ТЕМА 1. СУЩНОСТЬ ОРГАНИЗАЦИОННОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Основные направления, принципы и условия организационной защиты информации

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

⇩

Организационная защита информации — **составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации**

!

Организационная защита информации на предприятии — **регламентация производственной деятельности и взаимоотношений субъектов (работников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.**

⇩

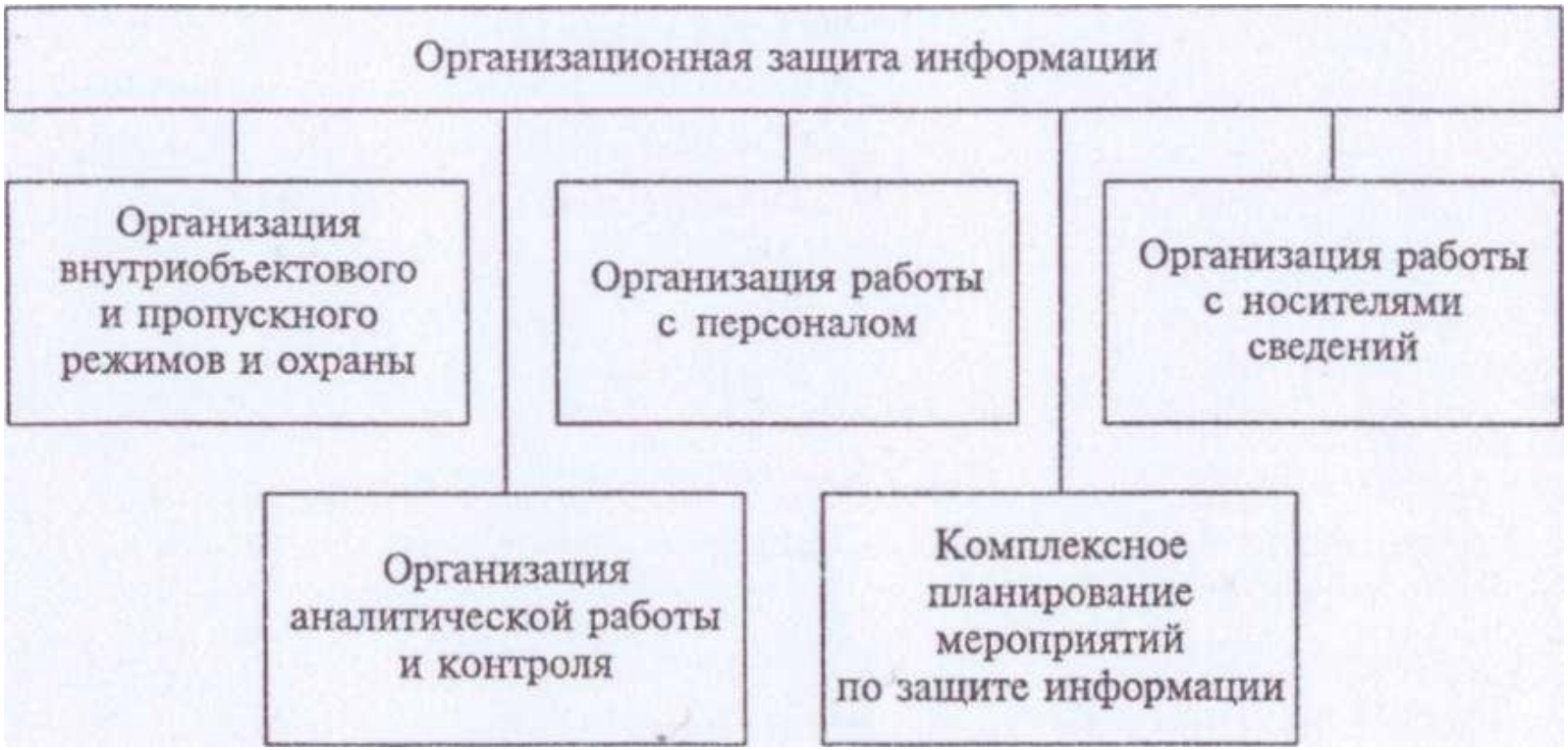
Первое из приведенных определений в большей степени показывает **сущность** организационной защиты информации.

