным зонам предприятия (производственно-технологические процессы, система материально-технического обеспечения производства, подразделения управления).

Этапы внедрения систем защиты информации

- **Второй этап предусматривает выявление угроз:**
  - определяется, кого может заинтересовать защищаемая информация;
  - оцениваются методы, используемые конкурентами для получения этой информации;
  - оцениваются вероятные каналы утечки информации;
  - разрабатывается система мероприятий по пресечению действий конкурента или любого взломщика.

Этапы внедрения систем защиты информации

- **Третий этап** - проводится анализ эффективности принятых и постоянно действующих подсистем обеспечения безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т.д.).
- **Четвертый этап** - определяются необходимые меры защиты. На основании проведенных на первых трех этапах аналитических исследований вырабатываются необходимые дополнительные меры и средства по обеспечению безопасности предприятия.
- **Пятый этап** - руководителями фирмы (организации) рассматриваются представленные предложения по всем необходимым мерам безопасности и расчеты их стоимости и эффективности.
- **Шестой этап** - состоит в реализации принятых дополнительных мер безопасности с учетом установленных приоритетов.
- **Седьмой этап** - предполагает контроль и доведение до персонала фирмы реализуемых мер безопасности.

Благодарю за внимание