Второе — раскрывает ее **структуру** на уровне предприятия.

Вместе с тем оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся **сил и средств.**

!

Основные направления организационной защиты информации приведены на рисунке 1.



!

Рис. 1. Основные направления организационного обеспечения информационной безопасности

Основные принципы организационной защиты информации:

принцип комплексного подхода — **эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;**

!

принцип оперативности принятия управленческих решений **(существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);**

принцип персональной ответственности — **наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.**

Среди основных условий организационной защиты информации можно выделить следующие:

- **непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;**

- **неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.**

При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты информации предприятия.

От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом.

Среди основных направлений защиты информации наряду с организационной выделяют правовую и инженерно-техническую защиту информации. Однако организационной защите информации среди этих направлений отводится особое место.

Организационная защита информации призвана посредством выбора конкретных сил и средств, в том числе правовых и инженерно-технических, реализовать на практике спланированные руководством предприятия меры по защите информации. Эти меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее утечке.

1.2. Основные подходы и требования к организации системы защиты информации

Успешное решение комплекса задач по защите информации не может быть достигнуто без **создания единой основы**, которой призвана стать сама система защиты информации на предприятии, создаваемая на соответствующей нормативно-методической основе и отражающая все направления и специфику деятельности данного предприятия.

!

Под *системой защиты информации* **понимают совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях.**

Для **решения организационных задач по созданию и обеспечению** функционирования системы защиты информации **используются несколько основных подходов**, которые вырабатываются на основе существующей нормативно-правовой базы и с учетом методических разработок по тем или иным направлениям защиты информации.

Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия с учетом устремленности конкурирующих организаций к овладению информацией и, тем самым, нанесению ущерба предприятию.

!

Важным элементом анализа является работа **по определению перечня** защищаемых информационных ресурсов с учетом особенностей их расположения (размещения) и доступа к ним различных категорий работников (работников других предприятий).

Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности.

При создании системы защиты информации, в первую очередь, учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания.

Предпочтение также отдается новым, перспективным направлениям деятельности предприятия, которые связаны с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям.

В соответствии с названными приоритетами формируется **перечень возможных угроз информации**, подлежащей защите, и определяются конкретные **силы, средства, способы и методы** ее защиты.

!

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность.

Система защиты информации должна быть:

1. *централизованной* — **обеспечивающей эффективное управление системой со стороны руководителя и должностных лиц, отвечающих за различные направления деятельности предприятия;**

2. *плановой* — **объединяющей усилия различных должностных лиц и структурных подразделений для выполнения стоящих перед предприятием задач в области защиты информации;**

3. *конкретной и целенаправленной* — **рассчитанной на защиту абсолютно конкретных информационных ресурсов, представляющих интерес для конкурирующих организаций;**

4. *активной* — **обеспечивающей защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;**

5. *надежной и универсальной* — **охватывающей всю деятельность предприятия, связанную с созданием и обменом информацией.**

!

1.3. Основные методы, силы и средства, используемые для организации защиты информации

Один из важнейших факторов, влияющих на эффективность системы защиты конфиденциальной информации, — **совокупность сил и средств предприятия, используемых для организации защиты информации.**

Силы и средства различных предприятий отличаются **по структуре, характеру и порядку** использования. Предприятия, работающие с конфиденциальной информацией и решающие задачи по ее защите в рамках повседневной деятельности на постоянной основе, вынуждены с этой целью создавать **самостоятельные структурные подразделения** и использовать высокоэффективные **средства защиты информации**.

!

Если предприятия лишь эпизодически работают с конфиденциальной информацией в силу ее небольших объемов, вместо создания подразделений они могут включать в свои штаты **отдельные должности специалистов по защите информации**. Данные подразделения и должности являются **органами** защиты информации.

!

Предприятия, работающие с незначительными объемами «закрытой» информации, могут на договорной основе использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных работников, высокоэффективные средства защиты информации, а также большой опыт практической работы в данной области. (например, работа с гостайной).

Ведущую роль в организации защиты информации на предприятии играют руководитель предприятия, а также его заместитель, непосредственно возглавляющий эту работу.

Руководитель предприятия **несет персональную ответственность за организацию и проведение необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации.**

⇩

ОН ОБЯЗАН:

⇩

- **знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;**
- **определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;**
- **проявлять высокую требовательность к персоналу предприятия в вопросах сохранности информации;**
- **оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.**

!

Заместитель руководителя предприятия **обязан постоянно изучать все стороны и направления деятельности предприятия для принятия своевременных мер по защите информации; руководить работой службы безопасности (иных структурных подразделений, решающих задачи по защите информации); выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ.**

!

На предприятиях для организации работ по защите информации могут создаваться следующие *основные виды структурных подразделений*:

- **режимно-секретные;**
- **подразделения по технической защите информации и противодействию иностранным техническим разведкам;**
- **подразделения криптографической защиты информации;**
- **мобилизационные;**
- **подразделения охраны и пропускного режима.**

Функции, возлагаемые на перечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях.

По решению руководителя предприятия данные подразделения организационно могут объединяться в службу безопасности, руководитель которой в некоторых случаях может быть наделен статусом заместителя руководителя предприятия и полномочиями должностного лица, осуществляющего руководство работой структурных подразделений предприятия, деятельность которых связана с использованием и защитой информации.

!

Режимно-секретное подразделение, мобилизационное подразделение и подразделение по технической защите информации и противодействию иностранным техническим разведкам создаются на предприятиях, выполняющих работы с использованием сведений, составляющих государственную тайну (вне зависимости от наличия на предприятии иной информации с ограниченным доступом).

!

Режимно-секретное подразделение **является основным структурным подразделением предприятия и решает задачи организации, координации и контроля деятельности других структурных подразделений (персонала предприятия) по обеспечению защиты сведений, составляющих государственную тайну.**

На предприятиях, не выполняющих работы со сведениями, составляющими государственную тайну, для решения аналогичных задач в отношении других видов информации с ограниченным доступом создается и функционирует *служба безопасности (служба защиты информации).*

Подразделение по технической защите информации и противодействию иностранным техническим разведкам **решает задачи организации и проведения комплекса технических мероприятий, направленных на исключение или существенное затруднение добывания иностранными разведками с помощью технических средств сведений, отнесенных к конфиденциальной информации и подлежащих защите.**

!

Подразделение криптографической защиты информации **создается в целях предотвращения утечки конфиденциальной информации при ее передаче по открытым каналам (линиям) связи с помощью технических средств, а также при использовании локальных вычислительных сетей, имеющих выход за пределы территории предприятия.**

!

Подразделение охраны и пропускного режима **создается в целях предотвращения несанкционированного (бесконтрольного) пребывания на территории и объектах предприятия посторонних лиц и транспорта, нанесения ущерба предприятию путем краж (хищений) с территории предприятия материальных средств и иного имущества. В некоторых случаях для решения задач охраны и пропускного режима на предприятиях могут создаваться отдельные самостоятельные подразделения.**

Мобилизационное подразделение **решает задачи всесторонней подготовки предприятия к работе в условиях военного времени, призыва и поступления мобилизационных людских и материаль ных ресурсов.**

Кроме перечисленных подразделений предприятия к работе по организации защиты информации могут привлекаться и иные структурные подразделения, для которых выполнение мероприятий по защите информации не является основной функцией.

К таким подразделениям относятся кадровый орган, орган юридической службы (юрисконсульт), орган психологической и вос питательной работы, пресс-служба предприятия и др.

!

Особо необходимо отметить важность участия в организации зашиты информации производственных, так называемых «тематических» структурных подразделений (отдельных должностных лиц), которые создают продукцию и товары (оказывают услуги), и в связи с ним самым непосредственным образом взаимодействуют с другими предприятиями и органами государственной власти.

Для проведения работ по организации защиты информации используются также возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области.

В их числе — постоянно действующая техническая ко миссия, экспертная комиссия, комиссия по рассекречиванию носителей информации, комиссия по категорированию объектов информатизации и др.

!

Чтобы добиться максимальной эффективности при решении задач защиты информации, наряду с возможностями упомянутых штатных и нештатных подразделений (должностных лиц) необ ходимо использовать имеющиеся на предприятии **средства** защиты информации.

Под *средствами защиты информации* понимают технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты информации, а также средства, устройства и системы контроля эффективности защиты информации.

Технические **средства защиты информации —** устройства (при боры), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.

!

Криптографические **средства защиты информации —** средства (устройства), обеспечивающие защиту информации путем ее криптографического преобразования (шифрования).

Программные **средства защиты информации —** системы защи ты средств автоматизации (персональных электронно-вычислительных машин и их комплексов) от внешнего (постороннего) воздействия или вторжения.

Эффективное решение задач организации защиты информации **невозможно** без применения **комплекса** имеющихся в распоряжении руководителя предприятия соответствующих **сил и средств**. Вместе с тем определяющую роль в вопросах организации защиты информации, применения в этих целях сил и средств предприятия играют **методы защиты информации**, определяющие порядок, алгоритм и особенности использования данных сил и средств в конкретной ситуации.

!

Методы защиты информации **— применяемые в целях исключения утечки информации универсальные и специфические способы использования имеющихся сил и средств (приемы, меры, мероприятия), учитывающие специфику деятельности по защите информации.**

Общие *методы защиты информации* подразделяются на правовые, организационные, технические и экономические.

Методы защиты информации с точки зрения их теоретической основы и практического использования взаимосвязаны.

!

Правовые методы **регламентируют и всесторонне нормативно регулируют деятельность по защите информации, выделяя, прежде всего, ее организационные направления.**

Организационные механизмы защиты информации определяют порядок и условия комплексного использования имеющихся сил и средств, эффективность которого зависит от применяемых методов технического и экономического характера.

Технические методы защиты информации, используемые в комплексе с организационными методами, играют большую роль в обеспечении защиты информации при ее хранении, накоплении и обработке с использованием средств автоматизации.

!

Технические методы необходимы для эффективного применения имеющихся в распоряжении предприятия средств защиты информации, основанных на новых информационных технологиях.

Среди перечисленных методов защиты информации особо вы деляются *организационные методы,* **направленные на решение сле дующих задач:**

1. **реализация на предприятии эффективного механизма управ ления, обеспечивающего защиту информации и недопущение ее утечки;**
2. **осуществление принципа персональной ответственности руководителей подразделений и персонала предприятия за защиту информации;**
3. **определение перечней сведений, относимых на предприятии к различным категориям (видам) информации;**
4. **ограничение круга лиц, имеющих право доступа к различ ным видам информации в зависимости от степени ее секретности/конфиденциальности;**
5. **подбор и изучение лиц, назначаемых на должности, связан ные с «закрытой» информацией, обучение и воспитание персонала предприятия, допущенного к такой информации;**

!

6. организация и ведение конфиденциального делопроизводства;

7. осуществление систематического контроля за соблюдением установленных требований по защите информации.

!

Приведенный перечень организационных методов не является исчерпывающим и, в зависимости от специфики деятельности предприятия, степени секретности/конфиденциальности используемой информации, объема выполняемых работ, а также опыта работы в области защиты информации, может быть дополнен иными методами.